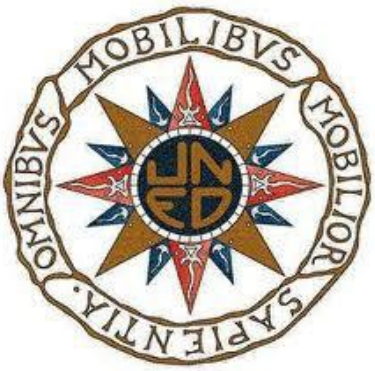
TESIS

PROTECCION DE DATOS PERSONALES EN LA HISTORIA CLINICA. EL DOCUMENTO DE SEGURIDAD EN LA NORMA ISO/IEC 27 002

MIREN AGURTZANE TAMAYO VIVANCO

LICENCIADA EN FISICA ELECTRONICA Y AUTOMATICA

MASTER EN INGENIERIA DEL SOFTWARE



DEPARTAMENTO DE INGENIERIA ELECTRICA, ELECTRONICA Y DE CONTROL, DIEEC

ESCUELA TECNICA SUPERIOR DE INGENIEROS INDUSTRIALES

UNED

2015

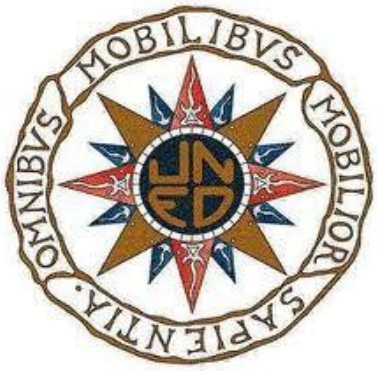
TESIS

PROTECCION DE DATOS PERSONALES EN LA HISTORIA CLINICA. EL DOCUMENTO DE SEGURIDAD EN LA NORMA ISO/IEC 27 002

MIREN AGURTZANE TAMAYO VIVANCO

LICENCIADA EN FISICA ELECTRONICA Y AUTOMATICA

MASTER EN INGENIERIA DEL SOFTWARE



DEPARTAMENTO DE INGENIERIA ELECTRICA, ELECTRONICA Y DE CONTROL, DIEEC

ESCUELA TECNICA SUPERIOR DE INGENIEROS INDUSTRIALES

UNED

2015

ESCUELA ADSCRITA DE LA UNED, MADRID:

ETSIIndustriales, DIEEC

TITULO DE LA TESIS DOCTORAL:

PROTECCION DE DATOS PERSONALES EN LA HISTORIA CLINICA.
EL DOCUMENTO DE SEGURIDAD EN LA NORMA ISO/IEC 27 002

NOMBRE Y APELLIDOS DEL AUTOR:

MIREN AGURTZANE TAMAYO VIVANCO

TITULO ACADEMICO PREVIO DEL AUTOR:

LICENCIADA EN CIENCIAS FISICAS, ESPECIALIDAD EN ELECTRONICA Y AUTOMATICA
MASTER EN INGENIERIA DEL SOFTWARE INDUSTRIAL, ESPECIALIDAD EN TIEMPO REAL

DIRECTOR DE LA TESIS:

JUAN PEIRE ARROBA. INGENIERIA ELECTRICA, ELECTRONICA Y DE CONTROL, DIEEC. ETSII NDUSTRIALES . MADRID
CO-DIRECTORA DE LA TESIS: ELENA GARCIA-CUEVAS ROQUE.
DERECHO POLITICO. FACULTAD DE DERECHO.MADRID

PROGRAMA DE DOCTORADO:
DERECHO DE LAS NUEVAS TECNOLOGIAS DE LA INFORMACION Y DE LAS COMUNICACIONES DEL DIEEC, UNED

A todos aquellos que creyeron y crean, hagan posible y certera
la e-Administración

2015

INDICE

Abreviaturas y sus Localizadores en Internet....13
Relación de Figuras....33
Relación de Tablas....35
PRESENTACION....37
English-Translation of the Presentation....39

INTRODUCCION....41

CAPITULO I: TAXONOMIA DE LA E-SANIDAD EN LA ADMINISTRACION....49

CAPITULO II: ESCENARIOS EN LA E-SANIDAD....67

1.-Semántica en el Derecho Informático....69
1.1.- Requisito Informado....70
1.2.- Autodeterminación por Consentimiento....73
1.3.- Ejercicio de los Derechos Arco....77
1.4.- El reconocimiento de la Intimidad....89
2. - Responsabilidad Técnica y Representación Legal 95
2. 1.- Responsabilidad Técnica....105
2.1.1.- Dato Médico como Dato Estadístico....107
2.1.2.- La TeleMedicina....109
2. 2.- Responsabilidad Legal....111
2.2.1.- Unidad de Defensor del Paciente....111
3.- Actores en la e-Sanidad....114
3.1.- El Controlador o Controller....114
3.2.- El Procesador o Processor....115
3.3.- La Agencia de Protección de Datos, APD y el Supervisor Europeo de Protección de Datos, European Data Protection Supervisor, EDPS....116
3.4.- El Promotor o Sponsor....120
3.5.- El Monitor....121
3.6.- Organizaciones de Investigación por Contrato, Contract Research Organization o CRO 122
3.7.- El Investigador....122
3.8.- El Auditor....123
3.9.- El Comité Ético de Investigación Clínica, CEIC....123
3.10.- La Agencia Española del Medicamento y Productos Sanitarios....124
3.11.- El Asistente en e-Sanidad....127
3.12.- El Perito....127
4.- Sistemas Informáticos Europeos....128
4.1.- Ficheros y Soportes Lógicos....132
4.2.- Sistemas Biométricos....145
4.2.1.- Vía Aérea....153
4.2.2.- Vía Marítima....154
4.2.3.- Protección de Menores....156
4.2.4.- Espacio Supranacional(Eurodac, Vis, SIS II)....157
4.2.5.- EL 'Tratado de Prum' acerca de Bases de Datos de ADN....162
4.3.- Sistemas de Alertas Alimentarias....165

4.4.- Mercado Interior, IMI....167
4.5.- Sistema Europeo de Alerta y Respuesta Temprana , EWRS....175
4.6.- El Sistema de la Historia Clínica en el Sistema Nacional de Sanidad, SNS....176
4.7.- El Sistema de Mutuas y Aseguradoras....180
4.8.- Farmacovigilancia e Investigación Clínica....187
4.9.- Soportes....189
4.9.1- ISO/IEC 27 002....190
4.9.2- Desarrollo Esquema Nacional de Seguridad: RD 03/2010....197
5.- Evaluación del Impacto en la Protección de Datos Personales, EIDP o PIA, Privacy Impact Assessment....203
6.- Orientación a una Propuesta ISO/IEC 27 002- ISO/IEC 27 799....206

CAPITULO III: ANALISIS DE RIESGOS LEGALES....219

1.- Criterios Comunes de Evaluación, CC....221
2.- Auditorías....223
3.- Datos de Carácter Personal....224
4.- Dimensiones de Seguridad....226
5.- Activos....226
6.- Gestión de Riesgos....228
7.- Esquema Nacional de Seguridad, ENS....232
8.- ISO / IEC 27 001-27 002....237
9.- Estudio de Viabilidad del Sistema y Gestión del Control del Cambio, Métrica 3....248
10.- Diccionario del Análisis de Riesgos....256
mot.1.-Convenio 108 de Estrasburgo....264
mot.2.-Convenio de Schengen....264
mot.3.-Constitución de 1978....265
mot.4.-Ley Orgánica LO 1/1982....265
mot.5.-D 95/46/CE 265
mot.6.-D 96/9/CEE....266
mot.7.-RDL 1/1996....267
mot.8.-Convenio de Oviedo....268
mot.9.-D 97/66/CE 268
mot.10.-L 5/1998....269
mot.11.-LOPDAT....269
mot.12.-D 31/2000/CEE....270
mot.13.-Ley 34/2002....271
mot.14.-Ley 41/2002....271
mot.15.- Ley 16/2003....272
mot.16.-La Comisión del Mercado de las Telecomunicaciones, CMT....272
mot.17.-Ley 32/2003....274
mot.18.-Ley L 59/2003....274
mot.19.-RD 183/2004....275
mot.20.-Ley 223/2004 277
mot.21.-RD 424/2005....277
mot.22.-D 2006/24/CE....278
mot.23.-Ley 1030/2006....279
mot.24.-Ley 11/2007, ...279
mot.25.-Ley 37/2007....280
mot.26.-Ley 56/2007....281

mot.27.-RD 1720/2007....282
mot.28.-D 2009/136/CE 283
mot.29.-D 2009/140/CE....284
mot.30.-RD 1671/2009....285
mot.31.-Resolución De Madrid....287
mot.32.-RD 3/2010....288
mot.33.-RD 4/2010....288
mot.34.-RD 207/2010....289
mot.35.-RD 1093/2010....290
mot.36.-RD 1718/2010....291
mot.37.-Directiva 2011/24/CE....293
mot.38.-RD 1495/2011....294
mot.39.-Orden HAP/566/2013....295
mot.40.-Ley 19/2013....297
mot.41.-Ley 3/2014....299
mot.42.-Ley 15/2014....300
mot.43.-RD 806/2014....302
11.- Elaboración del Documento de Seguridad....304
11.1.- Documento de Seguridad: su redacción y formato....306
11.2.- Políticas de Acceso: registros....307
11.3.- Soportes: selección y albergue....308
11.4.- Modelo de Datos: Normas de Etiquetado....310
11.5.- Aseguramiento del Plan de Calidad (hardware, HW y software, SW)....311
11.6.- Unidades Lógicas: Ficheros....312
11.7.- Periodicidades: Informes....314
11.8.- Estándares: semántica aplicada....315
11.9.- Tratamiento de Datos: responsabilidades de supervisión....316
11.10.- Auditorías....316

CAPITULO IV: SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION....319

1.- La clausula 4 de la norma ISO/IEC 27001....326
1.1.- Plan de Aseguramiento de la Calidad: Indicadores del Documento de Seguridad....331
1.2.- Marco Organizacional: WP 195 art. 29 Comisión Europea....335
2.- Control PDCA....339
2.1.- ENS....350
2.2.- El Marco de la Excelencia....354
2.2.1.- Evaluación de la Propuesta....356
2.2.2.- CAF, Common Assesment Framework....360
2.3.- Ingeniería de Software basada en Componentes....365
2.4.- Gestión de Proyecto....369

CONCLUSIONES....375

ANEXOS....381

ANEXO 1: Articulo 1. Responsabilidad Taxonómica en la Historia Clínica 381
ANEXO 2: Articulo 2. La Semántica en el Derecho de la Informática en la Historia Clínica 395
ANEXO 3: CURRICULUM VITAE....409

BIBLIOGRAFIA.....413

DOCUMENTOS Y ARTICULOS.....413
NORMAS Y ESTANDARES.....416
LEGISLACION.....421
LIBROS.....429

Abreviaturas y sus Localizadores en Internet

AAPP
Administraciones Públicas

ACE
Agencia de Certificación Electrónica
[http://www.ace.es]

ADN
Acido Dexosirribonucleico
[http://es.wikipedia.org/wiki/Friedrich_Miescher]

ADPIC
Aciuerdos sobre los derechos de la propiedad intelectual relacionados con el Comercio
[http://www.wto.org/spanish/docs_s/legal_s/27-trips.pdf]

AENOR
Asociación Española de Normalización
[http://www.aenor.es]

AEMPS
Asociación Española de Medicamentos y Productos Sanitarios
[http://www.aemps.gob.es/]

AEPD
Asociación Española de Protección de Datos
[http://www.agpd.es/portalwebAGPD/index-ides-idphp.php]

AESAN
Asociación Española de Seguridad Alimentaria y Nutrición
[http://aesan.msssi.gob.es/AESAN/web/sobre_aesan/sobre_aecosan.shtml]

AIPLA
American Intelectual Property Law Association
[http://www.aipla.org/Pages/default.aspx]

ALCA

Área de Libre Comercio de las Américas

[http://www.ftaa-alca.org/alca_s.asp]

AMIA

Ámerican Medical Informatics Association

[http://www.amia.org/about-amia/mission-and-history]

AMI

Acuerdo Multilateral sobre Inversiones

ARN

Autoridad Reguladora Nacional (Comunicaciones Electrónicas)

[http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_es.htm]

ARS

Análisis de Requerimientos del Sistema

[http://www.msc.es/organizacion/sns/planCalidadSNS/docs/ARS.pdf]

ARCO

Derechos ARCO, Principales derechos en materia de Protección de Datos Personales

[http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/index-ides-idphp.php]

BCR

Binding Corporative Rules

[http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm]

BBDD

Bases de Datos

BOE

Boletín Oficial del Estado

[http://www.boe.es/]

BSI

British Standard Institution

[http://www.bsigroup.es/]

CA

Certificate o Certification Authority

CAF

Marco Común de Evaluación o Common Assessment Framework

[http://www.aeval.es/export/sites/aeval/comun/pdf/calidad/guias/Guia_CAF_2013.pdf]

CC

Common Criteria

[http://www.commoncriteriaportal.org/]

CCAA,

Comunidades Autónomas

[http://www.msssi.gob.es/organizacion/ccaa/home.htm]

CBK

The Common Body of Knowledge

[https://www.isc2.org/]

CCN

Centro Criptológico Nacional

[https://www.ccn-cert.cni.es/]

CE

Comisión Europea o European Commission

[http://ec.europa.eu/index_es.htm]

CEDH

Convenio Europeo de Derechos Humanos

[http://www.echr.coe.int/Documents/Convention_SPA.pdf]

CEI

Comisión Electrotécnica Internacional o International Electrotechnical Commission

[http://www.iec.ch/]

CEIC

Comité Ético de Investigación Clínica

[http://www.msssi.gob.es/profesionales/farmacia/ceic/home.htm]

CEPT

Conferencia Europea de Adminitraciones de Correos y de Telecomunicaciones

[http://www.cept.org/]

CESID

Centro Superior de la Información de la Defensa

[http://www.cni.es/es/queescni/historia/elcesid/]

CNE-ISCII

Centro Nacional de Epidemiología del Instituto de Salud Carlos III

[http://www.isciii.es/]

CMT

Comisión del Mercado de Telecomunicaciones

[http://www.cnmc.es/]

CNE

Comisión Nacional de la Energía

[http://www.cne.es/cne/Home]

CNIL,

Commission nationales de l'informatique et des libertés

[http://www.cnil.fr/]

CODIS

Programa de Cotejo de Perfiles de ADN diseñado por el FBI

[http://www.interpol.int/es/Especialidades/Polic%C3%ADa-cient%C3%ADfica/ADN]

COSO

The Committee of Sponsoring Organizations (of the Treadway Commission)

[http://coso.org/]

CPSC

Comisión de Consumidores Estadounidenses para la Seguridad de los Productos, o United States Consumer Product Safety Commission

[http://www.cpsc.gov/]

CRO

Contract Research Organization

[http://www.google.es/url?q=http://apps.who.int/prequal/info_applicants/guidelines/cro_inspections.ppt&sa=U&ei=LeUfVP-SE4K1abCSgcgI&ved=0CDIQFjACOBQ&usg=AFQjCNHGVvmUI_c0F8CAqf_E5Dtta3WfHw]

CRL

Certificate Revocation List

[https://es.wikipedia.org/wiki/Lista_de_revocaci%C3%B3n_de_certificados]

CT

Expedientes de Código Tipo

DIM

Documento de Identidad del Marino

[http://www.fomento.es/MFOM/LANG_CASTELLANO/DIRECCIONES_GENERALES/MARINA_MERCANTE/TITULACIONES/Inscripcion_Maritima/DIM/default.htm]

DMCA

Digital Millenium Copyright Act

[http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281:]

DNI

Documento Nacional de Identidad

[http://www.dnielectronico.es/]

DOHA

Negociación Emprendida para liberalizar el comercio mundial, Qatar

[http://www.wto.org/spanish/tratop_s/dda_s/dda_s.htm]

EAL

Evaluation Assurance Level

[https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3%20-%20marked%20changes.pdf]

ECDC

European Centre for Disease Prevention and Control

[http://ecdc.europa.eu/en/Pages/home.aspx]

EDPS

European Data Protection Supervisor o Supervisor Europeo de Protección de Datos

[https://secure.edps.europa.eu/EDPSWEB/]

EEA-EFTA

European Economic Area, European Free Trade Association

[http://www.efta.int/eea/eea-agreement]

EEE

Espacio Económico Europeo

EEUU

Estados Unidos de América

EFTA

Asociación de Libre Comercio Europea o European Free Trade Association

[http://www.efta.int/]

EFQM

Fundación Europea para la Gestión de la Calidad

[http://www.efqm.org/]

EIDP

Evaluación del Impacto en la Protección de los Datos Personales

[http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php]

ENS

Esquema Nacional de Seguridad

[https://www.ccn-cert.cni.es/publico/ens/ens/index.html?n=2.html]

ENISA

European Union Agency for Network and Information Security

[http://rm-inv.enisa.europa.eu/]

EPO

European Protection Office

[http://www.epo.org/]

ERP

Enterprise Resource Planning

ETL

Extract, Transform and Load

ETSI

Instituto Europeo de Normas de Telecomunicaciones

[http://www.etsi.org/]

EUDRACT

European Clinical Trials Database

[https://eudract.ema.europa.eu/]

EURATOM

[http://www.minetur.gob.es/energia/nuclear/OrganismosInternacionales/Paginas/euratom.aspx]

EURODAC

[http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm]

BBDD de Huellas Dactilares en movimientos transfronterizos

[https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac]

EUROPOL

Oficina Europea de Policía

[https://www.europol.europa.eu/]

EUROJUST

Organismo Europeo para el refuerzo en materia criminal

[http://eurojust.europa.eu/Pages/languages/es.aspx]

EWRS

Early Warning Response System u Organismo de Alerta y Respuesta Temprana

[https://ewrs.ecdc.europa.eu/]

FBI

Federal Bureau of Investigation

[http://www.fbi.gov/]

FDA

La Administración para la Alimentación y los Medicamentos de los Estados Unidos

[http://www.fda.gov/]

FSIS

Servicio de Inspección y Seguridad Alimentaria

[http://www.fsis.usda.gov/]

FTC

Comisión Federal de Mercado, Federal Trade Commission

[http://www.ftc.gov/]

GFDL

GNU Free Documentation License

[https://gnu.org/licenses/fdl.html]

GNP

Gross National Product o Producto Nacional Bruto

HCR

Historia Clínica Resumida

[http://www.msc.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf]

HCDSNS

Historia Clínica Digital del Sistema Nacional de Salud

[http://www.msssi.gob.es/profesionales/hcdsns/home.htm]

HIPPA

U.S. Department of Health and Human Services

[http://www.hhs.gov/ocr/privacy/]

HW

Hardware

ICH

International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use

[http://www.ich.org/about/faqs.html]

ICM

Agencia de Informática y Comunicaciones de la Comunidad de Madrid

[http://www.madrid.org/cs/Satellite?c=CM_Presentacion_FA&cid=1109168858000&language=es&pagename=ComunidadMadrid/CM_Presentacion_FA/fichaConsjeria_Organismo]

ICMJE

International Committee of Medical Journal Editors

[http://www.icmje.org/]

ICO

Information Commissioner's Office, United Kingdom

[https://ico.org.uk/]

I+D+I

Investigación, Desarrollo e Innovación

IEEE

Institute of Electrical and Electronics Engineer

[https://www.ieee.org/]

IETF

The Internet Technical Task Force

[http://www.ietf.org/]

IHTSDO

International Health Terminology Standards Development Organization

[http://www.ihtsdo.org/]

II

Ingeniería Inversa

IMEI

International Mobile Equipment Identity o Identitidad Internacional del Equipo Móvil

[http://www.numberingplans.com/]

IMI

Sistema de Informaciín del Mercado Interior

[http://www.seap.minhap.gob.es/web/areas/sistema_IMI.html]

IMSI

International Mobile Subscriber Identity o Idebtidad Internacional del Abonado a un Móvil

[http://es.wikipedia.org/wiki/IMSI]

INTECO

Instituto Nacional de Tecnologías de la Telecomunicación

[http://www.inteco.es/]

IP

Internet Protocol

[http://rfc-es.org/rfc/rfc0791-es.txt]

IPEA

Autoridad de Examen Preliminar Internacional

[http://www.wipo.int/pct/en/access/isa_ipea_agreements.html]

IPI

Información Personalmente Identificable

ISFAS

Instituo Social de las Fuerzas Armadas

[http://www.defensa.gob.es/isfas/]

ISMS

Information Security Management System

ISCII

Instituto de Salud Carlos III

[http://www.isciii.es/]

ISO

The International Organization for Standardization

[http://www.iso.org/iso/home.html]

ITIL

Information Technology Infrastructure Library

[http://www.itil-officialsite.com/]

ITSEC

Information Technology Security Evaluation Criteria

[http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf]

JCAHO

The Joint Commission, or The Joint Commission on Accreditation of Healthcare of Organizations

[http://www.jointcommission.org/]

MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

[http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html #.VCkb-ldL4b4]

MUFACE

Mutualidad General de Funcionarios Civiles del Estado

[http://www.muface.es/]

MUGEJU

Mutualidad General Judicial

[https://mugeju.mjusticia.es/mutualnet/index.jsp]

NHIN

Nationwide Health Information Network

[http://www.healthit.gov/sites/default/files/what-Is-the-nhin--2.pdf]

LAECSP

La Ley de Acceso Electrónico a los Accesos Públicos

LES

Ley de Economía Sostenible

[http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf]

LISO

Local Informatics Security Officer

LO

Ley Orgánica

LOPD

Ley Orgánica de Protección de Datos de carácter personal, L0 15/1999

[https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750]

LORTAD

Ley derogada de Tratamiento Automatizado de Datos de 1992

LRJPAC

Ley de Protección Intelectual

[https://www.boe.es/buscar/act.php?id=BOE-A-1992-26318]

OACI

Orrganización de Aviación Civil Internacional, en inglés ICAO, International Civil Aviation Organization

[http://www.icao.int/Pages/default.aspx]

OCDE

Organización para la Cooperación y el Desarrollo Económicos, u OECD, Organisation for Economic Coopertation and Development

[http://www.oecd.org/]

OCN

Oficina Central Nacional

[http://www.interpol.int/es/Acerca-de-INTERPOL/Estructura-y-gobernanza/Oficinas-Centrales-Nacionales]

OIT

Organización Internacional del Trabajo

[http://www.ilo.org/global/lang--es/index.htm]

OMT

Organización Mundial del Comercio

OMS

Organización Mundial de la Salud

[http://www.wto.org/indexsp.htm]

OMPI

Organización Mundial de la Salud

[http://www.who.int/es/]

ONU

Organización Naciones Unidas

[http://www.un.org/es/]

ORECE

Organismo de Reguladores Europeos de las Comunicaciones Electrónicas

[http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/policy_agencies/berec/index_es.htm]

PCT

Patente Mundial

[http://www.wipo.int/pct/es/]

PCAOB

Public Company Accounting Oversight Board

[http://pcaobus.org/Pages/default.aspx]

PDCA

Plan.Do.Check.Act

[http://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

http://www.iso-9001-checklist.co.uk/iso-9001-training.htm]

PET

Privacy Enhancing Technology

[https://petsymposium.org/2015/]

PIA

Privacy Impact Assessment

[https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/]

PII

Personally Identifiable Information

[http://en.wikipedia.org/wiki/Personally_identifiable_information]

PKCS

Public Key Cryptography Standards

P3P

The Platform for Privacy References

[http://www.w3.org/P3P/]

RASFF

Rapid Alert System for Food and Field

[http://ec.europa.eu/food/food/rapidalert/index_en.htm]

RNVE o RENAVE

Red Nacional de Vigilancia Epidemiológica

[http://www.isciii.es/ISCIII/es/contenidos/fd-servicios-cientifico-tecnicos/vigilancias-alertas.shtml]

RRI

Reglamento del Régimen Interno de la Comisión del Mercado de las Telecomunicaciones

RSI

Reglamento Sanitario Internacional

[http://www.who.int/ihr/legal_issues/es/]

SAN

Sentencia Audiencia Nacional

SCIRI

Sistema Coordinado de Intercambio Rápido de Información

[http://aesan.msssi.gob.es/AESAN/web/alertas/alertas.shtml]

SET

Secure Electronic Transaction

*[*http://www.isaca.org/Journal/Past-Issues/2000/Volume-6/Pages/Secure-Electronic-Transaction-SET-Protocol.aspx *]*

SGSI

Sistema de Gestión de Seguridad de la Información

[https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/index.html *]*

SIRENE

Supplementary Information Request at the National Entry

[http://www.policia.es/org_central/dao/UCI/dao_uci_estructura.html *]*

SIS

Sistema de Información de Schengen

SNS

Sistema Nacional de Sanidad

SOX

Sarbox o SOA, Ley Sarbanes Oxley

STC

Sentencia Tribunal Constitucional

STEDH

Sentencia Tribunal Europeo de Derechos Humanos

STFCA

Sentencia Tribunal Constitucional Alemán

SW

Software

TC

Tribunal Constitucional

TCSEC

Trusted Computer System Evaluation Criteria

TDT

Televisión Digital Terrestre

[http://es.wikipedia.org/wiki/Televisi%C3%B3n_digital_terrestre]

TEDH

Tribunal Europeo de Derechos Humanos, también denominado Tribuanl de Estrasburgo y Corte Europea de Derechos Humanos

[http://www.echr.coe.int/Pages/home.aspx?p=home]

TLC

Tratado de Libre Comercio

UDA

Utilidades de Desarrollo de Aplicaciones

[https://code.google.com/p/uda/]

UIT

Unión Internacional de Telecomunicaciones

[http://www.itu.int/es/about/Pages/default.aspx]

USC

United State Code

[http://www.gpo.gov/fdsys/browse/collectionUScode.action?collectionCode=USCODE]

VIS

Sistema de Información de Visados

[http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm]

WTEC

World Technology Evaluation Center

[http://www.wtec.org/]

WHA

Resolución numerada de la Asamblea Mundial de la Salud

[http://www.who.int/mediacentre/events/governance/wha/es/]

W29

Grupo de Trabajo W2

[http://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php]

W3C

World Wide Web Consortium

[http://www.w3c.es/]

RELACION DE FIGURAS

Figura 1.
Perspectiva Lógica del ISW [368]

Figura 2.
EDT , Desglose de Trabajo [373]

RELACION DE TABLAS

Tabla 1.
Taxonomía del Paciente [062]

Tabla 2.
Taxonomía del Técnico Informático de la e-Sanidad [063]

Tabla 3.
Métrica-Gestión de Proyectos [253]

Tabla 4.
Métrica-EVS [255]

Tabla 5.
Entrada-Especificación Requisito Legal [325]

Tabla 6.
Supervisión ISO/IEC 27 001, Complemento ISO/IEC 27 002 [344]

Tabla 7.
Exposición de Conclusiones [350]

Tabla 8.
CAF-2013 – Perfil de Protección ISW [363]

PRESENTACION

La Auditoria *de Protección de Datos de Carácter Personal* impulsada bien por el *Centro Criptológico Nacional, CCN* , bien por alguna de las *Agencias de Protección de Datos* en las respectivas Comunidades Autónomas, con su consiguiente legislación regulada, encuentra su Apoyo en la Emisión de una relación de Guías por parte del Primero, y en un par de Documentos de Apoyo en la Elaboración del *Documento de Seguridad* por parte del Segundo, cuando este se reconoce como Instrumento Jurídico en la Especificación y Ordenación de la *Medidas de Salvaguardas* de Índole Técnica realizadas sobre la información de los Sistemas de Información , que son los datos.

En el ámbito de la *Historia Clínica, HC,* y debido a diferentes premisas (Nivel Alto de clasificación del dato clínico y Complejidad del *Código Tipo* de los Profesionales que participan), el *Análisis de Aproximación del Sistema de Seguridad de la Información, SGSI*, conlleva la elaboración de unas Taxonomías de los Grupos Resultantes, la identificación de unos Escenarios con sus correspondientes *Actores* , así como la Incorporación del consiguiente *Diccionario de Datos*.

El estudio orientado que realiza la legislación española en torno al *Documento de Seguridad* corre paralelo y soportado como recomienda nuestro *Esquema Nacional de Seguridad, ENS,* por una norma internacional en Seguridad de la Información , como es la *ISO/IEC 27001* y los controles que desarrolla en la *ISO/IEC 27002*. Estas normas proponen la aplicación de un Ciclo (P)Plan.(D)Do. (C)Check.(A)Act, que conlleva a su vez a la definición de un nuevo Control, Medida de Seguridad explicado sobre los controles de la *ISO/IEC 27002* y a fin de mantener el equilibrio encontrado entre las Taxonomías desarrolladas, y convirtiendo al nuevo control en *Componente* del *SGSI*.

La Introducción y Supervisión del nuevo Componente nos sirve para reiterar el apoyo que recibe la Administración Electrónica Española o *e-Administración* desde una perspectiva de la *Gestión de Riesgos* con su Métrica *MAGERIT.* Resultando el *Marco de la Excelencia* no una exigencia, pero sí una necesaria recomendación desde el punto de vista de la *Gestión de Proyectos* a fin de practicar un *Estudio de Viabilidad del Sistema* sometido a la *Gestión del Cambio* del propio *Documento de Seguridad.*

Las consideración de las Transferencias Internacionales de Datos en el ámbito de la *HC* elevan al *Supervisor Europeo de Protección de Datos* como máximo responsable en la Monitorización del

Dato en las diferentes Administraciones Europeas, así como en el Consejo de sus *Políticas de Seguridad*. A fin de satisfacer dicha supervisión se han respetado las Directrices proporcionadas por los Documentos de Trabajo generados por el *Grupo de Trabajo en materia de Protección de Datos de la Comisión Europea, Gt29* y en apoyo a la Especificación del nuevo *Componente* se aplica el Documento nº *WP 195*.

English-Translation of the Presentation

The Auditory on Personal Data Treatment driven either by the *National Criptological Center,* or either by the *National Regulatory Agencies* in their respectives Autonomical Communities and with their specific regulations, meets its support both on the publication of a profuse list of Guides, in the first case, and on a pair of documents which lead the possible implementations of the *Security Document*, *SD* , in the second one, when , besides, we recognize the *SD* as a juridic instrument on the specification and organization of the *Technical Safeguard Measures* based on the data of the *Informatic System, SI*.

On the scope of the *Clinical History*, and due to different premises (High level classification for the clinical data, and the complexity of the *Codes Types* of the Professionals who take part in), the Approximation Analysis of the *System Management Security Information , SGSI*, is associated with the elaboration of the respective *Taxonomies* of the resulted Groupes, the identification of *Scenaries* attached with their *Actors*, and, furthermore, with the integration of the *Data Diccionary*.

The oriented application that the Spanish Legislation develops around the *Security Document* is supported in comformance with the *National Security Scheme* recommendation , by using an international standard on 'Information Security' such as *ISO/IEC 27001* and the controls within it that are extended in *ISO/IEC 27002*. These standards propose the execution of a P(Plan). D(Do).C(Check).A(Act) Cycle whose followment gives us the possibility of reaching a new *Control* definition or *Safeguard Measure* explained over the *ISO/IEC 27002* controls with the goal both of maintaining the equilibrium between the published *Taxonomies*, and converting the new control in a component for the *Information Security Management System or ISMS*.

The introduction and supervision of the new component serves us to remark the help derived from the perspective of *Risk Management* with its metric *MAGERIT* in the Spanish Electronic Administration or *e-Administration.* By this way, *the Excellence Framework* results no an exigency, but a necessary recommendation from the point of view of *Project Management* with the objective of practising a *Viability Study of the System* on dependence of the *Security Document Change Management*.

On the consideration of the International Transferences of Data and on the scope of the *Clinical History*, the *European Data Protection Supervisor, EDPS*, is classified as the unique responsable of Monitoring the Data on the different european electronic administrations, who gives also counsel on *Security Policies*. In order to response to this legitimate supervision, it has been taken into account the Workshop Documents with corresponds to the *Data Treatment Working Group* named as *Gt29*, and to possibilitate the specification of the new component , the Document numbered as WP195 has been applied.

INTRODUCCION

Si difícil es para el legislador acercarse de manera prudencial al campo de las Tecnologías Informáticas , de entrada más difícil le puede resultar su equiparación al tecnólogo en su propósito de aplicar correctamente la legislación que se le va sugiriendo se aplica en el seno de la Administración Electrónica.

Se requiere del esfuerzo integrador de muchas personas trabajando funcionariamente , así como cooperando por cuenta ajena en forma de outsourcing participando en prototipos y consultorías integradoras de procedimientos que con el tiempo y la adecuada aprobación de auditorias internas y externas van encontrando su lugar o rechazo, a modo del viejo método científico de prueba y ensayo. E independientemente de que esa vieja fórmula con el tiempo pudiera desaparecer y aplicarse otras nuevas.

En ese roce que el buen sentido común y la coherencia humana pueden ayudar a suavizar, se han venido apuntando en el trascurso de los años observaciones y percepciones singulares, que no cabe duda irán encontrando su propio devenir , en algunas ocasiones refrendadas por documentos surgidos desde los propios Organismos supervisores y emisores de criterios en materia de protección de datos, y en otros expuestos después de muchísimo esfuerzo intelectual para un tecnólogo en su acercamiento de la defensa de lo que se ha venido en llamar el Derecho en la Informática.

Reconociendo, eso sí, la exigencia de ponerse de acuerdo por ambas partes y reconocer la observancia de una serie de principios que bien expuestos de manera legalista, no le incomoden al segundo y venga a devenir un nuevo territorio rico en experiencias y aportaciones por ambas partes , así como el reconocimiento debido que debería llevar asociado su divulgación y enseñanza.

Será la casuística, como en otros campos, y de ahí la importancia que en este caso merecerá otorgársela a futuros Informes Estadísticos, la que conducirá por propia inercia a la necesidad de formular mecanismos asintóticos entre ambos campos, dando lugar, tal vez a una nueva ciencia que se propague más allá del propio Derecho Informático.

La propia naturaleza de cada dato determina en alto grado los escenarios que deben observarse y donde estos datos serán tratados , surgiendo probablemente, un feedback entre sus estructuras y el grado de análisis y dominio de la manipulación en el tratamiento de cada tipo de dato , en este caso de carácter personal, y otorgándole un carácter especialísimo al dato sanitario, que es el que nos ocupará en el desarrollo de esta Tesis Doctoral.

El método de introducción que presentamos se basa en la concienciación de todas aquellas premisas que divulgadas de forma científica han podido venir en aproximar una Taxonomía de la Administración electrónica en Sanidad o e-Sanidad, y considerando que fundamentalmente la base de información residía en torno al campo de la Privacidad, en términos anglo-americanos, o Intimidad desde un perfil más europeísta. Por otra parte, se ha pretendido sumar a esta orientación el desarrollo actual que encuentra en su Estado del Arte el reconocido 'Summary Patient', formulado más allá de los Comités Éticos y la Medicina Legal.

Como consecuencia de esta disertación se llegan a proponer dos grupos taxonómicos en materia de e-Sanidad y una relación, para cada uno, de definiciones taxonómicas tal y como las observaría cada individuo perteneciente a cada Taxonomía, intentando y deseando representar una separación en la actuación de cada Grupo.

Esta orientación puede llegar a condicionar en mayor o menor medida el Índice que a continuación se expone, y que está presentado básicamente en un apartado mayormente densificado en bases de Derecho y una segunda parte que sería dirigida únicamente bajo premisas de aplicación de mecanismos de Calidad de la Seguridad de los Sistemas de Información, sin pretender romper la línea de exposición a lo largo del todo el texto.

Por la parte del Derecho y a falta de textos , por no reconocerse aún, de forma ortodoxa y profusa su Enseñanza, presenta una interesante conclusión que basa sus inicios en lo que en su día surgió como autodeterminación informática y como la Doctoranda entiende ha encontrado su fórmula y camino en el campo de la e-Sanidad, mayormente que en otros.

Idénticamente, estudiada la Jurisprudencia en materia del campo de las Telecomunicaciones, y presentando su respeto equiparador desde su perfil como Ingeniera de Software introduce requisitos legales presentados, con la mayor delicadeza, primero identificando la diversificación de Actores que participan en toda su extensión en esta materia, así como de los Escenarios Informáticos clasificados a día de hoy y que cuentan con su propia regulación, considerando colaterales que pudieran considerarse en procedimientos futuros y proponiendo algunas sugerencias integradoras.

Por otra parte, y en el feedback que se produce entre la inicial casi ausencia de legislación en los inicios de la extensión de Internet y el análisis ya fundamentado y consolidado de estándares reconocidos internacionalmente y producto de experiencias empresariales fruto de convergencia de Foros y Voluntades Participadas, se observan divergencias que en este Trabajo se ha tratado de superar en su exposición considerando como le resulta familiar al tecnólogo informático que una ausencia de legislación requiere siempre de la aplicación de los mismos, aun cuando normalmente sea desde la aplicación de la legislación en cada caso cuando éste se siente obligado a respetarlos con escrúpulo.

Una vez superada esta fase de percepción se descubrirá que los principios legales no reconocen más que un derecho fundamental que no debe ser sólo concienciado desde la parte del ciudadano-paciente del que se recaban datos para su tratamiento y mejora sanitaria, sino desde el descubrimiento maravillado que le deberá resultar al tecnólogo del mismo, y percepción de que puede repercutir precisamente en la Calidad de la Sanidad del Ciudadano.

Se recogen , pues, de esta forma los procedimientos reproducidos hasta la formulación de la Ley de la Sociedad de la Información L 1/2007 y sus consiguientes desarrollos RD 03/2010 y RD 04/2010, y los propuestos a partir de este momento , además del consiguiente apoyo que ya esta ley le otorga al grupo de estándares denominados de la familia 27 00X.

Se observará que no sólo el *Requisito Informado* observado como *Requerimiento Informático* o la importancia que adquiere la semántica alrededor del *Consentimiento Informado* son los que logran otorgarle a esta Tesis su singularidad, sino que toda la disertación en torno a la figura del denominado *Documento de Seguridad* a observar desde el responsable en materia de protección de

datos de la Unidad Técnica son originales, habiéndose encontrado en este segundo caso y capítulo un terreno de momento totalmente fértil y trabajoso.

Incluimos a lo largo de la exposición del Índice dos artículos publicados por la autora que habría que observarlos como el resultado-conclusión de una continua aplicación del método *Plan.Do.Check.Act, PDCA,* propuesto por Deming en torno a las propias ideas que se van tratando de programar.

Apuntar que un planteamiento muy primitivo del conjunto de la Tesis podría haber surgido en torno a la preocupación que la Doctoranda presentaba en torno a los Informes emitidos por el Grupo W29 en materia de protección de Datos realizaba acerca de los *BCRs* o *Binding Centre Resources* y la posible violación de los principios en materia de protocolos de comunicaciones de confidencialidad, repudio, disponibilidad e integridad, que aplicados en el campo médico desataban su plena inquietud.

Otorgándole especial importancia a los siguientes fundamentos legales,

- la observación de que la recopilación de requisitos informáticos supervisados como si fuera, porque de facto, así lo pueden ser requeridos por la Comisión del Mercado de las Telecomunicaciones da lugar a la Especificación de aquellos Escenarios donde se desenvuelve la Operativa de la *e-Health*[1]. Existe un dato realmente interesante al respecto del tiempo ganado con la aplicabilidad de la e-Health con un 22% del tiempo disponible por los médicos para la atención en proporción a los pacientes. Tomando como ejemplo el Hospital de Torrevieja , España, en términos cuantitativos podemos afirmar una mejora en el sistema sanitario. En sólo dos años, durante los cuales se iniciaron tecnologías móviles para atender a los pacientes, pasaron de tener un 195 de urgencias leves que llegaban al hospital a sólo un 2,5%. Es un claro ejemplo del uso del *m-Health*[2] de manera eficaz.

1 La OMS define la *e-health* como el uso en el sector de la salud de aquella información digital , transmitida, almacenada u obtenida electrónicamente para el apoyo al cuidado de la salud tanto a nivel local como a distancia. No se fabula si se decide que la e-health salva vidas, dado que permite el envío de datos online vitales en situaciones donde unos pocos minutos son los que separan a un paciente de la vida a la muerte. Existe un Observatorio global de la e-heatlh conocido como *Goe*, nacido a principios de 2005 y que publica un informe anual , así como directrices dirijidas a los países interesados. http://www.who.int/kms/initiatives/ehealth/en

2 ISTEPANIAN, R., & LACAL, J.. "Emerging Mobile Communication Technologies for Health: Some Imperative notes on

Existe una información ciertamente interesante al respecto de la aplicación de las televisión terrestre digital en cuanto a las posibilidades de aplicación que tiene respecto de los servicios de salud. Así, por ejemplo, la plataforma 'Sky' comenzó a ofrecer un servicio de salud a través de la televisión digital en Inglaterra, aunque ha obtenido muchas críticas.

Para aquellos que les resulte farragoso el uso de la tecnología Internet, a la hora de solicitar una cita con un médico, en el futuro y ya existen proyectos piloto se podrá pedir cita previa con el médico de familia mediante el uso de la TDT y de su correspondiente tarjeta sanitaria

- que el paciente amparado por la Ley de las Telecomunicaciones se le reconoce como *consumidor*[3] y ante el que debe de responder la premisa que los bienes o servicios puestos en el mercado para considerarse seguros no debe presentar riesgo alguno para la salud o seguridad de las personas, o únicamente los riesgos mínimos[4] compatibles con el uso o servicio y considerados admisibles dentro de un nivel elevado de protección de la salud y seguridad de las personas

- todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes, del mismo modo que supervisado conforme a procedimientos establecidos y en relación al *Registro de Actividad*[5] con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la

m-Health". The 25th Silver 59 Anniversary International Conference of the IEEE Engineering in Medicine and Biology Society. (2003): <<mHealth broadly encompasses the use of mobile telecommunication and multimedia technologies as they are integrated within increasingly mobile and wireless health care delivery systems>>
Istepanian, R.. "Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-care Connectivity". IEEE Transactions on Information Technology in Biomedicine, 8(4), 405-413. (2004):
<<mobile computing, medical sensor, and communications technologies for health care>>

3 El nuevo texto refundido en Defensa de los Consumidores. L 03/2014 y que sustituye al RD 1/2007 define al consumidor como:<< El concepto de consumidor y usuario engloba a las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. Son también consumidores y usuarios a efectos de la ley, las personas jurídicas y las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial>>, y a un producto como todo bien mueble conforme a lo previsto en art. 335 del Código Civil

4 RD 1/2007, capitulo III (art. 11)

5 RD 03/2010, (art. 23)

> normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios , reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Algunas observaciones genéricas: Igual que se hace una observación en relación a las legislaciones de la *LOPD* podemos apuntar que la *L 1/86 o Ley General de Sanidad* encuentra una primera percepción en la *ST 254/1993*(cita de *habeas data*), en torno al discurso y que también clarificado queda en la semántica, teniendo presente que la Sentencia del tribunal alemán 15/12/1983.

Además de la apreciación anterior se ha de señalar que en el año 2004 aparecen acuñados los términos m-health y t-health a la vez que se pone en marcha el proyecto de la farmacovigilancia.

El discurso histórico que se practica en torno a la Privavidad, y el modelo de aceptación de su Taxonomía, fundamentalmente en Norteamérica, nos anima a postular el equilibrio que se debería respetar en la consecucción de las áreas de Seguridad de las *Taxonomías* que se exponen y concluyen. En tal orientación decidimos apostar que la Seguridad en el Trabajo del e- Técnico reconocido como *Ingeniero de Software* conforme a las Guías del *IEEC* debe encontrar un grado de desarrollo similar a lo que ha venido en llamarse *Seguridad del Paciente*.

Destacar que el *Indice* de la Tesis propone la introducción de determinados *Requerimientos Informados* (definición y requisito legal de la Comisión del Mercado de las Telecomunicaciones), o *Requisitos Informáticos* (desde el área de la *Ingeniería del Software*) que diverge del tradicional discurso en apoyo del desarrollo del dogma legislativo, por considerar que son precisos de observar y analizar cuando se les considera como parte de determinadas especificaciones de determinadas *Categorías* de lo que venimos en llamar *Motivadores de la Gestión del Cambio en Métrica* y que contribuyen al Desarrollo y Mantenimiento del *Sistema de Seguridad del Sistema Informático*.

Si bien hemos prestado especial consideración al tratamiento de la Semántica dentro del Área

Médica y por ello hemos perseguido la publicación del segundo artículo registrado en el Anexo de esta Tesis, detectando que no se necesitaba de un incremento en la extensión de la Doctrina, sino de subrayar un hilo conductor en una trayectoria histórica.

De forma análoga se expone tanto en el contexto de la estructura de la *ISO 27001*, conjuntamente con la nueva versión del *Marco de la Excelencia*, una Propuesta que viene a reforzar la *Seguridad del Usuario* desde el lado del Trabajador que practica en la *e-Sanidad*, reforzando el Trabajo que vendría a establecer un grado de desarrollo desde el Marco de la Seguridad del Trabajador equivalente al ya alcanzado en el Área de la *Seguridad del Paciente*.

Ahora bien, ISO/IEC 27002 como compendio de controles desarrollados de ISO/IEC 27001 permite lo que se denomina un proceso de aproximación destinado al diseño y extensión del *SGSI, Sistema de Gestión de Seguridad de la Información, o ISMS, Information Security Managament System*, que no obliga a su certificación, como sí lo hace el *ISO/IEC 27001*. En la numeración de sus clausulas y subclausulas encontramos su numeración prácticamente alineada tal como se especifica en la relación *ISO/IEC 27001:Anexo A- ISO/IEC 27002.* El Anexo B de ISO/IEC 27001 describe precisamente el Ciclo PDCA necesario para la implementación del SGSI en cada una de sus etapas, recordándonos, en cualquier caso, que un pequeño Ciclo PDCA deberá de ser practicada sobre cada nuevo Control Diseñado, destacando en su fase C(Check) el modo en que ha contribuido en la Medida de la *Efectividad,* la cual suele decidir la Certificación del SGSI.

De este modo indicado, nos resultará más obvio como al final de la Tesis deberemos de poder recopilar la aproximación que se extrae Capítulo a Capítulo del Contexto Completo que hemos introducido, publicado y aquel que se pretenda superar por considerarlo fácilmente solucionable a la Vista de la Exposición completa que se hiciera de la norma *ISO/IEC 27002* en relación al *Documento de Seguridad*.

CAPITULO I: TAXONOMIA DE LA E-SANIDAD EN LA ADMINISTRACION

Abstract :

In order to express the main formulations of each Taxonomy, we walk along and by the hand of the main writers taking note each time of its main purposes that afterwords and recognising the 'Patient Security Summary' determine us to postulate two important focuses and its implementation

Claves :

Intimidad, Privacidad, Due Proccess, Uso Secundario, Grupos Taxonómicos, Seguridad del Paciente, SNS, Indicadores, Videovigilancia, e-Administración, Ciudadano, Técnico de la e-Administración, HC, Derechos ARCO, Incidencia, Alerta

La operativa que se va a recoger, esto es, el de la Historia Clínica protege en cierto modo del desconocimiento o falta de desarrollo del individuo que tenga acerca del derecho de proteger su intimidad, que en términos anglosajones es denominado *privacidad*.

Ahora bien, también es cierto que en otras ocasiones y no remitiéndose exclusivamente a los hechos materiales, ese mismo individuo 'detecta' que se ha agredido contra su persona de una forma que en ocasiones no se presenta inminentemente de forma substancial y que con posterioridad puede llegar a formular , para protegerse precisamente frente a ese tipo de agresión. Son precisamente este tipo de principios observacionales conducentes a llegar a formular toda una ley la que a continuación se intenta reorientar y describir.

Luego, inicialmente hablaremos de una Taxonomía de la Privacidad.

La Directiva de la Unión Europea en Materia de Protección de Datos protege el Derecho a la

Intimidad como principio fundamental[6]. Por su parte, en EEUU la Constitución aunque no menciona explícitamente el análogo de este palabra la trata como una salvaguarda de la santidad del hogar y de la confidencialidad de las comunicaciones desde la perspectiva de la intrusión del gobierno.

Desde 1970, el Congreso de los EEUU ha proporcionado algunas docenas de estatutos para proteger los registros del Gobierno, de estudiantes, de la información financiera, de las comunicaciones electrónicas, entre otras cosas.

De este modo, el *Informe de la Comisión 9/11*[7] recomienda que las agencias gubernamentales que comparten una gran cantidad de información entre ellas y sus negocios, debieran salvaguardar y proteger la privacidad de los individuos cuya información manejan.

En 1890 Samuel Warren y Louis Brandeis escribieron su famoso artículo 'El derecho de Privacidad'[8], arguyendo el reconocimiento legal de tal derecho, que definieron como 'el derecho a estar solo'. Esta categorización de dicho derecho ha llegado a alcanzar un estatus legendario, obteniendo el encauzamiento de la discusión de la privacidad a lo largo de todo el siglo XIX.

Warren y Brandeis declararon que su propósito consistía en considerar si la ley existente proporciona un principio que pueda ser adecuadamente invocado para proteger la privacidad de un individuo; y, si esto fuera así, en qué consistiría tanto su naturaleza como en qué consistiría dicha protección.

El propósito de Warren & Brandeis no era generar una importante concepción acerca de la privacidad, sino el explorar las mismas raíces de dicho principio en la ley y de cómo se desarrollaría este en el futuro. El discurso iniciado con la proliferación de los medios de comunicación antecedió a la Era de Internet que propondría nuevas cuestiones.

Aproximadamente alrededor del mismo tiempo que lo hicieron Warren y Brandeis, E. L. Godkin publicó un artículo en el que hacía notar que 'el derecho a decidir nuestro conocimiento sobre los pensamientos y sensaciones acerca de una persona, hechos privados y acciones sociales debería producirse bajo la protección del derecho público[9].

6 Directiva 95/46/CE, del Parlamento Europeo y del Consejo de la Unión Europea, (art. 1, 9, 13)
7 "The 9/11 Commission Report 394" National Commision on Terrorist Attacks upon the U.S. 2004
8 Samuel & Brandeis . "The Right to be Alone". December 1890
9 GODKIN, E.L. "The Right to Privacy". Scribner's Magazine Vol 8, pag. 58-68, 1890

El discurso teórico no proporciona ningún discernimiento acerca del grado del acceso necesario para constituir una violación de la privacidad.

En ocasiones, las personas no aceptan el secreto de forma completa: mas bien, se apuesta por la confidencia, que consiste en compartir la información con un selecto grupo de gente de confianza.

Los libros que leemos, los productos que compramos y las personas con las que no asociamos usualmente no se consideran secretos, y sin embargo, los consideramos como temas privados.

Generamos información conforme vamos desarrollando nuestra personalidad.

Las leyes que protegen la propiedad intelectual en la práctica protegen la expresión de las ideas y no las propias ideas. La complejidad que encierra la información personal es que además de ser una expresión del sí mismo, es registro de los actos históricos de nuestro comportamiento.

No debe de ser la presión y el pulso del Estado el que debiera definir los atributos por los que se caracteriza la personalidad: en tal línea se reafirma otro artículo que mantuvo bastante influencia llamado 'The Right to Privacy'[10], cuyo autor, Jed Rubenfeld indicó que la personalidad no puede excluir identidades imposibles de mantener o intolerantes sin abandonar el valor de neutralidad que se produce entre sus diferentes individualidades. Defendió la concepción alternativa que define el derecho a la privacidad como la libertad fundamental a tener una vida no totalmente determinada por la progresiva normalización del estado, otorgando el protagonismo requerido al *due process* que arbitra la cuarta enmienda estadounidense.

Por otra parte, no se puede ignorar la situación contextual en la que ocurre el significado. Se debe prestar atención sobre las relaciones en las que la información se trasfiere y los usos en los que la información es colocada; dichos relaciones difieren en su nivel de intimidad.
Se observa que la gente es preconsciente acerca de otros incluso en sus vidas privadas; Esa percepción ' de lo que ocurre' exige que ésta pueda venir desde una relación con el Gobierno, la política de la Comunidad, el empleo, la familia de uno, e incluso la raza, grupo étnico o grupo religioso. Por ello, y en muchas ocasiones, las personas se muestran conocedoras debido a lo que son y quien son. En otras palabras, no a través de los límites entre sectores de definición de conceptos, sino por medio de sus relaciones sociales.

10 RUBENFELD, Jed "The Right of Privacy". Faculty Scholarship Series. Paper 1569. 1989

La definición de un problema engloba cuidadosas observaciones en orden de conceptualizar generalidades. El nuevo hecho de recopilar hechos no conduce a nada. Es posible tener un trabajo de observación tan controlado por un entorno conceptual avanzado que las mismas cosas que son genuinamente decisivas en el problema y su solución se presentan excesivamente consideradas y tratadas.

Se enfatiza que debemos ser realmente cuidadosos en no permitir que dichos entornos conceptuales nos coarten nuestra habilidad de determinar situaciones concretas, reconociendo la importancia de la conceptualización y generalizaciones basadas en la experiencia. Por ello, se recomienda que el camino más óptimo en orden de evitar tal distorsión sería mantener una especial sensibilidad de la situación como un todo.

Las teorías trabajan hipótesis, no entidades fijas, y deberían ser creadas de situaciones concretas y constantemente testeadas y observando cómo van tomando forma a través de una interacción de situaciones concretas.

Los asuntos que consideraremos privados son modelados por la cultura y el tiempo y difieren a través de las sociedades y las épocas.

En la Inglaterra medieval, la agresión sexual era vista como parte del negocio de la comunidad. Frecuentemente se lanzaban acusaciones públicas de personas que mantenían este tipo de prohibidas relaciones. Cuando se presentaban pruebas al respecto, la Corte Eclesiástica realizaba una confesión pública de los implicados.
De la misma forma, y continuando con Inglaterra, el hogar fue considerado un castillo que encontró un discurso en la ley en el caso *Semayne*[11] : la casa es para cada cual su castillo y fortaleza.
Las comunicaciones se hicieron privadas porque las gente así lo quiso. La privacidad es una condición que nosotros creamos, y como tal dinámica es cambiante.

Más recientemente, Daniel Solove[12] propone una teoría que ayuda a resolver la variedad de diversos problemas que él mismo pondera en relación con su concepto. Estipula cuatro dimensiones: un método, un cierto grado de generalidad, una estructura que acomoda su variabilidad y, por supuesto,

11 Semayne Case. Wikipedia, the Free Encyclopedia
12 SOLOVE, Daniel J."Understanding Privacy". Harvard University Press, pag. 39-41, 2008

un foco, que nos indica el cambio de percepción producido en la era tecnológica al plantear esta cuestión de afrontar no sólo semánticamente la solución del concepto funcional intimidad-privacidad.

Una teoría de la privacidad debería dejar espacio para permitir variaciones históricas y culturales, aunque sin conceder demasiado variabilidad, apunta D.Solove.

The *Electronic Communications Privacy Act* de 1986 recoge que ningún tipo de información es inherentemente privado. La problemática en el reconocimiento de la naturaleza de la información nos descubre de que existen intereses creados en la aparentemente inocua información.

Luego, existe una expectación razonable acerca de los métodos que las Cortes americanas utilizan en la identificación de intereses protegidos por el derecho indicado de privacidad reconocido por la cuarta enmienda: debiendo siempre observar y si se llegara a balancear el criterio de privacidad frente al denominado 'bien social', en qué porcentaje y cómo debiera ser tratado si resultara devaluado en relación a un conjunto de intereses.

Cuando algo presenta un valor intrínseco, puede ser valorado por sí mismo, mientras que por contraste, cuando algo tiene un valor instrumentalizado, lo valoramos en la medida que puede reportar a otros algún valor.

Se deposita la confianza adquirida sobre determinados paisajes que si desaparecieran fallarían nuestros sentidos y quedaríamos desconcertados y faltos de esa sensibilidad creada que funcionara.

Debido precisamente a la devaluación del marco global que acompaña a la privacidad, normalmente la privacidad recibe inadecuada protección bajo la forma de daños que no compensan el daño reputacional o el daño individual.

Los daños infringidos a la privacidad afectan la naturaleza de la Sociedad y limitan actividades individuales que contribuirían al bienestar social.

El objetivo sería, pues la exposición y explicación de todas aquellas actividades que afectan a la privacidad. Estableciendo cómo y por qué pueden causar problemas. La respuesta al cuando y cómo encuentran regulación podrá ser contextuada tan sólo en el específico contexto en que surgen su

cuestionamiento.

Necesitamos conocer y entender los problemas con el objeto de evaluar la efectividad de su protección.

En la taxonomía que propone , se detectan cuatro actividades que pueden resultar perjudiciales en términos netamente informáticos:

- la *recopilación* de la información
- el *procesado* de la información
- la *diseminación* de la información
- y la definitiva *invasión* en la esfera íntima por estos métodos

.

Como toda taxonomía resulta un intento de categorización, y esto siempre se va a percibir de forma artificial. Debería no ser demasiado contextual o debería de poder decir muy poco más allá de cada específica situación descrita.

El robo de identidad es el resultado de un grupo mayor de problemas denominado 'inseguridad'. La inseguridad es un problema causado por el modo en que nuestra información es manejada y protegida.

La *Comisión Federal de Mercado, FTC ,* ha reconocido la inseguridad como un problema. Desde 1998, la FTC ha podido reconocer compañías que violaban las políticas de privacidad involucradas en 'actos delictivos' o que afectan el comercio. La FTC ha sobrellevado casos contra compañías que permiten de alguna manera una filtración de datos contra sus políticas de privacidad. Y, en algunos casos, sí que ha promovido acciones cuando se produjeran transacciones con datos violables como

presenta el caso Ely Lilly[13] donde mediante los servicios on-line de una determinada plataforma web denominada *Prozac* se enviaron sin consentimiento previo e-mails con información acerca de un antidepresivo a, al menos, unos 600 de pacientes.

13 "Eli Lilly Settles FTC Charges Concerning Security Breach". Release January 18, 2002. Didponible en: http://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach

En relación a este segundo uso de la información personal de un individuo, denominado *PII, Personally Identifiable Information*[14] ,las Administraciones de Australia, Korea y Canada se postulan en la denegación de dicho *Uso Secundario*.

En relación a la propuesta de Solove la *Nationwide Health Information Network*[15] , NHIN, realiza una apreciación en las relaciones extraídas precisando la delimitación de los siguientes grupos humanos:

- *primer* grupo:

  recolección de información. Supone la observación, escucha o grabación de la actividad del individuo. Desde esta misma fase debe incluirse la monitorización de aquellos controles tendentes a la monitorización de aquellos accesos autorizados y donde podría aparecer recogido el uso de la Biometría. El ciudadano puede en cualquier momento decidir continuar cediendo determinada PII a la e-Administración o no, dependiendo de la percepción que hubiera ido creando del conjunto de la dinámica. Tomando en consideración este aspecto señala *NHIN* que la 'The HIPAA Privacy Rule' intenta controlar la actividad de las organizaciones a fin de que dicha imagen negativa no se difunda. Siendo *HIPPA*, the *Health Insurance Portability and Accountability Act* publicada en 1996.

- segundo grupo:

  supone agregación, identificación, uso secundario y exclusión. En este punto y conocido en mayor magnitud en EEUU que en Europa, por ejemplo, una interacción de entidades privadas podrían interaccionar en combinar PII de una persona y consiguientemente mejorar la valoración de la situación de un paciente. La práctica exigiría de la Entidad la emisión de un *Informe de Prácticas de Privacidad* por los que explique los propósitos por los que una entidad realice el uso de esta PII sanitaria. Existe una derivación no contemplada suficientemente en ambas legislaciones en el entorno de la

14 PII, Personally identifiable information, http://en.wikipedia.org/wiki/Personally_identifiable_information

15 AMIA, Informatics Professionals. Leading the way. " Privacy Taxonomy For The Nationwide Health Information Network". Enero de 2005.
Disponible en: http://www.amia.org/sites/amia.org/files/2006-Policy-Meeting-nhin-paper.pdf

Telemedicina que pone de manifiesto que la exposición de resultados puede ser por donde podrían venir mayoritariamente esos rechazos, al contemplar proporciones de partes desnudas del cuerpo humano.

- *tercer* grupo:

la brecha que se produce en la confidencialidad, incremento sobre la accesibilidad de dicha información, apropiación, distorsión, teniendo que ver con las actividades que se producen con la difusión y trasferencia de este tipo de información

- *cuarto* grupo:

genera la invasión en asuntos privados, provocando actos invasivos que distorsionan la tranquilidad de alguien. No resulta tan claro si una exposición a un supuesto chantaje o *blackmail* hacia el paciente con intercambio económico debe ser situado en el tercer o cuarto mostrados

Las políticas que conciernen a la privacidad raramente especifican futuros actos secundarios de manera que las personas difícilmente pueden tomar decisión alguna al respecto de la información que se dispone de ellos, pues poseen poco conocimiento acerca de su potencial uso. Esta es la esencia de la necesidad de formulación de una Taxonomía.

Tradicionalmente se tiene la equivocada visión de que el conocimiento de ese potencial segundo uso del conocimiento de los datos personales de un individuo genera miedo e incertidumbre, creando un sentimiento de impotencia y vulnerabilidad. En este sentido el daño consigue un alineamiento con aquel generado por la inseguridad.

La personas crecen y cambian y revelaciones acerca de su pasado puede llegar a inhibir su habilidad para reconducir sus costumbres, de obtener una segunda oportunidad o en cualquier otra aptitud prefijada en alterar la dirección de su vida. Prácticamente en todos los estados se persigue la protección contra la falsedad que injuria una reputación.

Ahora bien, tal y como postula la Corte en India, el hombre precisa de un santuario donde se puede

sentir libre del control social. La importancia de tal santuario consiste en que el individuo puede deshacerse de su máscara, desistiendo por un momento de la proyección que hace de su imagen en el mundo que utiliza para ser aceptados por los demás. Algo que se encuentra más cercano de sus aspiraciones que de su naturaleza.

El modo en como conceptualizamos la privacidad resulta de vital importancia en la era de la información en la que nos encontramos, pues determina una forma de interpretar un complejo número de problemas que causan una importante irrupción en numerosas actividades de alto valor social.

La ley no encuentra ningún problema en la resolución de casos cuando existen, *due-to-due process*, daños físicos.

Hasta el siglo veinte las cortes se mostraban recelosas a la hora de reconocer perjuicio no físico. En parte porque las heridas imaginarias rozan la ficción, y en parte porque resulta complicado realizar una valoración económica que permita compensar un daño emocional.

Se trata de uno de los puntos que engloba la taxonomía: la recopilación de información puede interferir en las relaciones personales haciendo a la gente menos comunicativa o interfiriéndose en su asociación.

El privilegio más natural de un ser humano es el derecho a actuar por sí mismo, combinando sus expresiones con las de sus semejantes y actuando de común acuerdo con ellas. El derecho de asociación se muestra como inalienable en su naturaleza como derecho de ejercicio de la libertad personal.

Resulta realmente importante la elaboración de requerimientos funcionales para la efectiva operatividad de su estructura social.

Tenemos que ser conscientes de que debemos hacer una distinción entre lo que supone reconocer un problema y comprenderlo. De hecho, la ley puede reconocer un problema pero también puede llegar a alterar su naturaleza.

En EEUU es el individuo el que entona y eleva el discurso en relación al citado 'uso secundario',

mientras que en Europa esa revitalización se realiza a través de las *Agencias de Protección de Datos*.

La vida social y la importancia y cuidado que pone una persona concreta respecto a la publicidad o reserva de sus datos personales, hace que la línea divisoria entre intimidad y publicidad de sus datos pueda variar respecto a la regla general de protección.

Ahora bien, trascendido el problema de la intimidad-privacidad en la Taxonomía, no se debe de dejar de observar que en el marco de la Administración de la e-Sanidad , contamos con tres tipos de usuarios, que al menos, pueden desarrollar una Taxonomía y los indicamos: el ciudadano[16] como agente principal, el asistente clínico que lo puede atender y el técnico de que mantiene la estructura tecnológica.

Ahora bien, el planteamiento debe considerar otro tipo de actuaciones anteriores como puede ser el caso de P3P[17] , que en su momento exaltó el criterio de voluntad que debe emanar del ciudadano en el control del ejercicio de sus derechos al emitir información en Internet y establecer relación con una determinada Web, y por otra parte la percepción que el propio ciudadano tiene de la aceptación e integración del uso de determinados protocolos en el uso diario de la Red, sin considerar una aceptación oficial en la estructura de una Interoperabilidad consensuada.

A expensas del desarrollo de una Taxonomía Universal como propone la *Alianza Mundial para el Desarrollo del Programa de Seguridad del Paciente* y la *Organización Mundial de la Salud*, se propone fomentar una Cultura de la Seguridad entre los profesionales sanitarios, que se extendería a la ciudadanía por medio de la Formación, potenciando por otra parte tanto la Investigación o Estudio de Grado de la Salud Pública, como de la Medicina Legal.

Podemos hablar sin distorsión, de dos dimensiones de indudable trascendencia: la atención centrada en el paciente y la seguridad del paciente.

A esta percepción y actual desarrollo del Marco de Trabajo se pueden aunar tres enfoques complementarios: la acreditación basada en el cumplimiento de unos estándares[18] de la *Joint*

16 Ley 11/2007, de acceso público de los ciudadanos a los servicios públicos, (art. 3)

17 P3P, W3C Technology and Society domain. Privacy Activity Statement.. Disponible en: http://www.w3.org/Privacy/Activity.html

18 AIBAR REMON, Carlos , ARANAZ ANDRES,Jesus M. "Seguridad del Paciente y prevención de eventos adversos relacionados con la asistencia sanitaria. Unidad Didáctica 2: La Seguridad del Paciente: Una dimensión

Commission on Acreditation of Healthcare Organizations , *JCAHO* , la certificación fundamentada en la homologación y la normalización o cumplimiento de unas normas de la *International Organization for Standarization*, *ISO,* y la autoevaluación y el reconocimiento de la excelencia en el funcionamiento a partir del *Modelo Europeo de la Gestión de la Calidad*, *European Foundation for Quality Managament*, *EFQM*, como sistema de autoevaluación desarrollado a nivel europeo.

Uno de los mejores instrumentos orientados a analizar sistemáticamente los procesos de atención a la salud e instaurar planes de mejora es el denominado *Ciclo de Deming o de Shewart* de Mejora de la Calidad, conocido como P(Plan).D(Do).C(Check).A(Act), y que lo recogen esquemas como la serie de normas ISO/IEC 27001, 27002 y 27799 y que ha sido inicializado en la Introducción.
Debemos recordar que la salud no es tan solo la ausencia de enfermedad, también podemos afirmar que la 'Seguridad del Paciente' no es solamente la ausencia de riesgos relacionados con la atención recibida.

Para evitar precisamente, en el sistema de notificación de errores la principal limitación detectada conocida como sesgo de infranotificación, y en España, la *Ley de Cohesión del Sistema Nacional de Salud*, estableció recomendaciones expresas sobre los requisitos de infraestructuras para la mejora de la calidad, detallando los elementos sobre los que se debería apoyarse.

Debemos recordar que la *Historia Clínica*, *HC*, hasta ahora ha sido la prueba de que se ha venido utilizando en los Tribunales para valorar la asistencia o no de la responsabilidad profesional.

Conforme al desenvolvimiento de la Psicología del Error, los despistes, distracciones o fallos de la atención y los fallos asociados a la memoria son errores que ocurren cuando se realizan actividades cotidianas de forma rutinaria o inconsciente, el diseño de equipos, la prueba de errores, la instalación de alarmas, los check-lists, procedimientos y normativas son algunas de las estrategias que pueden contribuir a su reducción.

Recordemos los elementos que propone nuestra Ley de Cohesión del Sistema Nacional de Salud como requisitos[19] de infraestructuras a cumplir en el conjunto de las Comunidades Autónomas:

- *Normas de calidad y seguridad*, como forma de recopilar los requerimientos

esencial de la calidad asistencial". Ministerio de Sanidad . 2010. (.pag.11)
Disponible en: http://www.seguridaddelpaciente.es/formacion/tutoriales/MSC-CD1/pdfs/UNIDAD2.pdf
19 Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, (art. 59)

- *Indicadores*, que son elementos estadísticos que permitirán ajustar las diferencias de homologación entre Centros frente a riesgos

- *Guías de práctica clínica y guías de práctica asistencial*

- El *Código de buenas prácticas*

- *El registro de acontecimientos adversos*, que recogerá información sobre aquellas prácticas que hayan resultado un problema potencial de seguridad para el paciente Si nos detenemos un momento a observar la Taxonomía que se derivaría de los diferentes niveles del modelo asistencial en medicina, dígase en las modalidades tradicionales , podríamos incluir las competencias anteriormente referidas:

    - *Prevención Primaria:*

      tendente a evitar posibles causas de una enfermedad y a disminuir los factores de riesgo identificados, que en lo que nos afecta, podrían tratarse de Medidas Legislativas, Promoción de la Salud y Medioambientales

        - Fomento de la Cultura, como estamos apoyando
        - Formación de Profesionales
        - Erradicación de Procedimientos para los que existan alternativas más seguras
        - Establecimiento de Alertas Clínicas
        - Incorporación de Sistemas de identificación unívoca de paciente

    - *Prevención Secundaria:* tendente a mejorar el pronóstico existente

- Mantenimiento de Sistemas de Vigilancia y notificación de incidentes
- Optimización de los Sistemas de Comunicación a efectos de resolver con la mayor premura situaciones de riesgo

- *Prevención Terciaria:* tendente a retardar los efectos de la enfermedad
  - Modelación de las actitudes de Comités de Conciliación de las indemnizaciones a las que hubiere lugar

Podremos concluir que utilizando la misma semántica que se utiliza en la Gestión de Riesgos Sanitarios y dependiendo de la metodología utilizada podemos clasificar las medidas como:

- *Centinelas*, Haciendo referencia a sucesos infrecuentes y que requieren de un tratamiento puntual
- *Índices*, Que manejan la frecuencia de aparición y requieren de monitorización, incluso comparativas con otros Centros

En este punto podemos esbozar ambos lados de la Taxonomía que proponemos, por un lado la del ciudadano como usuario de la e-Administración y, por otro, el del técnico de la e-Administración que podría situarse en muy diferentes circunstancias y encontrarse ejecutando su profesión en diversas categorías, eso sí respetando siempre el siguiente esquema de interacción en sus diferentes niveles de percepción:

ALGUNAS TAXONOMIAS QUE MANEJA EL CIUDADANO	
Percepción del modo en cómo se recopila su PII	se presenta voluntariamente a la consulta y se recopila su información
Intervención sucesiva en la verificación de sus datos en la HC	puede validar actualmente la veracidad de sus datos en la HC en el mismo momento de la anamnesis, por intervención posterior, por propia voluntad de acceso a la plataforma de la e-Administración o por petición del ejercicio de sus derechos ARCO
Voluntariedad de participación en programas científicos o de videovigilancia	e.g. es solicitado por constar en la BBDD en un estudio de videovigilancia clínica
Ejercicio de Derechos ARCO y Medicina Legal	se le notifica que se ha producido un incidente con e- HC y hay o no consecuencias para su salud
Percepción en Feedback del tratamiento de datos que le llega de la Sociedad a la que pertenece	e.g. a través de noticias se hace consciente de que su información puede ser accesible por otras personas que las meramente de asistencia, por personal no autorizado sanitario, y se puede hacer un uso indebido de ellos
Participación en la Seguridad del Paciente	se le plantean diversas formas de actuación en la Defensa de sus Derechos ARCO, de los que fue Formado y ha de elegir el modo de interlocución por el Servicio que le compete, independientemente de producirse un incidente con su HC
Uso de la HC en el ejercicio de sus Derechos	no existe negligencia de ningún dato en su HC, pero se ha producido una negligencia médica: la HC como prueba judicial
Responsabilidad Civil	procedimiento por fallecimiento de un ciudadano
Manejo de otros derechos que el de su Estado y Jurisprudencia	e.g. se decide optar por la medicina privada y ha de ser informado de las diferencias de tratamiento respecto de su HC en la e-Sanidad, aunque el ejercicio del derecho le protege idénticamente

Tabla 1. Taxonomía del Paciente

Tabla 2. Taxonomía del Técnico Informático e-Sanidad

ALGUNAS TAXONOMIAS QUE MANEJA EL TECNICO DE LA E-ADMINISTRACION EN SANIDAD	
Responsabilidad de Impermutabilidad de Información	debe responder de la veracidad de los datos que maneja y que no experimentan modificaciones
Colaboración Auditada	debe poder proporcionar y filtrar en el documento curricular propuesto aquellos datos de los que con autorización formulada ya aceptada se ejerciera la defensa de los Derechos ARCO
Conocimiento de la Legislación a la que asiste	debe responder a la dinámica de las Auditorías Internas y Externas en materia de protección de datos
Responsabilidad de Incidencia	como responsable de un incidente debe , conforme al procedimiento establecido en la Política de sus Empresa, comunicarlo, y tratarlo minimizando su suceso
Aportación de su experiencia en la Optimización de la e-Administración	debe cooperar en el tratamiento de otros incidentes que se produjeran y en los que pudiera aportar conocimiento de causa y efecto
Monitorización de Incidencias	como responsable de una salvaguarda se exige vigilancia constante en su cumplimiento, debiendo reportar oportunamente su fallo
Análisis y Supervisión de la Medida de Control de la que es responsable	debe corroborar que la salvaguarda cumple escrupulosamente la normativa legal y el marco de interoperabilidad en el que desempeñe su trabajo
Manejo de Alertas de Incidentes	Capacidad de Respuesta Informada de su actuación conjunta

No debemos concluir este capítulo sin la mención que anteriores pensadores, y se pueden citar a muchos, ya realizaron en el pasado invocando la creación de la Lógica Simbólica, en el Mundo de la Filosofía, y el posterior desarrollo que adquirió en la Lógica Posicional si tratamos de virtualizar al máximo el lenguaje que representan los Escenarios formales de un determinado Entorno de Datos y su posterior tratamiento por el Mundo de las Computadoras, persiguiendo la racionalización y extracción de mayor información , si cabe, en la resolución de un problema social.

Del mismo modo que en el Mundo de la Física cada pequeña partícula onda-corpuscular encierra el misterio de modificar su comportamiento cada vez que se la observa, cada dato y el dato médico , más especialmente, encierra el misterio de la definición escenarios donde no sólo se crearon sino y en el caso que nos ocupa el entorno donde se le trata. Viéndonos obligados a señalar el Alto Cuidado que se le debe de poner a su manejo y estudio.

El propio seguimiento del Desarrollo de la Jurisprudencia en los países que configuran el Marco de aplicación nos permite concluir que aún no completadas algunas legislaciones se pueden extraer observaciones estadísticas que nos permitirían ir extrayendo aquellas líneas de investigación y bajo el punto de vista de una mente puramente técnica permitiera manejar a los legisladores nuevos puntos de seguridad sobre los que emitir el beneficio de permitir legalmente tal doctrina.

De la aplicabilidad de una Lógica Negativa , surge la definición de una Taxonomía Negativa expresada del siguiente modo

<<Como consecuencia de la corrupción de identidades surge una Sugestión Social de la que las personas extraen falsas conclusiones, pudiendo tomar cada nueva identidad vida por diferentes canales>>

La propia personalidad de la Taxonomía debiera poder hacer plantearnos en que medida puede ser esta consideración u análogas evitadas.

De este modo podemos apuntar la razonable expectación que despiertan los métodos utilizados por las Cortes Americanas en la identificación de los intereses protegidos por el derecho a la privacidad, balanceando estos criterios frente al denominado bien social y en que medida pudiera ser tratado si resultara devaluado este principio fundamental.

Y, aunque expresáramos con corrección cada uno de los Focos de Taxonomías planteadas para cada Figura reconocida en el Escenario de la e-Sanidad, siempre que una definición de Taxonomía Negativa pudiera ser expresada el Derecho Informático debiera poder reconocer perjuicio y en tal caso aplicar la Ley.

Actualmente están surgiendo nuevos escenarios de extrapolación de taxonomías relacionadas en nuestro caso con la Telemedicina por cuanto contempla la Domótica y lo que se ha venido en llamar los *smart devices*[20]. El Escenario completo ha quedado recogido en la denominada *Internet de las Cosas*[21] y despierta una clara alarma en lo que respecta a la recopilación del consentimiento del usuario por considerarse prácticamente inexistente o deficitaria. Es el primer documento oficial que comienza a reconocer públicamente la inquietud que debería motivar al segundo grupo de nuestra Taxonomía, Tabla II, al postular que los usuarios deberían ejercer completo control de sus datos personales a lo largo del ciclo de vida del producto (device), y cuando las organizaciones que se encuentran detrás del mismo depositen su fe en el ejercicio del consentimiento de recabación de datos personales , éste debiera ser claramente informado y proporcionado por el usuario de forma libre. Así mismo, y con el objetivo de proporcionar sus recomendaciones, éstas las consideran especialmente dirigidas a los fabricadores, desarrolladores de la aplicación , plataformas sociales, y cuerpos de estandarización, entre otros, considerando las terceras partes idénticamente a fin de que implementen la Privacidad y Protección de Datos sobre sus productos y servicios.

Aun si el dato clínico "se escapara" por la red, el ciudadano aun tiene la posibilidad de reaccionar como lo inician las Autoridades Europeas de Protección de Datos, Article 29 Working Party, que reunidos en su pleno nº 97, abogan por ir más allá del *Derecho al Olvido*[22] y facilitar un *Right to be -deListed,* porque lo que no se puede percibir tampoco se puede controlar.

No es de difícil de prever que algún día se conseguirá hablar científicamente de la *Salud de las Cosas*.

20 ARTICLE 29 DATA PROTECTION WORKING PARTY WP 202

21 ARTICLE 29 DATA PROTECTION WORKING PARTY WP 223

22 *Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea* Disponible en: https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es

CAPITULO II: ESCENARIOS EN LA E-SANIDAD

Abstract :

Legal recopilation of the principle actors involved in the responsability of managing clinical data all over the world notwithstanding its stage

Claves :

derecho sanitario, derecho informático, jurimetría, derechos arco, requisito informado, código tipo, consentimiento o autodeterminación, habeas data, dato sensible, persona jurídica, documento de seguridad, documento público, principio de transparencia, agente, uso secundario, código de buenas prácticas, , documento de instrucciones previas, cesión de datos, tarjeta sanitaria electrónica, vigilancia médica, farmacovigilancia, trial subject, controller o controlador, procesador o processor, promotor o esponsor, monitor, organización de investigación por contrato, seguridad del paciente, esquema nacional de seguridad, autoridad de certificación, autoridad de registro, fichero, llevanza del documento de seguridad, acontecimiento adverso, nivel adecuado de protección, tercer país o third country, código de conducta, building corporate rules, fraude informático, the privacy statement, resolución de madrid, alerta, the comitology decision, privacy by design, pets, pias, patient summary, consentimiento informado, disociación, riesgo, secreto médico

Si nos refiriéramos a una posible rama del Derecho que protegiera los derechos del ciudadano en el ámbito sanitario no sólo europeo, del que formamos parte, sino otro supranacional, hablaríamos del 'Derecho Sanitario' como mayoritariamente se ha estado citando en los 'Congresos Nacionales de Derecho Sanitario' en España.

Más, centrándonos en la imagen del ciudadano que desde su nacimiento sabe que los datos referidos

a su Salud se recopilan en Servidores pertenecientes a la Administración Estatal y que están hasta el día de su muerte tratados por medios informáticos, sujetos a Auditorías reguladas por normas internacionales debemos referirnos al Concepto de 'Derecho Informático'.

Si bien es cierto que existen autores españoles que realizan un prolífico y lógico seguimiento del concepto de *autodeterminación informática* alemán defendiendo a continuación el desarrollado concepto de la *libertad informática* español como es el caso de Antonio E. Pérez Luño[23], no estamos de acuerdo al afirmar que deba dejarse tan abierta la protección de la intimidad al resto de los derechos fundamentales, pues como se expondrá más adelante se deja lugar a una falta de protección no ya nacional sino a la generación de un déficit a la hora de generar una marco supranacional que puede ver frenado el propio Estado Europeo.

Se considera que esta deficiencia en la defensa del derecho a la dignidad e intimidad humana frena idénticamente la consolidación del denominado 'Derecho Informático' al no estarse reconociendo el amplio ámbito en el que se despliega y debido precisamente a su carácter tan transversal como en este trabajo tratamos de expresar.

Recordemos que para definir una rama del Derecho, el nuevo derecho debe contemplar las nuevas relaciones reguladas normativamente o bien reconocerlas jurisprudencialmente, poder aplicar sus principios jurídicos y poder introducir nuevos valores. De esta forma nos recuerda Eugenio Ull Pont

en su volumen <<Derecho Público de la Informática>> la referida autonomía debe poder contemplar el conjunto de sus aspectos: autonomía legislativa, autonomía doctrinal, autonomía didáctica y autonomía científica. Este autor junto a Miguel Ángel Dávara desde su <<Manual de Derecho Informático>> recopilan este término[24].

.

En este apartado de la Tesis dedicado al análisis del *Derecho Informático* involucrado desde la perspectiva del tratamiento de un dato clínico mientras este pueda existir, se tocan los siguientes

23 Revista Aldaba nº 32 de la Universidad de la UNED de Melilla del 2004

24 DAVARA RODRIGUEZ, Miguel Angel. Manual de Derecho Informatico. Editorial Aranzadi. Introduccion. 2002
ULL PONT, Eugenio Derecho Público de la Informática.Protección de Datos de Caracter Personal. UNED Ediciones. 2003. Cap. 3, (pag. 25)
Véase, vid. CANALES GIL, Alvaro y PIÑAR MAÑAS, Jose Luis. "Legislación de Protección de Datos"(adaptada a la Ley 2/2011)". IUSTEL. 2011

apartados desde aquellas perspectivas que se ha considerado más oportuno expresar conforme a la sección desde la que hubiera sido invocado:

- Derecho a la Intimidad
- Protección de Bases de Datos
- Derecho de la Propiedad Intelectual e Industrial en el Comercio Electrónico
- Derecho de las Telecomunicaciones
- Protección Programas de Ordenador
- Protección de Datos Biométricos
- Ley de Sanidad e Historia Clínica. Farmacovigilancia
- Ley de E-Administración

No se habrá de olvidar que nos está interesando considerar mayormente la perspectiva del paciente y la del técnico informático involucrados sin pretender en ningún momento que estos se perturben como era el objeto de la Taxonomía.

1.-Semántica en el Derecho Informático

Desde el inicio en la legislación española el concepto de autodeterminación del ejercicio de los derechos de acceso, y posteriormente reconocidos como *Derechos ARCO* encontró precisamente en

el campo de la *e-Sanidad* la integración de la tradicional exposición *Libertad informativa vs. Autodeterminación*. Con lo cual, una tradicional definición informática de una especificación de Escenario asume desde la legitimidad su reconocimiento de existencia de ser como asume la *Comisión del Mercado de las Telecomunicaciones, CMT*, permitiendo de este modo entender como ha recogido el *Esquema Nacional de Seguridad* en la denominada Sociedad de la Información una lógica de trayectoria de Sistemas Informáticos más ampliamente analizados como los Supervisados desde el *Consejo de la UE* y donde aparecen categorizados al máximo nivel unidades de control como el *Documento de Seguridad* e *Incidencia* y recordando siempre que es el ciudadano en su libre percepción de la intimidad el responsable auténtico del tratamiento de sus datos clínicos, no debiendo olvidar el Estado el amparo suficiente que debe proporcionar para cubrir dicha Defensa

1.1.- Requisito Informado

Aun cuando la especificación de requisitos de un Sistema Informático realiza una invocación a la correspondiente del software que permite el manejo de los programas que componen la Operativa de la Administración Electrónica y las Bases de Datos, podemos, de acuerdo con las directrices que se citan desde las normas estandarizadas orientadas a la presentación de requisitos, indicar, por una parte, y recordar que las características[25] que debe regir una especificación de requisitos en un sistema deben ser:

- correctas
- no ambiguas
- completas
- consistentes
- expuestas en orden de importancia teniendo consideraciones hacia la seguridad de la operativa
- verificables
- modificables
- traceables

25 Engineering Standards Committee of the IEEE Computer Society, IEEE Recommended Practice for Software Requirements . IEEE Std 830-1998. Software , (pag.10.)

Asimismo, la norma[26] para la implementación de especificaciones de requerimientos de un sistema nos recuerda que un requerimiento:

- se constituye como una condición o capacidad necesaria por un usuario para resolver un problema o bien alcanzar un objetivo

- se constituye como una condición o capacidad que debe ser perseguida o funcionalmente incluida por un sistema o por uno de sus componentes a objeto de satisfacer un estándar u otro documento oficial

En ningún caso, un requerimiento debe solaparse con las especificaciones de otro. Además, desde un punto de vista genérico se deberían incluir todas las especificaciones que pueden ser definidas por un consumidor potencial a fin de obtener ese grado de *completo* que se le otorga por definición. De modo que queda perfectamente claro que es necesaria la indicación de sus límites.

Por otra parte, el concepto *Requisitos Informados*[27] que se recoge y defiende desde la *Comisión de las Telecomunicaciones*, CMT, nos recuerda la necesidad de recopilar en fehaciente labor aquellas operativas , distinguidas en este caso observadas por la Legislación a fin de no incurrir en dobles propósitos definitorios y poder responder con mayor exactitud al Diseño del Sistema Informático.

Recordemos que la base de la propia definición del concepto indicado, el del requisito informado , por parte de los operadores de Telecomunicaciones a dicha Comisión exige un alto conocimiento técnico, económico y jurídico en el momento de su exposición. La actualización está sometida a dos años de actualización. La propia Audiencia Nacional recuerda que se deben observar dos criterios a la hora de determinar la proporcionalidad del requerimiento solicitado: objetivo y subjetivo.

26 Software Engineering Standars Committee of the IEEE Computer Society, IEEE Guide for Developing Systems Requirements Specifications. IEEE Std 123, (pag. 9)

27 Coleccion: Jurisprudencia Comentada. Jurisprudencia de Telecomunicaciones. Editorial Aranzadi. Cap IV. II. Naturaleza Jurídica de los Requerimientos de Información". 2008 (pag. 250)

En el caso concreto de la Historia Clínica[28] existe la posibilidad de la existencia de la historia en forma no digital y de que las diferentes Comunidades Autónomas se encuentren en fases varias de implantaciones y pruebas de su Sistema de Información en la plataforma de la e-Sanidad , teniendo que garantizar, en cualquier caso, aquellas situaciones en las que el ciudadano pueda interaccionar con su Historia Clínica sin recurrir a dicha plataforma en el contexto de los centros sanitarios.

Por otra parte, y ya en el Contexto de la e-Sanidad, es el *Sistema Nacional de Sanidad o SNS*[29] el que delimita el procedimiento, incluido la interfaz por medio de la cual tiene acceso al mismo.

Ahora bien, el dato de la historia clínica por el que el ciudadano puede inferir especial interés en el ejercicio de sus derechos puede tener orígenes bien distintos: el de una *anamnesis* básica de su médico de atención primaria bien se trate la entidad a la que acuda de pública o privada, o el de un dato correspondiente a la Atención Especializada. Además, hemos de integrar los ámbitos de la Farmacovigilancia, el de los Estudios Clínicos y la Protección de Riesgos laborales que típicamente llevan asociados la relación con una Mutua.

Se puede aseverar sin género de duda, que resulta de vital importancia el poder tener acceso a unos no suficientes sino decentes y adecuados *Requerimientos de la Unidad del Sistema Informático Médico* que se pretende afrontar. La importancia de esta observación está recogida, no olvidemos, en la Doctrina de la Jurisprudencia desarrollada en torno a la Comisión del Mercado de las Telecomunicaciones o CMT, para la que una no veraz información puede reconocer el perjuicio causado sobre un ciudadano, y en consecuencia resultar penalizado el origen de la mala información.

La correcta expresión de los requerimientos citados que han de recoger, por otra parte, las Operativas del Personal de Recursos Humanos que la Soportan, puede exigir en tal medida un Buen Diseño de su Arquitectura.

La experiencia futura llegará a demostrar cómo una incorrecta definición de esta arquitectura puede

28 Ley L 41/2002, , de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, (art .3)

29 Ley L 16/2003, de cohesión y calidad del Sistema Nacional de Salud, SNS, (art.1)

ayudar en colaborar en extender una confusión que mal manejadas puede incurrir en grave perjuicio para el ciudadano-paciente, y por extensión, al colectivo de la población.

En ocasiones, los *Códigos Tipos*[30] pueden ayudar a corregir esta tendencia, viéndose obligados a reforzar la dinámica del Personal Corporativo por no verse reflejada en la Aplicación Informática que manipulan.

Por su parte el Sistema de Mutuas y Seguros Médicos permite añadir un punto de seguridad que el Empresario decida en qué grado aplicar ante la inseguridad que pude ofrecerle un trabajador, y que bien tratada puede reforzar la tranquilidad del asegurado.

1.2.- Autodeterminación por Consentimiento

Con especial cuidado debemos referirnos a la multiplicidad de significados que algunos términos pueden encontrar como es el caso de la palabra autodeterminación en el contexto en el que nos estamos expresando. Por una parte contamos con la explicación que hizo en su momento la Exposición de motivos de la LORTAD[31] refiriéndose a:

> •"Las garantías de la persona son los nutrientes nucleares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de *autodeterminación*, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático"

> •Por su parte, el principio de *consentimiento*, o de autodeterminación, otorga

30 Agencia de Protección de Datos. Elaboración de Códigos Tipo. Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/elaboracion_codigos_tipo/index-ides-idphp.php . También LOPD, Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, (art.32)

31 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, derogada e invocada desde la LOPD

a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita; sus contornos, por otro lado, se refuerzan singularmente en los denominados *datos sensibles*, como pueden ser, de una parte, la ideología o creencias religiosas, cuya privacidad está expresamente garantizada por la Constitución en su art. 16.2 y, de otra parte, la raza, la salud y la vida sexual

Queda expresado el modo en cómo la inicial legislación en materia de protección de datos y recogida la LORTAD tras su derogación en la actual Ley de Protección de Datos, LOPD, y en cómo entendía el derecho a la autodeterminación informativa , según sentencia del Tribunal Constitucional Alemán, STFCA de 15 de Diciembre de 1983*:*

- "la facultad del individuo, derivada de la idea de *autodeterminación* de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida. De este modo, un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo las condiciones de la elaboración automática de datos, ninguno *sin interés.* A consecuencia de lo que antecede, el grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad

- Hace falta, más bien, conocer la relación de utilización de un dato para poder determinar sus implicaciones para el derecho de la personalidad. Sólo cuando reine la claridad sobre la finalidad con la cual se reclaman los datos y qué posibilidades de interconexión y de utilización existen se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la *autodeterminación informativa*

Precisando en todo caso de una disertación la separación entre este concepto y lo que se vino en

llamar *libertad informativa* como más adelante se comentará.

El término anglosajón referido como *privacidad* extrae de lo que no se considera *public* como *private* o dicho de otro modo resaltando aquellos ámbitos de la vida en los que los demás no tienen derecho a inmiscuirse, a lo íntimo. Así se han ido mezclando los conceptos de intimidad y privacidad de tal suerte que por privacidad se entiende no sólo a la facultad que una persona tiene para poder excluir a cualquier persona o ente del conocimiento de su vida personal sino que, además, se incluye la posibilidad de controlar qué aspectos de esta vida personal puedan ser conocidos por otras personas.

La legislación estadounidense viene a desarrollar lo que se denomina un *right to privacy*[32] , expresando el derecho a la intimidad entendido como separación y defensa del individuo frente a la sociedad a través de su *Privacy Act* de 1974 y que incorporó las recomendaciones recogidas un año antes por el Departamento de Salud, Educación y Bienestar de un estudio de "Registros, computadoras y derechos de los ciudadanos" en el que se proponía un código *federal fair information practices* encaminado a salvaguardar la intimidad personal aconsejando la creación de registros , observando el mantenimiento de copias , regulando cada consentimiento informado y el consiguiente ejercicio de los derechos de acceso.

En la legislación española el término que se maneja es el de intimidad y concretamente y vinculadas al principio de derecho de libertad informática contamos con , al menos, las siguientes expresiones:

- *STC 110/1984:* "La discusión reside en la connotación que se tiene del concepto de la intimidad. Así, por ejemplo, destaca que su fundamento parte de la idea del respeto a la vida privada personal y familiar que debe quedar excluida del conocimiento ajeno y de las intromisiones de las demás, salvo consentimiento del interesado"

- *STC 11/1998:* "La garantía de la *intimidad*, latu sensu, adopta hoy un

32 The Free Dictionary, Thesaurus. Disponible en: http://www.thefreedictionary.com/right+to+privacy

entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a dicha persona. La llamada *libertad informática* es así derecho a controlar el uso de los mismos datos insertos en un programa informático ,habeas data, y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

- art. 18.4 CE: "habrá que limitar el uso de la informática para garantizar el honor y la intimidad personal y el pleno ejercicio de sus derechos"

Observando el devenir legislativo, el art. 12 de la *Carta Internacional de los Derechos Humanos* de 1948 establece que nadie será objeto de injerencias arbitrarias en su vida privada, su domicilio o su correspondencia ni de ataques a su honor y su reputación y que toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques.

Como fuerza moral no conlleva vinculación jurídica expresa, excepto para los Estados que la han incluido en su propia Constitución.

Veinte años después, en 1968 el Convenio de Europa surge como consecuencia de la emisión de una serie de resoluciones:

- nº 22/1973, respecto a los datos de titularidad *privada*
- nº 29/1974, de titularidad *pública*

, provocadas a su vez por La Recomendación 509 en 1968 de la Asamblea del Consejo de Europa dirigida al Comité de Ministros con el propósito de que la Convención Europea para la Protección de los Derechos Humanos buscara la forma de proteger los derechos de la persona.

No pudiendo entrar en contradicción la interpretación de las normas constitucionales con estos principios:

- *art. 8.1*: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"

- *art. 8.2*: "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás"

1.3.- Ejercicio de los Derechos Arco

En 1985 se habla ya del primer *Sistema de información inter-países europeo* permitiendo la emisión de visados y revisión de documentación transfronteriza con soporte a fines policiales. El denominado *SIS* que ya se presenta en su fase II, nos sugiere en el *art. 118* de su estatuto una serie de observaciones que ratificado el acuerdo e incorporado a la legislación nacional quedó integrado tras la derogación de la LORTAD en la LOPD y cuyas indicaciones son factiblemente auditables desde los nuevos desarrollos en la legislación competente a la *Sociedad de la Información* por la Ley que regula el Esquema Nacional de Seguridad o L 11/2007 y sus desarrollos a posteriori en los RD 03/2010 y RD 04/2010 [33]:

- control de entrada en las instalaciones
- control de los soportes de datos
- control de la introducción
- control de utilización
- control de acceso

33 RD 03/2010, (art.3, art. 34, Anexo 2.4)

- control de la transmisión
- control de trasporte

La responsabilidad civil, *art. 1902* del Código Civil, se fundamentaba en la existencia de daño efectivo y comprobable como presupuesto de cualquier reclamación de perjuicios causados: si se comprobaba el daño, se presumía que el agresor era el culpable. Su posterior formulación legal en 1982 en la *Ley Orgánica de Protección Civil de Derecho al Honor, a la Intimidad Personal y familiar y a la propia Imagen* refleja en su *art. 9.*3 la existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima, refiriéndose al daño moral.

La inicial y posterior sustituida Ley de Protección de Datos de 1992 conocida como LORTAD formula el denominado concepto de *dato sensible* que no tendría que ser declarado, *art. 16.2*, salvo por consentimiento de la persona y por escrito a excepción de lo establecido en el *art. 20.3* según la cual las Fuerzas y Cuerpos de Seguridad podrán recoger esta clase de información sin su consentimiento, excediendo en principio a lo propuesto en el texto europeo lo que motivó recursos de inconstitucionalidad por parte del Defensor del Pueblo.

En caso de datos no especialmente protegidos se le otorga al afectado un plan de treinta días para manifestarse su tratamiento[34].

Las disposiciones de Schengen quedan salvaguardadas por el Real Decreto 1332/1994 conforme consta en el art. 4.1.b donde así mismo se indican las pautas para el tratamiento de datos en ficheros de carácter estadístico. Igualmente queda reglamentada la obligación de notificar la creación de un fichero, en los supuestos de titularidad pública y en los de titularidad privada.

El texto precedente de la actual Ley en materia de Protección de Datos, la Directiva D 95/46/CE da paso a otra, la D 97/66/CEE[35] que quedarán incorporadas a Derecho legal en 1999 en la referida

34 L 15/1995, RD 39/1997

35 D 97/66/CE de la Unión Europea sobre el tratamiento de los datos personales y protección de la intimidad en el sector de las telecomunicaciones

LOPD.

En la categorización de datos la LOPD inicia la definición de dato sensible haciéndose coincidir con la proporcionada por la Directiva D 95/46/CEE como cualquier información concerniente a personas físicas identificadas o identificables, siguiendo con una categorización de especialmente protegidos en nuestro ámbito a aquellos referidos a la salud y los manejados por la Administración.

En el ámbito europeo el *Convenio 108* se permite en virtud de su *art. 3.2 b* que los Estados, con ocasión de la firma, del depósito, del instrumento de ratificación, aceptación, aprobación o adhesión o con posterioridad, pudieran manifestar que aplicarán

"también el presente convenio a informaciones relativas a agrupaciones, asociaciones, fundamentos, sociedades, corporaciones y cualquier otro organismo, formado directa o indirectamente por personas físicas, tuvieren o no personalidad jurídica"

Algunos países incluyeron rápidamente esta clausula respecto a la protección de datos de las "personas jurídicas" , art. 3.2 de la ley austriaco, el art. 2 de la ley luxemburguesa, sin embargo, la mayoría no la contemplaron tan inmediatamente: Alemania, Australia, Reino Unido, etc.

Básicamente,

> *"Se observa durante el debate doctrinal de todos los países que cuando se habla de personas jurídicas a las cuales se les puede extender el campo de aplicación de la protección de datos se piensa fundamentalmente en las* empresas*. Por ello la segunda crítica se centra en que tales personas jurídicas no necesitan la protección de un derecho humano (o fundamental) sino la de otras ramas del derecho (derecho civil y penal, derecho mercantil, derecho de patentes, de marcas, etc). Opiniones autorizadas como la de Spiros Simitis o Manuel Heredero convergen en que la protección que se debe otorgar a las personas físicas y a las personas jurídicas ha de ser diferente. Así mientras en las personas físicas lo que se protege es la privacy, en las personas jurídicas lo que se protege es la sunshine, es decir, la publicidad. En el caso de las empresas no resulta, siempre y en todo caso, interesante la transparencia. El derecho de acceso podría ser*

enormemente negativo para la libre competencia, la protección del secreto de los negocios y de la estrategia industrial. Ahora bien, como ha destacado Hernando Collazos, si la tutela que merecen estas personas jurídicas no es la de un derecho humano será necesario desarrollar una doctrina del secreto y de la divulgación de datos referentes a la actividad comercial[36]"

Debiendo observar claramente cuáles son los casos en cada momento de observancia de definición de un fichero que como reitera la LOPD quedan excluidos, de la necesidad de integrarse en un fichero automatizado para los siguientes supuestos como :

- aquellos que posean las personas físicas en el ejercicio de actividades exclusivamente personales o domésticas , por ejemplo, los de una agenda electrónica o PDA.

- los sometidos a la normativa sobre protección de materias clasificadas, por ejemplo, los secretos del CESID

- los establecidos para la investigación del terrorismo, aunque el Ministerio del Interior debe comunicar su existencia y su finalidad a la Agencia de Protección de Datos

- los regulados por la legislación de régimen electoral , sobre todo, el censo

36 GONZALEZ MURUA, Ana Rosa. "El Derecho a la Intimidad, el Derecho a la Autodeterminación Informativa y la L.O. 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos Personales".Universidad del País Vasco.Working Paper nº 96. Barcelona 1994. Disponible en: http://ddd.uab.cat/pub/worpap/1994/hdl_2072_1371/ICPS96.pdf.

- los que se utilicen para *fines estadísticos*[37]

- los que almacenen datos en informes personales de calificación que se encuentren amparados por la legislación del Régimen del personal de las Fuerzas Armadas, etc.

En todo caso, el ciudadano tiene el derecho a estar informado acerca de la existencia, finalidad y de los destinatarios de la información, estando legislativamente prohibido otorgarlos por la fuerza.

Sin embargo, conforme a su art. 11.2.d y f no se precisará un consentimiento cuando la comunicación tuviera como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, o bien por motivos de urgencia en una actuación sanitaria.

La existencia de un fichero implica su archivo y conocimiento auditado ante el Registro de la Agencia de Protección de Datos a fin de encontrarse hábil en un posible ejercicio de la defensa de los *Derechos ARCO*[38] .Y Considerando que el ejercicio del derecho de acceso a los documentos públicos ayuda al público a formar una opinión sobre el estado de la sociedad y sobre las actividades públicas entendiéndose por documento publico significa toda la información registrada (archivada) de cualquier forma, elaborada o recibida, y en posesión de las autoridades públicas, en la solicitud de acceso a los documentos públicos, un solicitante no podrá ser obligado a dar sus razones por tener acceso a un documento oficial[39].

De registro e idénticamente que en el caso anterior han de ser inscritos y depositados los *Códigos Deontológicos* o de buena práctica empresarial.

37 L 32/2003 (art. 9.b), 2006/24/CE (art.10), L 41/2002 (art.23)

38 LOPD (art. 5.1.d), L 41/2002 (art.18), L 56/2007 (art. 1.d)

39 Convenio del Consejo de Europa sobre el acceso a los Documentos Publicos, (art. 4)

Va a ser el *real decreto RD 994/1999* de Medidas de Seguridad el que inicia el trabajo de un *Documento de Seguridad*[40] siempre y cuando se manejen datos de carácter personal donde habrán de estar bien definidas y documentadas las funciones y obligaciones de cada persona, la estructura de los ficheros y descripción de los sistemas de información; procedimiento de notificación, gestión y respuesta ante incidencias y de realización de copias de respaldo y de recuperación de datos.

Para la notificación y gestión correspondiente, se contará con el haber de un *Registro de Incidencia*[41] .Los tres niveles de seguridad que establece bajo, medio y alto serán posteriormente analizados y desarrollados en el *RD 03/2010* conforme a la métrica que ha venido siendo observada en la Administración.

El concepto de Privacidad aparece explícito nuevamente en la identidad de la *Directiva 2002/58* integrada *ya* en la D 2006/24/CE *o* al que se le añade el concepto de *Comunicaciones Electrónicas* ampliando el campo de operación de este concepto en el contexto de las Telecomunicaciones actuales. Es en este caso cuando el campo se amplía a las *personas jurídica*s que había sido obviado en la D 95/46/CEE.

Se produce en este nivel la aparición de los

- *servicios de valor añadido* como todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación

- *datos de localización* como cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas

40 RD 994/1999 (art.8), sustituido por el art. 81, 82, 84, 86 más Cap. II y consideraciones de aplicaciones por Niveles de Seguridad en Cap. III del RD 1720/2007

41 RD 03/2010 (Anexo 2.4)

disponible para el público.

Previo a explicar el camino que siguió el concepto de la libertad informática en nuestro país, exponemos brevemente la jurisprudencia necesaria que vino a desembocar en la argumentación que se desarrollará con posterioridad a este apartado.

- 1984, Caso Malone: Resulta interesante observar la denegación inicial de la no contemplación de unos datos frente al desarrollo de un Derecho Comparado en otras legislaciones *Tribunal Europeo de Derechos del Hombre:* reconoce expresamente la posibilidad de que el art. 8 de la Convención pueda resultar violado por el empleo de un artículo técnico, que permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma

- *STC 254/1993:* Continuación del caso anterior, se acuña por primera vez el concepto de Libertad Informativa frente al doctrinal germano y antecesor de "Autodeterminación Informativa". Incorporando alusiones directas al habeas data y habeas corpus pese a las pocas veces que se ha pronunciado el TC sobre la relación entre la informática y la intimidad, este caso supone un hito en el derecho positivo, al menos por las siguientes consideraciones: tratarse del primer caso nacional en el que se cuestionó la intimidad frente a la informática, sentencia anterior comentada STC 114/1984; pronunciación de la libertad informativa no totalmente contrapuesta al concepto, previo a su publicación, defendido por la doctrina como autodeterminación informática "Es suficiente con constatar que, al negarse a comunicarle la existencia e identificación de los ficheros automatizados que mantiene con datos de carácter personal, así como los datos que le conciernen a él personalmente, la Administración demandada en este proceso vulneró el contenido esencial del derecho a la intimidad del actor, al despojarlo de su necesaria protección. Como señala el Ministerio Fiscal la garantía de la intimidad adopta hoy un

contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada 'libertad informática', es así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)"

- STC 202/1999: Primer caso a nivel nacional donde se juzgaban unos datos personales en el marco de una aplicación informática. Contando tan sólo con el desarrollo de la LORTAD, se esgrime la Libertad Informativa de la sentencia anterior.

Se trataba de una base de datos denominada de "absentismo con baja médica" Viniendo a confirmar la sentencia el debate procesal de los siguientes hechos, el archivo no estaba dado de alta en la Agencia de Protección de Datos, no existiendo, por tanto responsable oficial del mismo tenían acceso al mismo los cuatro médicos contratados por la entidad crediticia como médicos de empresa y, por otro, un empleado del Banco adscrito al área de personal, que no ostentaba la condición de facultativo y que facilitaba la clave de acceso al sistema. Se atentaba contra el art. 4 de la LORTAD. El acceso debía limitarse al propio interesado, invocándose al respecto el art. 22.4 de la *Ley 31/ 1995, de 8 de noviembre, de Prevención de Riesgos Laborales*.

La garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada“ libertad informática” es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención.

- STC 292/2000: Ya desarrollada la LOPD se continúa la presentación y resolución del recurso de inconstitucionalidad por parte del Defensor del Pueblo, esgrimiendo la ya consolidada Libertad Informativa de STC 254/1993, aun cuando de vez en cuando aparece todavía en el texto alusión al doctrinal "autodeterminación informativa".

  Se convierte en un nexo entre la referencia directa a la libertad informática y a la definición de *habeas data*,

  "Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática, lo que se ha dado en llamar libertad "

  "La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998)"

  Se trataba de la presentación de un recurso de inconstitucionalidad contra los incisos de los arts. 21.1 (Comunicación de Datos entre Administraciones Públicas), y arts. 24.1 y 2 (Otras excepciones a los derechos de los afectados)

La argumentación utilizada resulta clara, la LOPD no había fijado como le impone la Constitución los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas sino

que se había limitado a identificar la norma que puede hacerlo en su lugar que, aunque puede ser reglamentaria y de rango superior, con mayor razón para el caso de que la modificación lo sea por una norma de similar rango a la que crea el fichero (y esta basta que sea una disposición general, que no una Ley, publicada en un Boletín o Diario Oficial) la que pueda autorizar esa cesión inconsentida de datos personales, contrario a la Constitución.

Según el *art. 13* de la propia LOPD, los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad; resulta difícilmente compatible con la denegación del derecho a ser informado del art. 5 LOPD acordada por la Administración Pública con el único fundamento de la persecución de una infracción administrativa . El Fallo en este caso fue positivo para el Defensor del Pueblo.

El artículo 18.4 de la Constitución en el que se quiso fundar el nuevo derecho de autodeterminación informativa estudiando la corriente de doctrina no estableció ningún nuevo derecho, sino un límite a una facultad , "el uso de la informática" derivable del derecho general de la libertad, art. 17.1 C o de la libertad específica de comunicación, art. 20.1 CE sobre la base de derechos expresamente consagrados en la Constitución ("el honor y la intimidad personal y familiar", art. 18.1 CE). Se trata pues de una clausula que establece límites expresos en el ejercicio de derechos fundamentales.

Dicho límite quedó registrado en la sentencia STC 254/1993 cuyo título recoge expresamente las palabras *libertad informativa*.

Además, la solución escogida ofrece la ventaja de favorecer la construcción de un régimen jurídico más eficaz y la elaboración de una doctrina más coherente y sistemática al acotarse, con precisión, los campos propios de uno y otra.

Concluyendo, en cualquier caso, que no pareció conveniente una ampliación del campo de protección del derecho a la intimidad.

Su discurso quedó focalizado en la dialéctica *autodeterminación informática vs. libertad informática* introducida en la sentencia del Tribunal Constitucional alemán STFCA de 15 de Diciembre de 1983. Esta aceptada apertura a posteriores desarrollos en orden a otorgar protección frente a nuevas situaciones de peligro que puedan surgir con el desarrollo tecnológico y social quedó perfectamente reflejada en sentencia STC 292/2000 la respuesta de recurso de inconstitucionalidad por parte del Defensor del Pueblo postulando la necesidad del *habeas data*.

El tratamiento del recién definido dato sensible que no cuenta parangón similar en EEUU, sí cuenta con el apoyo de la *Directiva 2002/58/CE* en materia de cooperación de este tipo de datos entre Administraciones Públicas.

Como observación final comentar que la Ley de Bonn de 1977 y reformada en 1999 explica por vía jurisprudencial una serie de causas que no se dan en España,

- No recoge expresamente un derecho a la intimidad
- Reconoce que la dignidad de la persona es un derecho fundamental

De modo que el *Tribunal Constitucional Federal Alemán, TFCA*, ha creado nuevos derechos entendiéndolos como desarrollo del derecho a la dignidad de la persona postulando la facultad del individuo, derivada de la idea de autodeterminación de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida.

En nuestro país se ha optado finalmente por, independientemente de que la intimidad comparta con otros derechos el nivel de fundamental, porque este derecho permanezca abierto , flexible y capaz de acomodación para ulteriores desarrollos en orden a otorgar protección frente a las nuevas situaciones de peligro que puedan surgir con el desarrollo técnico y social.

Si no se encuentra conexión directa con alguno de los derechos fundamentales consagrados por la

CE, ese derecho nuevo podría verse privado de la significación propia de los derechos fundamentales. Desde esta perspectiva, sí se consideró más útil el estimarla comprendida en un derecho fundamental ya reconocido, el de la intimidad.

Todo comenzó en junio de 1969, cuando un diario alemán publicó un artículo en el cual se advertía sobre los peligros que la informática planteaba a los derechos de los ciudadanos. El artículo concluía planteando la necesidad de una ley. El Primer Ministro del estado de Hesse leyó la noticia e inmediatamente ordenó que se elaborara una ley que tratara el problema de las bases de datos públicas que contenían datos de todos los ciudadanos. En ese entonces, el gobierno apoyaba la existencia de un banco de datos centralizado que contuviera la información de los ciudadanos. La publicidad del gobierno citaba el siguiente ejemplo: "Si Vd. maneja en la ruta y tiene un accidente y se encuentra inconsciente, con un solo acceso al ordenador será posible conocer sus antecedentes, su historia clínica, sus enfermedades, etc. Las chances de sobrevivir se incrementarán significativamente.

A raíz de esta nota periodística, el tema se instauró en la opinión pública y el 7 de octubre de 1970, el estado alemán de Hesse ya tenía su ley aprobada. Surgía así la primera ley de protección de datos del mundo.

No resulta demasiado alejado observar que mientras en las empresas no se apueste por otorgarle un derecho fundamental a la personalidad jurídica, y siga bajo el amparo de otras ramas del derecho: de patentes, de marcas, civil y penal no se alcanzará un principio de transparencia negativo en todo caso para la protección del secreto de los negocios. Distando la situación del *Principio de Transparencia*[42] *propuesto en la Resolución de Madrid y recogida en una cita anterior de la LORTAD ,*

> 1.Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere.
>
> 2.La persona responsable deberá facilitar a los interesados, al menos,

42 L 11/2007 (art.4)

información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente Documento, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

3. Cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.

4.Cuando los datos de carácter personal no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado a la persona responsable.

5.Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad.

6.Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.

1.4.- El reconocimiento de la Intimidad

Por su parte, si revisamos el contenido del origen de la definición de los Derechos Humanos en la

denominada *Carta Internacional de Derechos Humanos* comprende un conjunto de textos que incluye además de la Declaración, los dos pactos adoptados en 1976 y los dos protocolos facultativos correspondientes.

No conlleva vinculación jurídica expresa, excepto para los Estados que la han incluido en su propia Constitución. Su alcance engloba '*universalidad* ' puesto que se constituye como la primera referencia internacional común en cuanto a las libertades fundamentales y los derechos humanos.

La *Declaración Universal de Derechos Humanos* es la más importante redacción elaborada por la *Organización de las Naciones Unidas* , *ONU*. Reacciona frente los siguientes documentos,

- La Declaración de Roosevelt, también llamada de las "Cuatro Libertades"

- La Carta del Atlántico, firmada por EEUU y Gran Bretaña en agosto de 1941

- La Declaración de las Naciones Unidas, de 1 de Diciembre de 1942, denominada "La Carta"

- La Declaración de Filadelfia, de 10 de mayo de 1944, de la Organización Internacional del Trabajo ,OIT

- La Declaración de la Conferencia de Dumbarton Oaks, de 7 de octubre de 1944

- La Declaración de la Conferencia de Chapultepec, de 8 de marzo de 1945

• La Conferencia de San Francisco, de 26 de Junio de 1945 . El art. 12 establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques"

• La Recomendación 509 en 1968 de la Asamblea del Consejo de Europa dirigida al Comité de Ministros con el propósito de que la Convención Europea para la Protección de los Derechos Humanos buscará la forma de proteger los derechos de la persona, motivó una serie de resoluciones

• La Recomendación desembocó en el surgimiento del Convenio 108 del Consejo de Europa. Fue suscrito el 28 de enero de 1981 para proteger los derechos de la persona en materia de datos personales en Estrasburgo. España lo firmó el 28 de Enero de 1982, pero no lo ratificó hasta tres años después, el 27 de Enero de 1984

Comienza la categorización de datos sensibles: raza, religión, opinión, salud, sexo, .., que no habrán de tratarse salvo que se apliquen unas garantías apropiadas. La ampliación de estos derechos para sus Estados miembros cuenta con la posibilidad de la relación de *art. 5 a 11.*

De manera que, según los *art. 10.2, 18.4 CE*, la Constitución deberá interpretarse teniendo en cuenta los Tratados y Convenios Internacionales ratificados por España. Sus principios tienen el valor de derecho interno, conforme al art. 96.1 CE.

La interpretación de las normas constitucionales al igual que las leyes que las desarrollen no pueden entrar en contradicción con estos principios , por el art. 4, Capítulo II.

Su objetivo "garantizar a cualquier persona física sean cuales fueren su nacionalidad o su residencia,

el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona", art. 1.

A su vez, el artículo 8 dice

> "8.1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 8.2.No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás"

Surge la necesidad de compartir información, y para satisfacerla se genera el llamado *Sistema de Información de Schengen, SIS ,* estableciéndose en las fronteras un visado uniforme para todos los estados que lo componen. Se pretende crear y mantener un sistema de información común, con una parte nacional de cada una de las partes contratantes y una unidad de apoyo técnico. El SIS podrá utilizarse a efectos de expedición de visados, de permisos de residencia y de admisión de extranjeros donde las condiciones que tienen que respetar los estados vienen determinados por el *art. 118.*

Desde la entrada en vigor del *Tratado de Amsterdam*[43] *, el Comité ejecutivo de Schengen e*s sustituido en sus competencias por el Consejo de la UE.

El contenido del derecho a la intimidad sólo está proclamado por la Constitución, pero no definido. Para la jurisprudencia , su idea originaria tiene como finalidad principal el respeto a un ámbito de

43 Modificación del Tratado de Maastrich (Titulo XIII y XIV. En vigor dese 1999, art. 51, art. 73 q, art. 117, art. 118, art. 129)

vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado, TC, S. 110/1984, fundamento jurídico 3.

Estas limitaciones al contenido normal de los derechos fundamentales vendrán determinadas por su contenido esencial que debe respetarse en todo caso, pero que además deben ser razonables y proporcionadas.

Por consiguiente, debemos considerar los límites legítimos del derecho de la intimidad, y en particular en el tratamiento automatizado de los datos personales. Es decir, cuál es su contenido esencial.

En la exposición de motivos de la LORTAD se hablaba de que el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la '*Privacidad*' y no de la '*Intimidad*': aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona al domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del *art. 18* de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.

En España la protección de un derecho fundamental como lo es el de la intimidad de la persona se encuentra actualmente protegido por una ley orgánica tal y como el *art. 18. 1* de la Constitución, en concreto por la *LO 1/82* .

Con anterioridad a la ley, el amparo que anteriormente se otorgaba a estos derechos se realizaba a través del art. 1902 del Código Civil.

En Estados Unidos el denominado 'right of privacy' se protege a través de los ilícitos de daños comúnmente conocidos como *torts*. En Alemania, al igual que en el reto del continente la protección se realiza a través del Derecho Penal. El modelo anglosajón, como en el resto de cuestiones apuesta por la responsabilidad civil.

Los códigos constitucionales europeos alertan sobre la dificultad de controlar la información y el uso que se hiciera de los sistemas informáticos. Por otra parte, y en relación a proteger el derecho de la intimidad se priorizan la libertad de las comunicaciones y el secreto por velar por la autonomía del ciudadano en su ámbito de vida privada.

El *Grupo de Trabajo W29* originario en la Comisión Europea tiene como una de sus funciones principales la de formular dictámenes sobre los niveles de protección en la Unión Europea y en los terceros países, y emitir recomendaciones sobre cualquier cuestión referente a la protección de las personas con respecto al tratamiento de los datos personales.

Se reconocen los siguientes principios fundamentales en la protección de las personas a través de sus datos personales:

- *Principio de 'limitación de objetivos'*: los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la trasferencia

- Principio de '*proporcionalidad y de calidad*': los datos deben ser exactos y estar actualizados, además de pertinentes y no excesivos con relación al objetivo para el que se trasfieren o tratan con posterioridad.

• Principio de '*transparencia*': en la recogida de los datos, debiendo informarse a los interesados sobre el objetivo del tratamiento y de la identidad del responsable en el tercer país.

• Principio de '*seguridad*' : Se hace por tanto necesario definir el concepto de *IPI*, como '*Información Personalmente Identificable'*: haciéndose referencia a todo lo que en la red electrónica puede ser vinculado o relacionado con una persona y por ello con su privacidad, dignidad y libertad para posteriores consideraciones de la Ley.

La Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen *art. 7*, menciona que tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el *art. 2* de esta ley: La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.

Las acciones de protección frente a las intromisiones ilegítimas caducarán transcurridos cuatro años desde que el legitimado pudo ejercitarlas.

La Ley Orgánica 1/1982, de 5 de mayo, protege civilmente a la intimidad personal y familiar frente a todo género de intromisiones ilegítimas. Cuando la intromisión sea constitutiva de delito se aplicará el Código Penal.

La ley establece diferencias entre si la lesión se produjo antes o después de un fallecimiento y si la persona llegó a denunciar esta situación.

2. - Responsabilidad Técnica y Representación Legal

Del reconocimiento de la importancia del desarrollo de las Taxonomías , como se ha querido dejar patente en el *Capítulo I* de la presente Tesis, podemos extraer algunos principios o consideraciones generales que nos pueden servir a modo de guía previo a exponer el discurso vigente acerca de las

responsabilidades tanto desde el campo legal como desde el técnico en el área de tratamiento de la Historia Clínica:

- resaltando la importancia de los *agentes*[44] identificados en cada época en torno a la percepción y tratamiento de la privacidad y su posterior consideración desde un estado inicial de bienestar, y ampliando el campo de observación cuando el ciudadano hubiera alcanzado el horizonte de paciente resulta factible detectar más fácilmente aquellas situaciones por las que debe discurrir el desarrollo del dogma legislativo , la labor del legislador y la de un supervisor técnico que adoptará medidas de salvaguarda a fin de sobrellevar posibles incidencias en el tratamiento de estos especialísimos datos de carácter personal

- a fin de poder detectar aquellos posibles *Niveles de Intimidad* que el individuo considera equilibrio entre su percepción , anteriormente descrita, y la consiguiente manipulación del dato clínico no se deberá olvidar , sino más bien registrar aquellos escenarios y contextos en los que se extraen estos significados

- con independencia del *status quo* en el que se encontrara el ciudadano , éste debiera preguntarse en qué medida se es *consciente* de lo que ocurre, bien fuera en relación al Gobierno, a la familia, al Empleo, a las políticas de cada comunidad, etc.

- Reconociendo la *Naturaleza* de la Información y de cómo se crean intereses sobre ella, resultará factible superar la perspectiva de cómo cada Sociedad protege los problemas en torno a la Intimidad Personal frente al denominado 'bien social'

44 N. HUHNS, Michael, P. SINGH, Munindar. "Agent Jurisprudence". IEEE Internet Computing. March – April 1998.
SARTOR Giovanni. "A Formal Model of Legal Argumentation". 1994

- se puede concluir que cada Taxonomía debiera decir más bien poco más allá de su propio contexto

- advertencia de los posibles peligros , para cada Grupo Humano, que participe en la manipulación del dato médico del posible *Uso Secundario*[45] que se le pudiera dar

- de modo genérico se identifican tres grandes *grupos* en torno a lo que se ha venido en llamar estructura de la e-Sanidad: el propio paciente, el técnico más o menos caracterizado en su profesión y que debe evitar la perdida de información; y, la del asistente sanitario no informático que en el día a día interacciona y trata la salud del paciente.

- para el reconocimiento de principios y agentes debemos mantener continuamente activo el *Ciclo de Deming*[46] o "*Plan.Do.Check.Act"*

- reconociendo la necesariedad de la actualización y colaboración en la elaboración de los *Códigos de Buenas Prácticas,* así como de la importancia de recabar adecuadamente aquellos *Requerimientos Informados* correspondientes a cada Sistema Nacional de Salud cada Grupo Humano de Taxonomía que participa en el soporte de la e-Salud detectará con mayor nitidez aquellas entradas y salidas para los activos que hubiera que proteger o vigilar dentro de su Grupo. Es de este modo, como el Tecnólogo sabe de antemano que nunca es un plus el manejo y aplicación de estándares reconocidos internacionalmente

Conforme al *Convenio de Oviedo de 1997* propuesto por el *Consejo de Europa* se establece en su *art. 5* que una intervención en el ámbito de la sanidad tan solo podrá efectuarse después de que la persona afectada haya emitido su expreso *consentimiento*, consentimiento que por otra parte podrá ser retirado en cualquier momento.

45 N*HIN, Nationwide Health Information Network*: una vez que ha sido recolectada la información con un propósito, después se usa con otro diferente, y fuera del contexto en el que fuera recopilado. Este es el pral. razonamiento para bloquear el Derecho ARCO

46 ISO/IEC 27 001, ISO/IEC 27 002

A continuación y sin la consideración esta del paciente, por ejemplo, en situaciones de 'urgencia' y desde el punto de vista médico podrá ser llevada a cabo cualquier intervención en favor de la salud de la persona afectada. Debiendo, no obstante, observarse los deseos anteriores del paciente si así constara, *art. 9*.

Toda persona tiene derecho a que se respete su vida privada respecto a la información en materias de salud, respetándose en cualquier caso, la voluntad del paciente a no ser informado.

El *art. 23* reconoce la contravención precisamente de estos derechos o principios garantizando una protección jurisdiccional de los preceptos que propone. Y es su *art. 26* el que no admite restricción a tales derechos establecidos.

Referencias directas las encontramos en el siguiente articulado:

- a.10 D 95/46/CE
- a.6 LOPD
- a.3, a.8 L 41/2002
- a.6.2 RD 223/2002
- a.22 L 11/2007

El paciente podrá manifestar en el 'documento de instrucciones previas' su voluntad manifiesta con objeto de que esta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de hacerlo personalmente o bien una vez llegado el fallecimiento sobre el destino de su cuerpo o de los órganos del mismo. Este derecho reconocido en el *art. 11* que se otorga al paciente puede designar, además, un interlocutor que mediara entre él y el médico pertinente o equipo sanitario. Creara, por consiguiente, el Ministerio de Sanidad y Consumo el Registro Nacional de Instrucciones Previas, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud.

Por su parte la Ley *L 11/2007* reconoce al ciudadano el derecho a manifestar consentimiento, pudiendo este emitirse y recabarse también por medios electrónicos.

Casos más complejos que incluso deberían poder justificarse judicialmente nos lo presenta la

Agencia de Protección de Datos en su 'Informe 488/2004' planteando, por ejemplo, la tesitura de la comunicación de los datos a otro facultativo de la misma especialidad que una consultante, motivada por el cese de su actividad.

Debe recordarse, nos recuerda su argumento, que de la interpretación del ya mencionado *art. 17.1* y del *art. 18.1* de la Ley, que dispone que "El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella", se desprende que los datos sólo podrían ser comunicados a otros facultativos en caso de que los mismos fueran a realizar una actividad de diagnóstico o tratamiento del paciente o el propio paciente solicitara la transmisión de su historia a su nuevo médico, sin perjuicio del deber de conservación del anterior.

Continuando con el añadido de dichas complejidades nos presenta la Agencia de Protección de Datos un nuevo caso cuando se produce un cambio en el servicio de prevención, la comunicación de los datos relativos a la vigilancia de la salud de los trabajadores a la nueva entidad que desarrolle el servicio de prevención sería un supuesto de 'cesión de datos' habilitado en el ya citado *art. 23.1* de la *Ley 15/1995* en relación con el art. *30.3* de la misma Ley, derivado de la obligación de puesta a disposición del nuevo servicio, derivado a su vez, de la obligación de mantenimiento de la historia clínico-laboral prevista en el reseñado *art. 37.3. c)* del *Real Decreto 39/1997*. Es decir, estaríamos ante un supuesto de cesión de datos de carácter personal, que al estar autorizado en una Ley, no necesitará del consentimiento de los trabajadores , *art. 11.2.a* de la *Ley 15/1999*).

Continua añadiendo la Agencia que una Mutua, que presta el servicio de vigilancia de la salud de los trabajadores, deberá proceder a la inscripción del ficheros de "vigilancia de la salud" como responsable del tratamiento que realiza según dispone el *art. 23.1 d)* de la *Ley 31/1995* el empresario está obligado a, "elaborar y conservar a disposición de la autoridad laboral" la documentación relativa a la "Práctica de los controles del estado de salud de los trabajadores previstos en el *art. 22* de esta Ley y conclusiones obtenidas de los mismos en los términos recogidos en el último párrafo del apartado 4 del citado artículo".

La Ley, por otra parte, no impide otros usos posteriores de los datos médicos, sin perjuicio de que se introduzcan salvaguardas para garantizar la confidencialidad del paciente. Así, en su *art. 16.3* se contempla el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, siendo obligado preservar los datos de identificación personal del

paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente.

Existe una necesidad de consentimiento expreso, aunque no necesariamente escrito para los datos relacionados con la salud, el origen racial y la vida sexual.

En caso de datos no especialmente protegidos se le otorga al afectado un plazo de treinta días para manifestar su tratamiento.

La solicitud de consentimiento respecto de un tipo de datos no podrá ser nuevamente ejecutada en el plazo de un año a contar desde la fecha de su solicitud. Tanto el derecho de acceso como el otorgamiento del consentimiento informado prescriben al de un año.

No será necesario el consentimiento del interesado en caso de urgencia relativa a la salud o para la realización de estudios epidemiológicos en los casos legalmente previstos.

En casos de trasferencias internacionales, el consentimiento informado se hace necesario para establecer la relación contractual entre el afectado y el responsable del fichero, debiéndose, no obstante:

- notificar a la Agencia Española de Protección de Datos
- e informar al interesado

Históricamente el consentimiento informado tiene su origen en el denominado *Código de Núremberg*[47].

47 Código de Nuremberg. Disponible en: http://www.bioeticayderecho.ub.edu/archivos/norm/CodigoNuremberg.pdf

De acuerdo con el *Código de Buenas Prácticas Clínicas*[48]' tanto las entrevistas del consentimiento informado como su expresión escrita debe contener las siguientes indicaciones de alguna forma:

- que el estudio implica investigación
- el propósito del estudio
- el acuerdo del estudio
- procedimientos a seguir
- responsabilidades del sujeto
- indicaciones de aquellos aspectos del estudio que resultan experimentales
- razonables riesgos que se prevén para el sujeto
- los beneficios esperados
- procedimientos alternativos del tratamiento
- compensaciones por perjuicios
- indicación del pago prorrateado, en su caso, por la participación
- la posibilidad de abandonar en cualquier momento el ensayo
- la identificación de la responsabilidad de la confidencialidad del sujeto en el acceso a sus datos
- duración
- número de sujetos

48 Código de Buenas Prácticas Clínicas. CPMP/ICH/135/95, (pag. 18) Disponible en: http://ec.europa.eu/health/files/eudralex/vol-10/3cc1aen_en.pdf

Un paciente puede precisar requerir el conocimiento de determinada información acerca de su historia clínica para la aplicación del tratamiento médico correspondiente que se le decida aplicar en una determinada zona geográfica de nuestro planeta. La contextura del Centro donde se pueda producir este hecho puede ser de carácter público o privado.

Cualesquiera fuera la naturaleza jurídica de los casos, se precisará la observación de la colaboración de la aplicación de la legislación de los países origen y demandante del servicio informático. Entre ambos cuerpos y apoyándose en la dinamización internacional entre ambos que se hubiera decidido existirán, además, normalizaciones y regulaciones de Organismos reconocidos que en el trascurso de la dialéctica se hubiera decidido aplicar como garantes y acompañantes en su desempeño.

El nivel de acuerdo decidido desde el Gobierno de ambos países decidirá el grado de traba a la hora de proporcionar dicha información y el formato en que será recibido por parte del Centro de Atención Médica.

Habida cuenta de la posibilidad de Acceso por parte del ciudadano de la información necesaria acerca de su Historia Clínica, se le puede plantear al mismo el ejercicio o la determinación de sus propios criterios de filtrado de su información en la medida contemplada por la *Ley General de Sanidad* que se le aplicara. Tal derecho es reconocido como ejercicio de los *Derechos ARCO*, esto es, de *Acceso, Rectificación, Cancelación y Oposició*n, resumiendo en cierto modo la defensa que le está permitida en materia de protección de datos.

Tanto es más cuando se puede ver ampliada esta perspectiva de aplicabilidad con fines de estudio de carácter estadístico. Y, de igual modo, qué ocurre en el desarrollo de la intervención médica con el manejo de los *Consentimientos Informados*, idénticamente se puede aplicar el concepto del tratamiento de su Historia Clínica, *HC,* en el contexto de la e-Administración.

Ya en último término se podrá provocar el bloqueo de datos o cancelación, quedando esta información tan sólo a disposición de la Administración Pública, Jueces y Tribunales. Quedando siempre amparado el paciente ante la Agencia de Protección de Datos.

El derecho de acceso contempla el conocimiento del fin último para el que se estuviera desestimado un tratamiento de datos, pudiendo ejercerse en su caso un derecho de oposición, y conocimiento

exacto de las características del fichero en el que se encuentra invocado.

Los accesos restringidos podrán obtenerse por escrito, y por visualización de pantalla de ordenador .

Existen otros derechos considerados en relación a la seguridad del paciente dentro en el contexto de la e-Sanidad si tenemos en cuenta el modo en que todo ciudadano es destinatario de una *Tarjeta Sanitaria Electrónica en* la que reside una identificación digital y por medio de la cual puede identificarse en el marco de su sistema sanitario con revocación de firma electrónica.

En este punto son las Comunidades Autónomas las que se hacen responsables tanto de la tramitación de la tarjeta como de las autentificaciones realizadas en el contexto de la operativa, debiendo proporcionar idénticamente un Servicio de Atención al Cliente.

Por otra parte y dependiendo del desarrollo que haya alcanzado la aplicación de la Telemedicina en su Comunidad Autónoma, podrá disponer de otra serie de dispositivos médicos como localizadores , servicios de domótica, pdas, etc.

La interoperabilidad entre Comunidades Autónomas permite al usuario de la e-Sanidad el acceso y obtención de informes clínicos determinados a fin de ser almacenados en dispositivos electrónicos, no considerando necesaria la citación de las copias impresas por considerarlas siempre hábiles y obvias.

Se encuentra el ciudadano con la posibilidad de vetar el acceso de determinados informes entre Comunidades y de la utilización de un sistema de alertas que le indique siempre cuál es el curso de sus diligencias incluidos las denegaciones del derecho que hubiera podido recibir.

El modelo de acceso a esta tipo de información deberá encontrarlo habilitado las veinticuatro horas del día y a lo largo de toda la semana.

Una tercera clasificación de los derechos del ciudadano se puede presentar desde el punto de vista de los *Sistemas de Prevención Laboral* como puede ser el caso de las Mutuas y Aseguradoras, del que siempre se deberá poder obtener el 'prorrateo' del seguro que le ampara y aquel 'Código Tipo' al

que se encuentra adscrito un Promotor en un Sistema de Vigilancia Médica o Farmacovigilancia independientemente de que se produzca el tratamiento de datos de su HC fuera o dentro del país donde reside.

El sujeto participante en el marco sanitario también conocido como *Trial Subject*[49], puede por su parte, adoptar otra posición respecto de la defensa de sus derechos, haciéndose consciente que ni el investigador ni ningún otro miembro de la plantilla del centro sanitario donde se le deben respetar los derechos como ciudadano de la Unión Europea debieran influir en la decisión de su continuidad en el estudio o tratamiento.

No parece justo realizar una desligazón entre la figura del consumidor y el proceso concreto de generación y tratamiento de los consentimientos informados, puesto que entraña una responsabilidad manifiesta por parte del paciente no sólo el ejercicio de los Derechos ARCO sino la participación completa en el proceso de asistencia sanitario con las correspondientes afirmaciones o denegaciones de las fases de toda asistencia.

Por otra parte, podremos analizar la oportunidad de las coberturas que el Estado ha querido otorgar al papel del consumidor como usuario del servicio sanitario informático que le ofrece la Sociedad en la que vive.

Manifestamos las siguientes caracterizaciones que pueden llegar a condicionar la figura del consumidor en el ámbito de la e-Sanidad:

- por el eje ejercicio de los Derechos Arco

- por el ejercicio de los derechos a Sanidad y derechos de las Telecomunicaciones[50]

49 o paciente. CPP/ICH/135/95. July 2002;RD 1736/1998, (art. 62); 2006/24/CE, (art. 7); RD 223/2004, (art. 1)

50 1.- SANCHEZ BLANCO, Miguel, MORAN RIVERO, Jose Manuel, SOLER MATUTES, Pere "Jurisprudencia de Telecomunicaciones". Editorial Aranzadi, S.A. 2008. : (pag. 42) constituye doctrina pacífica y consolidada del Tribunal Supremo que la CMT tiene atribuida *potestad normativa*. Dicha potestad se ejercita a través de las Circulares. En la SAN 31 de marzo de 2006, donde se discute la legalidad de la Circular 2/2004, fueron objeto de dichos <<límites formales>>. De la Sentencia escrita se deduce la importancia del preceptivo << Informe de Legalidad>> previsto en el apartado 3 del artículo 26 de la Orden de 9 de abril de 1997, así como también la innecesariedad, en la materia

2. 1.- Responsabilidad Técnica

En esta Tesis se perfilan algunos procesos que la Sociedad del Bienestar debiera reconocer tales como el adecuado desarrollo de Taxonomías por cada Naturaleza de Dato de Carácter Personal, el consiguiente proceso en Formación a cada Grupo Focalizado, el desarrollo de legislaciones que vigilen el derecho a la intimidad y la protección de datos de carácter personal y sus correspondientes reconocimientos por parte del ciudadano de nuevo en materia de Formación. Bajo estos procesos mínimos probablemente no necesitaríamos estar hablando de este apartado, en cuanto apenas existe en el Mundo Académico reconocimiento de la Enseñanza del Derecho Informático, pues primeramente ha de resultar manifiestamente reconocido por el propio Derecho , y en paralelo con las dinámicas de superaciones de Planes de Riesgos y Políticas de Seguridad no son sino el devenir de los propios marcos que proponen los estándares internacionales en el resultado de sus experiencias satisfactorias los que poco a poco van sugiriendo un camino que observado de forma superficial puede parecer conducen al camino contrario.

Cuando el Técnico Especializado que maneja los datos sanitarios reconoce no sólo el propio *Nivel de Seguridad* que le otorga la especificación legal ha de resolver y la solución analizada técnica que le ha de proporcionar que nunca resulta, por otro lado, imposible, sino además el Rol que debe desempeñar en este nuevo espacio del Derecho Informático, no deja de llamarnos la poca atención, que hasta el momento se le ha prestado al *Documento de Seguridad* que con posterioridad se resolverá, por observar que a fecha actual pocos e-Técnicos han conocido de su existencia.

Es el objetivo de esta Tesis el resaltar la importancia de la diferenciación al respecto de los Grupos Taxonómicos que se proponen, por considerar que la simple observación de esta diferenciación ya conduce a resultados positivos, tanto más cuanto mayor se considere su buena aplicación.

concreta de la portabilidad, de dar audiencia a las asociaciones de consumidores y usuarios en el procedimiento de elaboración de Circulares; (pag 43) El Tribunal Supremo también ha aplicado el principio de jerarquía normativa para anular preceptos contenidos en Circulares de otros organismos de Estado. Entre estas, puede citarse la SNS 2 de Octubre de 1989. Las Circulares de la CMT no pueden regular materias que sean objeto de reserva de ley a estos efectos, el artículo 23 Ley 50/1997 declara expresamente que los reglamentos no podrán tipificar delitos, faltas o infracciones administrativas, así como atributos, cánones u otros cargos o prestaciones personales o patrimoniales de carácter público. El artículo 52.1 Ley 30/1992 manifiesta que para que produzcan efectos jurídicos las disposiciones administrativas habrán de publicarse en el Diario Oficial que corresponda; (pag. 45) El apartado 2 del artículo 52 Ley 30/1992 manifiesta que las resoluciones administrativas de carácter particular no podrán vulnerar lo establecido en una disposición general, aunque aquellas tengan igual o superior rango a estas.

2.- L 11/2007 ,(art. 3) (redefinición Firma Electrónica), y L 56/2007 , (art. 51) (prueba documental soporte, siendo el objeto doble de protección en salud pública y en relación a personas jurídicas que tengan la condición de consumidores y usuarios)

El e-Técnico debe preocuparse no sólo en resolver de forma magistral , como no cabe esperar otra cosa, su labor técnica sino de otorgarle aquellos valores que no debiera negar y dejar de reconocer en el trascurso de su desempeño, apartando otras consideraciones que pudieran surgir y debiendo relegarlas a unos segundos planos.

El personal sanitario deberá acomodarse continuamente al *Código de Buenas Prácticas* y a *los Comités de Ética Profesional* en el ejercicio de su desempeño. Continuando con nuestro razonamiento el Técnico de e-Administración deberá observar idéntica actitud en el marco privado-público en el que pudiera ocurrir su relación contractual observando siempre estos principios actualmente únicamente reglados por la Ley 11/2007,y su desarrollo según los RD 03/2010 y RD 04/2010.

Cuando sea necesario el desempeño de algún servicio informático por parte del responsable de un fichero determinado no será considerado como *comunicación* aun tratándose de un acceso de datos a terceros.

Por otra parte, la realización de tratamientos de datos por cuenta ajena deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su contenido y valor añadido.

Los mecanismos de acceso han de producirse por medio de un mecanismo que resulte gratuito al ciudadano. Únicamente se puede denegar el acceso si se hubiere ejercido ya tal derecho y contabilizando, según disposición oficial, un año desde el acceso registrado.

Independientemente de la existencia de una empresa subcontratada que cubra dicho servicio, y en el momento de producirse una solicitud de acceso, debe ser comunicada dicha petición inmediatamente a la Entidad Sanitaria correspondiente a fin de llevar por el mismo procedimiento indicado la diligencia.

El correo electrónico se considera válido a efectos de establecer tales peticiones y aceptaciones.

Si el ciudadano considerara que existe una inexactitud en alguno de los datos, se realizará una notificación pudiendo aportar aquella documentación justificativa de tal apreciación.

Al responsable del fichero, y consiguientemente a todos los Técnico de la e-Sanidad que se vean relacionados en su salvaguarda, se le debe exigir la exactitud de los datos incluidos en la HC.

2.1.1.- Dato Médico como Dato Estadístico

No existiendo aún suficiente experiencia estadística generada al respecto de una observación técnica positiva cuyos datos no puedan ser negados a la hora de generar opiniones que produzcan publicaciones profusas en revistas de reconocido impacto, proponemos unas ingenuas e inocentes indicaciones en el reconocimiento de la Naturaleza del Dato Clínico que nos pueden ayudar a potenciar campos aun por explorar y donde aun cabe mucho trabajo:

El Ser Humano es un ser que reconoce la Medicina como aquella Ciencia que le permite su bienestar Físico, tan sólo con esta premisa ya nos sentimos obligados a expresar que necesariamente el individuo ha de reconocer que su Esencia ha de reconocer su Bien Estar y Estado de Buena Salud para el desempeño de sus múltiples actividades.

- Como una indicación que se encuentra internamente reconocida y que, normalmente, no se expresa, pero de que desde aquí sí se considera necesario exponer, se propone que la enfermedad reconoce al enfermo como una voluntad de haberse sentido mal que obliga a indicar que el dato médico no es sino un dato estadístico que puede dejar de existir cuando el enfermo ya no lo es: luego se identifican incluso escenarios o actitudes que pueden haber conducido al ciudadano a tal estado y la voluntad del enfermo de salir de tal situación.

- Tal vez y expresado de forma no tan metafísica, la siguiente imagen nos saque de nuestra confusión: la aparición , por ejemplo, del microscopio ayuda a reconocer precisamente todo el esfuerzo de observar los mecanismos del Ser vivo como precisamente el resultado de la interacción de la conducta de nuestros tejidos y las bacterias en algunos de los desordenes físicos que se reconocen como enfermedad. En este punto y precisamente por encontrarnos viviendo en una era totalmente tecnológica, esta segunda idea apoye nuestra

Tesis de que efectivamente el dato médico es desde el inicio un dato estadístico

- La escribiente intuye que tan sólo este reconocimiento cambiaría completamente la forma de abordar legalmente este tipo de dato de carácter personal en cuanto precisamente es aquí donde no se ha generado suficiente legislación. Es como si el legislador hubiera obviado, por alguna razón , no muy certera este primer paso haciendo aplicar la lógica de todo el *apartado 3.2*

- Señalando aquellos hitos donde sí existe este tratamiento:

    - Se observa que aparentemente el dato clínico es tratado de forma estadística en el momento que se produce su disociación[51] y no desde el principio, por su

51 *Enciclopedia Jurídica INTECO*: Dato de carácter personal que ha sido sometido a tratamiento para que la información que se obtenga de él no pueda asociarse a ninguna persona física identificada o identificable. Término relacionado con el procedimiento de disociación definido en el artículo 3.f. de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Circular e-Landwell 001: La dirección IP como dato disociado

El informe 327/03 de la Agencia Española de Protección de Datos (AEPD) llega a la conclusión de que las direcciones IP, tanto fijas como dinámicas, son datos de carácter personal a los que hay que aplicar medidas de seguridad de nivel básico. Los razonamientos de la AEPD son los siguientes: 1. Los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios a los que han asignado direcciones IP. 2. Con la asistencia de terceras partes responsables de la asignación de la dirección IP se puede identificar a un usuario de Internet por medios razonables. 3. Existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos. Sin embargo, existen muchas actividades en las que se trabaja con direcciones IP completamente disociadas y en las que no es posible identificar a un usuario concreto de Internet por medios razonables. Exigir el tratamiento de dichas direcciones IP como datos personales, con la consiguiente aplicación de medidas de seguridad de nivel básico, sería altamente costoso para muchas empresas. No son direcciones IP que puedan ser asociadas a una persona física por medios razonables, por ejemplo, los de todos aquellos usuarios que acceden a Internet a través del servidor proxy de su proveedor de acceso o de la empresa en la que trabajan. En estos casos, la dirección IP pública del usuario no coincide con su dirección IP privada y su identificación sólo puede conseguirse mediante un mandamiento judicial o en los casos expresamente previstos por la Ley. Entiendo que ninguno de esos supuestos representa un medio razonable de identificación. Tampoco debe considerarse un medio razonable el uso de técnicas ilegales de identificación de usuarios a los que se refieren los antes mencionados puntos 2 y 3 de los razonamientos de la AEPD. Respecto al punto 2, los datos personales de identificación de un usuario no pueden ser cedidos por los responsables de la asignación de la dirección IP si no existe un consentimiento previo del afectado, concurren los requisitos establecidos por la Ley o son solicitados a través del oportuno mandamiento judicial. Respecto al punto 3, la mayoría de las actividades descritas pueden representar una invasión de la intimidad del usuario, ya que los datos de identificación son obtenidos y tratados sin su consentimiento y utilizando técnicas que pueden tener cabida en el artículo 197 del Código Penal. Según mi modo de ver, la comisión de un delito no es un medio razonable de identificación, y el hecho de que haya unos pocos que puedan hacerlo no debe penalizar a todos los demás, que actuan legalmente. Por otra parte muchos procesos de tratamiento de direcciones IP se realizan sin intervención humana, y forman parte de la gestión cotidiana del tráfico de paquetes IP que permite el funcionamiento de Internet. Las actividades de routing y de caching, por ejemplo, no

mera existencia

- Consideramos que incluso esta apreciación podría condicionar no sólo el momento de la creación de estructuras organizacionales como los Centros Tecnológicos asociados a la Biomedicina e Investigación Farmacológica, sino a la distribución de sus propios recursos. Es por ello, que en este punto sugeriríamos y basándonos en Trabajos ya realizados el Análisis de Resultados desde los Observatorios internacionales que ya han publicado experiencias en relación a la Producción de Tecnología , orientada desde el principio a la Protección de la Intimidad y aplicado al campo de la Medicina. El sustento de los Centros Tecnológicos dentro de la I+D+I se fundamenta precisamente sobre valoraciones de los datos estadísticos tal y como están siendo contemplados por la legislación vigente actual, esto es, como datos de carácter especialísimo en materia de protección de datos. En tal medida se refiere el Consejo de Europa en relación al 'Profiling'[52] y la automatización de datos personales recomendando la práctica de determinadas tecnologías como se ha venido en denominar a las PETS[53]

2.1.2.- La TeleMedicina

Al casi no existir conocimiento de la existencia de Teletrabajadores, la primera consideración que se debe realizar es la del reconocimiento del Teletrabajador que también es un e-Técnico, esto es, no se debe dejar de hablar de la e-Sanidad sin consideración de la Telemedicina.

---

deberían entenderse en ningún caso como tratamiento de datos personales.

52 Recomendación CM/Rec (2010) 13 del Comité de Ministros a los Estados Miembros en relación al Profiling y la automatización de datos personales, (1099th meeting), citando textualmente : „Considering that the lack of transparency or even 'invisibility' of profiling add the lack of accuracy that may derive from the automated application of pre-established rules of inference can pose significant risks for the individuals rights and freedoms“ y recordando en su art. 1.2 en relación al Profiling „means an automatic data processing technique that consists of appliying a 'profile' to an individual particularly in order to take decisions concerning her or him for analysing or predicting her or his personal preferences, behaviours and attitudes“. Así mismo, el art. 2.2 reproduce la siguiente afirmación en relación a la recomendación de determinadas prácticas tecnológicas: „Member states should encourage the design and implementation of procedures an systems in accordance with privacy and data protection, already at their planning stage, notably through the use of privacy-enhance technologies. They should also take apropiate measures against the development and use of technologies which are aimed, wholly or partly, at the illicit circumvention of technological measures protecting privacy“

53 CAVOUKIAN, Ann. “*Privacy-Enhancing Tecnologies: The Path to Anonymity* Volume II”. : Disponible en: www.ipc.on.ca/images/Resources/anoni-v2.pdf

Actualmente el estado del Arte en relación a la figura contractual de esta figura es la siguiente : actualmente no existe en el conjunto de los países miembros integrantes de la Comisión Europea un marco jurídico para el Teletrabajador.

De momento se cuentan con las siguientes situaciones identificadas[54]:

- relacionados con los problemas específicos en la 'vigilancia de la salud' y prevención de riesgos, se toma en cuenta el RD 486/1997, el RD 1215/1997, que establece las disposiciones mínimas de seguridad y salud para la utilización por los trabajadores de los equipos de trabajo y el RD 773/1997 y el RD 488/1997, por el que se establecen disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización.

- Relacionados con los centros de teletrabajo[55] o *Agencias de Servicios*, dígase de espacios físicos al servicio de tercero para su uso compartido no necesariamente a una misma empresa que desempeñan su trabajo de forma independiente, pero que aprovechan como usuario las diversas formas niveles de equipamiento que ofrece el telecentro según sus propias necesidades.

- La denominada *Teletrabajo Móvil* y que permitiría trabajar en cualquier lugar, eso sí, pudiendo ceder en cualquier momento a la Oficina Central.

La aceptación de Taxonomías y la aceptación de la adecuación de optar por determinadas Tecnologías como es el uso de robots parece condicionar en gran manera la introducción de la Telemedicina si se compara el desenvolvimiento de los países europeos y la zona norteamericana como se apunta en el *Informe WTEC*.[56]

Una postura reactiva, esto es , proteccionista, no parece el mejor camino. Por otra parte, el uso de

54 SELLAS I BENVINGUT, Ramón. El Régimen Jurídico del Teletrabajo en España. Ed. Aranzadi. 2001

55 art. 1.5 *Estatuto de los Trabajadores*, ET en relación a los Centros de Trabajo y el art. 44 .1 ET: art. 1.5 ET: << a efectos de esta ley se considera centro de trabajo la unidad productiva con organización específica, que sea dada de alta como tal, ante la autoridad laboral; art. 44.1 ET: << el cambio de titularidad de la empresa centro del trabajo o de unidad productiva autonoma de la misma>>

56 WTEC report. Bekey. et. al. 2006

robots[57] parece hacer replantear viejos problemas en el tema de la protección de la Privacidad y Datos de Carácter Personal[58]:

- debido a que no toda situación puede ser prevista y a los robots se les presupone autonomía y cierta capacidad de reacción de manera independiente y su testeo puede resultar problemático desde el punto de vista legal,

- los robots interactivos y dispositivos médicos pueden recopilar información de manera que se puedan compartir en otras plataformas o trasferir a otros sistemas, surge un planteamiento bidireccional en el desarrollo normativo

2. 2.- Responsabilidad Legal

2.2.1.- Unidad de Defensor del Paciente

Salvo tratamientos agresivos o intervención quirúrgica el consentimiento podrá ser expresado verbalmente según la ley *L 41/4002*. Además El 'reconocimiento por representación' se plasma en el *art. 9* por razones de insuficiencia del estado físico o psíquico del paciente, cuando este estuviera incapacitado legalmente y cuando siendo menor de edad no alcanzare su entendimiento a comprender este supuesto; por lo demás prescribe la edad de 16 anos.

Hemos de recordar que tan sólo aquellas personas que no tengan perturbadas sus facultades y no se consideraran vulnerables serán responsables de concretar el consentimiento informado.

Se puede presentar un caso en el que el sujeto no puede leer o bien su representante legal no lo puede hacer, en este supuesto caso, un *testigo* imparcial debería participar en la entrevista del consentimiento informado, y cuando se hubiera asentido oralmente a dicha conformidad, el testigo firmará el mismo. De esta forma será representado que el consentimiento informado fue libremente consentido por el *Subject* o bien su representante legal.

57 The word 'robot' was coined in 1920 by Karel Cajzek, a Czech writer, before the firt real robots. It is related to the Czech word for work 'robota' and used for a machine that would be used for freeing men of tedious and heavy work

58 'Robotics for Healthcare'. (pag. 28 y pag. 29)

Un ciudadano siempre se podrá constituir en representante legal de otro ciudadano si así se le reconociere.

El canal de conocimiento de la identidad de las personas que pueden manejar su HC debe estar idénticamente habilitado.

La figura del representante legal se extiende su acción desde el manejo del *Consentimiento Informado* así como desde el *Documento de Instrucciones Previas*.

Desde la parte del *consentimiento informado*, se pueden presentar las siguientes situaciones:

- ejerciéndolo el propio médico cuando no es posible hacerse cargo por otro modo de la situación

- indicado por incapacidad legal

- cuando siendo menor de edad un paciente no es capaz de entender la situación y tiene doce años cumplidos en España, pudiendo variar este dato siendo, por ejemplo, de dieciséis en otro país distinto al nuestro

Desde la parte del *documento de instrucciones previas*, por su parte:

- por mayoría de edad, y en manifiesta voluntad puede indicarse el tratamiento que llevaría en plenitud de conocimiento un paciente, las medidas y observaciones que habría que considerar en caso de su fallecimiento y la indicación de un posible representante legal que sirviera como interlocutor para continuar en su caso con la aplicación de las instrucciones previas llegados el caso

- en la HC han de constar aquellas anotaciones registradas acerca del consentimiento

- habiéndose de producirse siempre por notificación escrita, es factible su <<revocación>> en cualquier momento

Así mismo, se reconoce un par de situaciones diferenciadas más de forma internacional por considerarse grupo diferenciado dentro de la ciudadanía: el de los inmigrantes y el de los prisioneros.

Cerrando este apartado con idéntica invocación a como se iniciara, con motivo del 602 encuentro del Consejo de Europa, la recomendación expresa como no. *R(97) 18* en materia de protección de datos y procesos estadísticos, en su apartado 4.3.b.i y citado como *Lawfulness*: <<The data subject or his or her legal representatives has given his or her consent according to principle 6>>.

Cualquier ciudadano que acredite el incumplimiento de la LOPD puede dirigir una denuncia a la AEPD, utilizando el modelo de denuncia que facilita dicho organismo en su página web.

Por otra parte, los corredores de seguros y los corredores de reaseguros tendrán la condición de responsables del tratamiento respecto de los datos de las personas que acudan a ellos, por los que una vez extinguida la relación, no procederá a la devolución de los datos, en los términos del art. 12 de la LOPD a la entidad consultante. La correduría de seguros, si hubiera obtenido con anterioriedad a la rescisión de la relación contractual, legítimamente el consentimiento de los asegurados, podrá seguir tratando los datos, en los términos en los que autorizó cada asegurado.

Otro tipo de consideraciones más generalistas y de estructura menos simplista deberá atenerse a la clausula denominada *third -party beneficiary clause* que textualmente dice que cuando se hubiera producido daño bien en la parte del controller o del importador, se presumirá una compensación. Precisamente en la transferencia de datos y conforme al *Documento WP 12* generado por el Documento de Trabajo del art. 29 de la Comisión Europea, la citación del contenido de los principios en la trasferencia de datos a terceros país deberá respetar:

- el principio de limitación: la información deber ser procesada con un propósito específico y con comunicación posterior no incompatible con un propósito original

- principio de transparencia

- principio de seguridad

- Derechos ARCO

- restricciones de futuras transferencias

3.- Actores en la e-Sanidad

Se precisa necesario realizar una recopilación del rol de aquellos actores que intervienen con responsabilidad en el ámbito de la e-Sanidad. Fundamentalmente recogemos la definición de las caracterizaciones regladas oficialmente en el oficio de su profesión y del documento emitido por la *Comisión Europea* en materia de trasferencias de datos a terceros países[59]:

3.1.- El Controlador o Controller[60]

Figura que, independientemente del contexto en el que estamos elaborando los requisitos informados de los escenarios de la e-Sanidad, aparece en los ámbitos de trasferencias de datos a terceros países. En concreto, dicha definición se perfiló en el contexto de propuesta de Directiva en el año 1990, habiéndose registrado el concepto de controller en el año 1981 en la *Convención del Consejo de Europa*.

Inicialmente, el concepto de controller estuvo asociado al de *controlador de archivo* desligándose con posterioridad de la actividad clásicamente asociada a un fichero, con la inclusión de la relación con el ciclo completo del flujo de datos, llegando a considerar a éste como un 'conjunto completo de operaciones'.

El propósito y significado del procesado de datos personales se determina por el controlador, bien se tratare este de una persona jurídicamente legal, autoridad pública, que sólo o conjuntamente con otros realiza tal acción[61] , viniendo a apoyar lo que se ha venido en denominar en el ámbito anglosajón *allocate responsability*.

59 European Commission. "Frequently asked questions from the EU/EEA to third countries". Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

60 D 97/66/CE

61 D 95/46/CE, (art. .2), (art.17)

Por medio de regulación se le insta a implementar técnicas adecuadas o salvaguardas, y a adoptar medidas organizacionales, sobre todo, cuando la información se distribuye por una red.

Por su parte, deberá decidir aquella legislación que resulte aplicable al procesado de la operación o al conjunto de ellas. Añadiéndose a ésta el descubrir: el objeto y propósito de cada una de sus funcionalidades, la determinación y definición de los datos personales y la vigilancia de aquellas operaciones y terceras partes que intervinieran.

En el ámbito de la e- Administración más concretamente se puede decir que cada una de las unidades administrativas se constituye como un controlador de su propio propósito puesto que actúan como intermediarias entre el ciudadano y cada una de las administraciones; por su parte, cada portal, también se constituye como un controlador ya que se procesan las peticiones de dichos ciudadanos y de los documentos públicos con propósitos diferentes para los que inicialmente fueron recolectados.

Es, precisamente, este último concepto el que ha venido la Agencia de Protección de Datos en denominar *Responsable de un fichero o de tratamiento* pudiéndose tratarse de una persona u órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales, y más en concreto notificando los ficheros ante el Registro de Protección de Datos, verificando y asegurando que sean los datos auténticos y veraces, recabando los consentimientos informados y garantizando el cumplimiento de la legislación estatal.

3.2.- El Procesador o Processor[62]

La existencia del procesador va a depender en todo momento de la decisión del controlador que puede delegar esta responsabilidad en la propia organización o bien considerarla exterior a la misma.

Aun habiéndose producido una delegación por parte del controlador, ambas figuras, las del controlador y la del procesador han de resultar legalmente independientes y con diferentes grados de autonomía y responsabilidad

El concepto de procesador va a destacar en el contexto de la confidencialidad y seguridad del

62 D 95/46/CE, (art. 4.d, art. 4.e)

procesado, haciéndose resaltar que en la división de roles, una misma entidad puede actuar de controlador para ciertas operaciones de procesado y como procesador para otras.

La existencia de la figura de controlador o procesador conlleva la obligación a concretar un contrato de acuerdo con la ley.

Lo que no va a presentar específica legitimación o autorización va a ser la determinación de la definición de ambos roles.

El *encargado de tratamiento* puede tratarse de una persona física o jurídica, pública o privada, pudiendo adoptar la forma de un órgano administrativo que, solo o conjuntamente con otros ejecuta dicha función, y en cualquier caso, fruto de una relación jurídica que le vincula con el mismo y delimita el ámbito de sus actuación para la prestación de un servicio.

Un ejemplo muy cotidiano corresponde al del informático ajeno a la organización del responsable que realiza tareas de mantenimiento de software

3.3.- La Agencia de Protección de Datos, APD y el Supervisor Europeo de Protección de Datos, European Data Protection Supervisor, EDPS

La Agencia de Protección de Datos es el ente de derecho público que reza por el cumplimiento de la normativa sobre protección de datos personales bien en el ámbito público bien en el ámbito privado, por lo que se le otorga una carácter independiente de las Administraciones Públicas y que ayuda a los responsables y encargados de tratamientos de establecer la legislación en materia de protección de datos y a resolver aquellas dudas que se le pudiesen presentar.

Por su parte, la Agencia emite 'dictámenes jurídicos' sobre las cuestiones de mayor complejidad en esta materia. Idénticamente la *Subdirección General de Inspección de la Agencia Española de Protección de Datos* realiza también Inspecciones Sectoriales de Oficio.

Cuenta con un área de *Atención al Ciudadan*o que informa y asesora a la ciudadanía sobre aquellos aspectos que les pudiera interesar de la legislación en materia de protección de datos o aplicación de

la LOPD.

En relación a la Internacionalización de Datos, la Agencia ejercerá el control de los datos introducidos en la parte española de la base de datos del *SIS, Sistema de Información Schengen*, designando dos representantes el Director de la Agencia a efectos de autoridad de control común de protección de datos del *Sistema de Información Schengen.*

Conforme al art. 26 del *RD 428/1993* y por el que se aprueba el *Estatuto de la Agencia de Protección de Datos* corresponde al *Registro General de Protección de Datos*, además de expedir certificaciones de asientos, rectificar sus errores, instruir expedientes de modificación y cancelación y publicar una relación anual de los ficheros registrados, la instrucción de aquellos expediente de autorización de las transferencias internacionales de datos.

Es precisamente el ámbito de la *Transferencia Internacional de Datos* al que queremos dedicarle este apartado en el contexto de Sistemas Informáticos Supranacionales: bien se considere por cesión o por comunicación de datos[63], o cuando se tuviera por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero en territorio español se obtiene la significancia de una transmisión[64] de datos fuera del territorio del Espacio Económico Europeo, EEE.

La Transferencia Internacional de Datos requiere autorización del *Director de la Agencia Española de Protección de Datos* con la excepción de que los datos se trasfirieran a un país que ofrecieran un nivel adecuado de protección[65] o a empresas de Estados Unidos que hubieran suscrito los principios de Puerto Seguro[66] de conformidad con la *Decisión 2000/520/CE de la Comisión* y entendiéndose se precisará subscribir un contrato cuando se tratara de una prestación de servicios.

Las transferencias internacionales de datos reguladas por los art. 33 y 34 de la LOPD y por el Título VI RLOPD, reglamento de desarrollo de la *Ley Orgánica de Protección de Datos de Carácter*

63 Las comunicaciones de datos en el EEE constituyen cesiones de datos a efectos de la aplicación de la LOPD

64 *Exportador de Datos*: persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero, art. 5.1.j RLOPD
Importador de Datos: persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercero país, ya sea responsable del tratamiento, encargado del tratamiento o tercer, art. 5.1 RLOPD

65 Declaración de países a fecha de 06 de agosto de 2014 por la Agencia Española de Protección de Datos: Suiza, Canada, Argentina, Guernsey, Isla de Man, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda

66 Disponible en http://www.export.gov/safeharbor

Personal, aprobado por el *Real Decreto 1720/2007* nos recuerda , que no será necesaria la autorización previa del Director de la *Agencia Española de Protección de Datos* cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

En concreto para las Empresas dedicadas en régimen de Outsourcing y/o prestación de servicios se considerarán reúnen las garantías adecuadas aquellos contratos celebrados en los términos previstos de las *Decisiones 2001/497/CE, 2004/915/CE, 2010/87/UE*.

Modelos más complejos de permiso de transferencias entre un encargado de tratamiento (exportador) y un subencargado (importador), y siempre que el exportador aportara garantías suficientes de respeto a la vida privada de los afectados y a sus derechos y libertades fundamentales se pueden encontrar por medio de los Documentos correspondientes al *Grupo de Trabajo, art. 29 D 95/46/CE*, conocido como *GT29* publicados como *Reglas Vinculantes* o *Binding Corporate Rules, BCR*[67]. Por su parte los *art. 70.4* y el *Título IX Cap. V RLOPD* establecen el régimen jurídico aplicable a las transferencias internacionales en el seno de una multinacional.

Como segundo ámbito de consideración particular al apartado, y en relación a sus funciones Inspectoras, *art. 28 RD*, cuando se le compete efectuar dichas funciones sobre ficheros de titularidad privada o pública y con periodicidad puntual o circunstancial , examinando los *Soportes de Información* que contuvieran los datos personales, y se sobreentiende, el Inventario que resulta en cadena de su conjunto respetando una escrupulosa trazabilidad del dato.

Profundizando en esta cuestión requiriendo el pase de programas software y algoritmos de procesos de los que los datos fueran objeto, incorporándose a esta inspección y auditoría el examen de los sistemas de transmisión y acceso a los datos.

En aplicación de la *regulación (EC) No 45/2001* en el contexto de las transferencias internacionales de datos personales, y bajo el amparo del los *art. 25* y *26* de la directiva *D 95/46/CE* y que se asiste a las condiciones de su cumplimiento conforme a su *art. 9*, el *EDPS*[68] deberá ser consultado de acuerdo

67 ARTICLE 29 DATA PROTECTION WORKING PARTY WP 155, 154, 153, 107 y 74

68 Es una autoridad de supervisión independiente dedicada a la protección de los datos personales y su privacidad y que promueve sus buenas prácticas en las instituciones de la Unión Europea. Entre sus tareas tiene las de monitorizar el procesado de dichos datos en el seno de las Administraciones , el consejo sobre políticas y legislación que afectan a la Privacidad, así como la cooperación con autoridades análogas . Es una figura creada en el año 2001

al *art. 28.2* de la ley.

En concreto al citado *art. 9* se aplica en las transferencias de datos personales[69] que no pertenezcan a la Unión Europea y que no se encuentran sujetos a la Directiva

Siempre que la Comisión contemple de forma adecuada el entorno de la transferencia de datos el Controlador no se encuentra obligado a informar al EDPS. Sin embargo, y en respuesta al *art. 25.4 de la Directiv*a y dentro del marco de trabajo de monitorización y supervisión que le compete por el *art. 9.5* puede este decidir, esto es, el *EDPS* la solicitud oportuna de información por parte del Controller sobre un caso fundamentado.

Por otra parte, los Controladores se encuentran obligados a remitir consultas en los siguientes términos:

> a) como consecuencia de innovación y complejidad incorporada o bien a resultas de su propia institución
>
> b) se prevea una claro impacto en los derechos de los afectados y debido a los riesgos observados

Recordemos que el Controller de no existir legislación hábil en torno a una determinada transferencia deberá adoptar salvaguardas técnicas a fin de proporcionar protección a los datos personales transferibles, siendo ejemplo de estas medidas de seguridad las BCRs y que no trabaja sino la protección suficiente del dato en su destino. Por lo tanto y de momento, no han de responder a ningún formato concreto y pudiendo resultar tanto como parte de un contrato como una declaración

69 *EDPS position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies,14 July 2014*: el término transferencia de datos personales no encuentra definición legal, ni en la Directiva D 95/46/CE ni en la Regulación (EC) No 45/2001, de modo que el término ha sido utilizado en relación al flujo de datos entre Estados miembros y/o sus instituciones y que se encuentran bajo el amparo de la Directiva; el concepto transferencia internacional de datos es usado en su contexto natural cuando nos referimos a que el dato se mueve o se permita que se transmita entre diferentes usuarios. El EDPS , por su parte, ha realizado una petición ante la reforma prevista en la Protección de Datos a fin de subsanar esta negligencia que por otra parte tan sólo ha sido discutida en el *caso Lindqvist* y que defiende que no se está produciendo transferencias de datos a un tercer país en el sentido reconocido por el art. 25 de D 95/46/CE cuando un individuo de un Estado Miembro carga a unos datos en página web con su servidor localizado en dicho Estado Miembro u otro.
Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf

vinculante.

3.4.- El Promotor o Sponsor[70]

Fundamentalmente se encuentran las siguientes definiciones,

- Responsable del inicio, gestión o financiación de un ensayo clínico

- Responsable de la elección de la figura intermediaria entre él y el investigador principal cuando ambos no concurren en idéntica persona. Concurra o no dicha personalidad siempre habrá de perseguir el fomento de la investigación

- Responsable de la elección de una posible organización de investigación, participante por contrato a terceras partes

- Responsable de las instalaciones

- Responsable de la emisión del beneficio potencial pactado debido a los prejuicios experimentados

- Responsable de la puesta en conocimiento en el Ministerio Fiscal de aquellas autorizaciones de ensayos clínicos que incluyera población de menores

- Responsable de la contratación del *Seguro de Responsabilidad* que cubra la responsabilidad de todo el equipo que participara en la actividad. Cabe la posibilidad de la no existencia de dicho seguro con lo que la responsabilidad se denomina 'solidaria' admitiendo responsabilidad de la carga de prueba

70 CPMP/ICH/135/95. July 2002. 4.2.8. (pag. 21): <<el promotor o sponsor es el responsable del aseguramiento del plan de calidad, y de los sistemas de control de calidad, y que tanto los datos, como la documentación se genera de acuerdo a como se ha estimado en el protoclo y clausulas del contrato. Así mismo, es el sponsor el responsable del acuerdo de seguridad que establece el acceso directo tanto a las localizaciones, datos, documentos. Informes justificantes de la monitorización y auditoría tanto interna como externa>>

- Responsable del aseguramiento del Plan de Calidad y de los Sistemas de Control de Calidad, y que tanto los datos como la documentación que se genere sea de acuerdo a como se ha estimado en el protocolo y clausulas legales del contrato

- Emisor de la solicitud simultánea o no de cada uno de los tres centros responsables de un dictamen favorable bien por parte del *Comité Ético de Investigación Clínica*, de las direcciones de cada uno de los centros donde se realizara el ensayo y de la Agencia Española de Medicamentos y Productos Sanitarios. En ocasiones resultará conveniente la solicitud revisada por parte de

  la Comunidad Autónoma[71] Algunas Comunidades Autónomas poseen modelos propios a utilizar por los centros

- En caso de reacciones adversas o inesperadas en un ensayo clínico, responsable de poner en conocimiento, en los plazos establecidos por la legislación, a las entidades anteriormente indicadas. La información comunicada a tales entidades deberán incluir la clausula de contener datos disociados

- Responsable de la adhesión a un determinado *Código Tipo,* recordando que un Código Tipo no entra en vigor hasta el momento en que se realiza su registro en la Agencia de Protección de Datos[72]

3.5.- El Monitor[73]

Se recuerda que se trata de una figura intermediaria entre el investigador principal seleccionado por el promotor y este mismo, de manera que, oportunamente, ejercerá de puente entre ambos , sirviendo de garantía en las actividades de visitas, protocolo, información adecuada entre participantes,

71 RD 223/2004, , de 6 de febrero, por el que se regulan los ensayos clínicos con medicamentos. Cap. III (art. 9, 11, 12, 13 y 14). Vigente hasta el 18 de septiembre de 2011, fecha de entrada en vigor del Real Decreto 1276/2011, de 16 de septiembre, de adaptación normativa a la Convención Internacional sobre los derechos de las personas con discapacidad.

72 Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/elaboracion_codigos_tipo/index-ides-idphp.php

73 RD 223/2004, por el que se regulan los ensayos clínicos con medicamentos, (art.1, art.36)

garantía de las instalaciones y legalismo en la selección de investigadores, seguimiento del protocolo y análisis de los consentimientos informados.

En cualquier caso, la función de monitorización puede ser una función delegada a una organización externa en modalidad de outsourcing.

La delegación de tal función implica la verificación y exactitud de los datos manejados sin participar en la decisión de la finalidad de los mismos, sin implicar recogida o registro por su parte de la información.

El monitor participa, de hecho, en lo que se conoce como 'vista previa' dentro de sus funciones de visualización acerca de la idoneidad del centro donde se desarrolla la actividad.

3.6.- Organizaciones de Investigación por Contrato, Contract Research Organization o CRO[74]

Empresa contratada por outsourcing para representar determinadas funciones del promotor como bien puede resultar ser el monitoreo, contemplándose la posibilidad de manejo tan sólo de datos disociados, tal y como le compete al promotor. Pudiéndose darse el caso de contemplar el caso de un monitor interno y un monitor externo.

Desde el punto de vista de la protección de datos, no le compete responsabilidad alguna.

3.7.- El Investigador

Las funciones deberán ser las mismas que las del *Promotor*. Deberá asegurarse de que todas las personas participantes en el ensayo clínico se encuentran adecuadamente informadas acerca del protocolo subscrito, el producto investigador y / o bien las tareas o funciones con las que se le relacionan.

En el inicio de la investigación debería 'escribir' una *Opinión Favorable* acerca de los *consentimientos informados* que se van a producir, esto es, de los formatos que se van a presentar, así

74 RD 223/2004, por el que se regulan los ensayos clínicos con medicamentos, (art.36)

como por cada revisión o modificación que se produjera y fuera relevante para el consentimiento informado.

Va a ser el investigador el que comunique a la institución la decisión de no continuar con el ensayo bien sea por una falta de acuerdo con el promotor o por haber llegado con él a un mutuo acuerdo, proporcionando una adecuada explicación del caso. Así mismo, y conforme a la legalidad deberá comunicar sus decisiones regularmente al *Comité Ético de Investigaciones Clínicas*.

La necesidad de retención del historial clínico a la finalización del mismo será comunicado a la institución en modo escrito.

Por su parte, el *Comité Ético de Investigación Clínica* o *CEIC* es el Responsable de la emisión de la emisión del dictamen sobre el protocolo.

3.8.- El Auditor

Figura reconocida tanto a nivel externo oficial o contratada a terceras partes, como interna a la institución y que permite emitir una valoración del grado de cumplimiento de la legislación en materia de protección de datos, o de las salvaguardas técnicas a fin de proteger los sistemas de información

3.9.- El Comité Ético de Investigación Clínica[75], CEIC

Por medio de un *Dictamen* sobre el protocolo de ensayo, la idoneidad de los investigadores y la adecuación de las instalaciones, así como de los métodos y los documentos que vayan a utilizarse para informar a los sujetos del ensayo con el fin de recabar su consentimiento informado, esta organización independiente , constituido por profesionales sanitarios y no sanitarios es la encargada de velar por la protección de los derechos, seguridad y bienestar de los ciudadanos que participen en un ensayo clínico, ofreciendo garantía pública.

75 RD 223/2004, por el que se regulan los ensayos clínicos con medicamentos, art.2 Definiciones y Cap.III De los Comités Éticos de Investigación Clínica

Una expresión más correcta sería precisar que el ensayo clínico solo podrá ser iniciado cuando se hubieran considerado que los beneficios esperados tanto para el sujeto como para la Sociedad justifican sus riesgos.

En relación al consentimiento informado de los participantes deberá respetar el conjunto de recomendaciones europeas al respecto. A fin de que los diferentes Comités Éticos de las Comunidades Autónomas puedan compartir estándares de calidad y criterios de evaluación homogéneos en la obtención del citado Dictamen, se crea el *Centro Coordinador de los Comités Éticos de Investigación Clínica* adscrito al Ministerio *de Sanidad y Consumo.*

Cuando participaran dos o más Centros ubicados en España, se emitirá un único Dictamen independientemente del número de Comités Éticos de Investigación Clínica Implicados.

En cualquier caso, la recabación del consentimiento informado del ciudadano deberá ser libre y voluntaria , así como el tratamiento , comunicación y cesión de los datos de carácter personal deberá ser expresada en dicho consentimiento amparándose en la Ley de Protección de Datos vigente, a fin de reconocer sus Derechos ARCO.

Por su parte, el *Centro Coordinador de los Comités Éticos de Investigación Clínica* será responsable tanto de gestionar la Base de Datos de Ensayos Clínicos de la red Nacional de Comités Éticos de Investigación Clínica como de coordinar con las Comunidades Autónomas el desarrollo de un sistema informático de comunicación entre Comités Éticos de Investigación Clínica.

3.10.- La Agencia Española del Medicamento y Productos Sanitarios[76]

Creada mediante *Real Decreto 1275/2011*, encuentra entre sus principales funciones:

- Organizar, coordinar e impartir docencia, promover y realizar proyectos de investigación y proporcionar asesoría científica y técnica, en todos los campos

76 AEMPS, Disponible en:http://www.aemps.gob.es/laAEMPS/portada/home.htm

que le son propios

- Identificar, evaluar y gestionar los riesgos derivados de los medicamentos autorizados, así como coordinar el *Sistema Español de Farmacovigilancia de medicamentos de uso humano y veterinario*, y participar en las correspondientes redes europeas. Actuar como centro nacional de referencia en materia de farmacovigilancia

- Actuar como Organismo Notificado, evaluando la conformidad de los productos sanitarios, realizando las auditorías de los sistemas de calidad, certificando las normas específicas de dichos sistemas y emitiendo los certificados CE con vistas a la colocación del marcado CE en dichos productos

- Realizar la inscripción de autorizaciones y el mantenimiento y actualización de las mismas en el Registro de Medicamentos, así como asignar el Código Nacional a los medicamentos de uso humano y veterinario

- Evaluar, autorizar, modificar, renovar, restringir, suspender o revocar la autorización de comercialización de los medicamentos de uso humano y veterinario elaborados industrialmente

La *Ley 29/2006*, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios, encomienda a la Agencia la realización de los informes de utilidad terapéutica de los medicamentos, emitido por el Director de la Agencia.

Todo el personal al servicio de la Agencia, así como, los expertos y miembros de Comités mantendrán la confidencialidad, incluso después de haber cesado en sus funciones.

El *Real Decreto 1164/2002*, de 8 de noviembre, por el que se regula la conservación del patrimonio

documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original, establece que aunque en todos los departamentos ministeriales se creará una *Comisión Calificadora de Documentos Administrativos* en la que estarán representados los correspondientes organismos públicos, a no ser que tengan su propia comisión calificadora, es en este caso cuando cobra mayor importancia la creación de dicha Comisión conforme consta en la *Orden SPI/341/2011*, debido al considerable volumen de documentos administrativos que genera.

Dicha Comisión Calificadora fundamentalmente:

- Impulsará la automatización de los diferentes archivos de la Agencia y velar por el correcto uso, conservación y consecución de los documentos administrativos en soporte distinto al original

- Propondrá criterios sobre el régimen de acceso a los expedientes, documentos y series documentales conservados

Ejemplo de *Ficheros* de los que es responsable lo encontramos en la *Orden SSI/130/2013* por la que se regulan los 'ficheros' con datos de carácter personal gestionados por el Ministerio de Sanidad y Consumo ante los que deberá a adoptará medidas de gestión y organización que sean necesarias, asegurando, la confidencialidad, seguridad e integridad de los datos, así como las vigilancias oportunas en materia de protección de datos :

a) CERTIFICADOS DE VIAJEROS, en el marco del tratamiento internacional. Se le aplica Medidas de seguridad con indicación de nivel Alto

b) ATENCIÓN E INFORMACIÓN AL CIUDADANO, siendo destinataria la *AEMPS* en Gestión integral de las consultas, quejas y sugerencias realizadas por cualquier ciudadano. e le aplica Medidas de seguridad con indicación de nivel Bajo

En el marco Europeo encuentra su analogía y soporte en la *Agencia Europea de Medicamentos, EMA* , fundamentándose sus procedimientos y requerimientos en las provisiones de la directiva *Directiva 2001/83/EC* y en la *Regulación (EC) No 726/2004* además de las ordenanzas en áreas específicas: orfandad, productos destinados exclusivamente a niños y productos de terapias avanzadas.

En relación a los Sistemas Informáticos el art. 41 del *RD 223/2004*, por el que se regulan los ensayos clínicos con medicamentos, establece que La *Agencia Española de Medicamentos y Productos Sanitarios* se responsabilizará de la inclusión en la base de datos europea de ensayos clínicos EUDRACT de los datos relativos a los ensayos clínicos que se lleven a cabo en el territorio nacional, de acuerdo con lo establecido en las instrucciones para la realización de ensayos clínicos en España o, en su caso, las directrices de la Comisión Europea, que publicará el Ministerio de Sanidad y Consumo.

3.11.- El Asistente en e-Sanidad[77]

Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de este como instrumento fundamental para sus adecuadas asistencias.

De modo , que no será factible que los facultativos no relacionados con la actividad preventiva y diagnóstica de un determinado paciente pueda acceder a los datos. Aplicándosele al personal sanitario un *Nivel de Seguridad Básico* conforme a la Ley de Protección de Datos.

3.12.- El Perito[78]

De idéntica manera que cada ciudadano tiene derecho a no verse sometido a una decisión con efectos jurídicos, sobre ellos o que afecte de manera significativa , que se base únicamente en un tratamiento de datos destinados a evaluar aspectos de su personalidad en correspondencia con el *Derecho de*

77 Responsabilidad de los ficheros en una sociedad médica. Informe 253/2006

78 Ley de Enjuiciamiento Civil. L 1/2000, (art. 99, art. 100, art. 105, art. 124-128, art.159, art.169, art.183, Sección Quinta Completa)

impugnación de Valoraciones valorado en el art. 13 de la Ley Orgánica 15/1999, pudiendo impugnar aquellos actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad, y recordando que la valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado, el ejercicio del *Perito* resulta del todo Voluntario, aun cuando necesario en la Exposición de la Prueba en los Procesos Civiles.

Acerca de la Condición de los Peritos , el *art. 340* de la *Ley de Enjuiciamiento Civil* tan sólo cita la siguiente clausula:

1. Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias.

2. Podrá asimismo solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondiente al objeto de la pericia. También podrán emitir dictamen sobre cuestiones especificas las personas jurídicas habilitadas para ello.

3. En los casos del apartado anterior, la institución a la que se encargue el dictamen expresará a la mayor brevedad qué persona o personas se encargarán directamente de prepararlo, a las que se exigirá el juramento o promesa previsto en el apartado segundo del *art. 335*

4.- Sistemas Informáticos Europeos

Se van a representar aquellos sistemas informáticos desde los que actualmente debemos considerar la Protección de Datos orientada hacia la *Seguridad del Paciente*. Aun no queriendo practicar una observación dividida de ambos lados del Océano Atlántico, debido a la cercanía de su influencia, nos

vemos obligados a citar lo que públicamente es conocido y comparado.

4.1 Ficheros

4.2. Sistemas Biométricos

- 4.2.1. Vía Aérea
- 4.2.2. Vía Marítima
- 4.2.3. Protección de Menores
- 4.2.4. Espacio Supranacional: EURODAC, VIS, SIS
- 4.2.5. Tratado de Prum o Bases de Datos de ADN

4.3. Sistemas de Alertas Alimentarios

4.4. El Mercado Interior, IMI

4.5. El Sistema Europeo de Alerta y Respuesta Temprana, EWRS

4.6. El Sistema de la Historia Clínica en el Sistema Nacional de Sanidad, SNS

4.7. El Sistema de Mutuas y Aseguradoras

4.8. Farmacovigilancia e Investigación Clínica

4.9. Soportes

- 4.9.1. ISO/IEC 27 002
- 4.9.2 Desarrollo Esquema Nacional de Seguridad: RD 04/2010 y RD 03/2010

Las nuevas tecnologías permiten oportunidades de mejora, eficiencia y reducción de costes, que hacen ineludible la consideración de las formas de tramitación electrónica, tanto para la tramitación de expedientes, como para cualquier otra actuación interna de la Administración.

En concordancia con el *art. 18.4 CE*, se encomienda la limitación del uso de la informática para preservar el ejercicio de los derechos constitucionales.

En relación a las Copias electrónicas el *art. 30* nos recuerda en su apartado tres que las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

La sección i) del apartado 4 establece el 'Principio de neutralidad tecnológica y de adaptabilidad' al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos y por las Administraciones Públicas,

así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán *estándares abiertos* así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

En el Capítulo II se postula la utilización de medios electrónicos en la tramitación del procedimiento del *art. 35* por iniciación del procedimiento por medios electrónicos. Así mismo, la iniciación de un procedimiento administrativo a solicitud de interesado por medios electrónicos requerirá la puesta a disposición de los interesados de los correspondientes modelos o sistemas electrónicos de solicitud en la sede electrónica que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares en los términos establecidos en el apartado i) del artículo 4 y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.

El *Esquema Nacional de Interoperabilidad* y *Esquema Nacional de Seguridad* retomado en el *art. 42* de la Ley L 11/2007 sugiere que la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, estándares abiertos y estándares internacionales reconocidos, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes.

Los empleados públicos de la Administración General del Estado recibirán formación específica que garantice conocimientos actualizados de las condiciones de seguridad de la utilización de medios electrónicos en la actividad administrativa, así como de protección de los datos de carácter personal, respeto a la propiedad intelectual e industrial y gestión de la información.

En relación a las certificaciones electrónicas inicialmente, conviene recordar que fue el protocolo SET[79] el que se constituye como el primer proyecto de certificación a escala global que se va a

79 La norma de calidad aplicable **ISO-9126** dirijida a producto puede conducirnos a la elaboración de una *métrica* adecuada a automatizaciones y evaluaciones de "enlaces rotos" en la aplicación , caracterizándose a nivel de protección de datos porque cada parte involucrada en la transacción precisa de un certificado digital, y manteniendo una criptología asimétrica a diferencia del protocolo más socialmente conocido como el SSL. En febrero de 1996 VISA International, Microsoft, IBM, Netscape y Verisign entre otras grandes compañias anuncian la creación de SETCo, una empresa cuyo objetivo sería la creación de un sistema seguro y universal de pago electrónico a través de Internet. La primera implementación y las especificaciones finales del mismo verían la luz en la segunda mitad de 1997 En la actualidad el protocolo mayormente extendido es el SSL, Secure Sockets Layer, ligado en su creación a la empresa "Netscape". Este protocolo falla fundamentalmente en dos de los pilares sobre la que se asienta la ciencia de la Criptología: la Integridad y el No-Repudio, resueltos teóricamente en un nuevo protocolo, denominado SET, Secure Electronic Transactions, que permitiría la globalización de este intercambio de datos.

Arquitectura del Protocolo de Comunicaciones Set. Disponible en: http://www.ietf.org/rfc/rfc3538.txt?number=3538

realizar. Hablar de una relación Root, CA-Brand, CA-Geopolitica y CA[80] es definir toda una estructura de autoridades que posibilitan que la certificación digital mundial pueda mantenerse propiedad de las entidades emisoras de tarjetas de crédito, entre las que destacan las pertenecientes a "Visa Internacional" y "MasterCard Internacional", auténticas propulsoras del SET. A su vez estas entidades son certificadas por la Autoridad Certificadora Raíz por medio de una petición en un archivo estándar, el PKCS#107. En el caso de que fuera aprobada la solicitud se genera otro archivo de respuesta, denominado PKCS#7 en forma de remite.

Las autoridades de certificación de marca de Autoridades de Certificación Geopolítica o *CA-Geopolítica* son los responsables de emitir la generación de archivos de certificados revocados; una vez confeccionados estos archivos serán distribuidos, cada uno, como CRL. Un ejemplo de entidad de este tipo es la "*ACE*, Agencia de Certificación Española". Se constituyó en 1997 y está formada por el Grupo Telefónica (40%), SERMAPA-Visa España (20%), CECA(20%) y Sistema 4B (20%). Su misión principal es dar respuesta a las necesidades derivadas de la implementación de protocolos seguros para transacciones por Internet por medio de la emisión de certificados electrónicos.

Este tipo de autoridades de certificación final se encargan de emitir los certificados a los usuarios finales del sistema, clientes, vendedores y pasarelas de pago. Además, se precisa de un proceso de autenticación de los datos que en él van a figurar. Esta verificación de datos corresponde a unas entidades creadas al efecto, que se denominan *Autoridades de Registro*. Típicamente, son los propios bancos, permitiendo con ello que los certificados estén asociados a cuentas bancarias y no a personas físicas.

Sus principales misiones son validar solicitudes de certificado en base a determinados procedimientos de identificación según el tipo, solicitar luego el correspondiente certificado a la Autoridad Certificadora y entregar el mismo, una vez obtenido, al usuario final del mismo, usando para ello un disquete u otro soporte adecuado. Un vendedor debe tener al menos dos pares de claves (cifrado y firma) para participar en las transacciones . Además, un vendedor debería tener varios conjuntos de claves de cifrado y firma debido a implementaciones físicas, de seguridad, política de adquisidores, etc.

80 Agencia de Certificación Electrónica, ACE. Disponible en: http://www.ace.es

Por ejemplo, un vendedor que opere en múltiples servidores puede elegir tener un conjunto de pares de clave de cifrado y firma para cada servidor. Se deben generar nuevos pares de claves periódicamente. El número de certificados necesitados por un vendedor está en función del número de pares de claves de cifrado y firma, y el número de marcas que le afectan.

Existen también una variedad de motivos que influyen en el número de pasarelas de pago con las que el vendedor debe intermediar.

Un vendedor debe tener relaciones con múltiples bancos adquisidores. No podrá procesar todas las marcas que el vendedor acepta. Además, existe otro factor: los bancos adquisidores podrán elegir operar con múltiples pasarelas para equilibrar la carga.

4.1.- Ficheros y Soportes Lógicos

La situación maestra surge cuando se acoge una demanda desde la Agencia Tributaria al amparo de la Ley de Protección de Datos y su Reglamento de Desarrollo RD 1720/2007 a profesionales sanitarios en relación a documentación clínica como puede tratarse de los consentimientos informados o la historia clínica con fines de inspección.

No vamos a entrar en consideración al respecto de la falta o no de procedimientos de verificación, por parte de la Agencia Tributaria, de cumplimiento del buen expediente tan útil, por otra parte, en épocas categorizadas como de crisis. Pero sí revisaremos los principios sobre los que produce su actuación en materia de protección de datos. Respetando, en cualquier caso siempre la separación entre la defensa de unos derechos y sus mecanismos de protección.

Los datos anteriormente mencionados tendrán la consideración de *datos de salud* de conformidad con la definición contenida en el art. 5.1 .g) según el cual serán datos de carácter personal relacionados con la salud "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se considerarán datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética."

Conforme al esquema presentado en la Tesis los datos relacionados con la discapacidad ya mencionados recibirán el soporte añadido de la perspectiva que permite la exposición y transcurso de los datos genéticos y la historia clínica relacionada con la radiación nuclear.

Los art. 6 y 11 de la Ley Orgánica 15/1999, encuentran por vía de excepción particulares restricciones en el art. 7 de la citada Ley Orgánica, cuyo apartado 3 establece como regla general que "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".

Resulta ejemplo manifiesto de lo que se expone el *Informe 0242/2010* emitido por la Agencia de Protección de Datos y orientado a la Hacienda Tributaria de Navarra.

Así como un dato aislado puede perder su validez informativa, idénticamente puede resultar erróneo, en cuyo caso se podrían vulnerar los siguientes derechos:

- el de igualdad
- el de la intimidad
- el de asociación o el de educación
- el de acceso a un empleo
- el derecho a obtener una prestación de la Seguridad Social

En buena práctica los legisladores se pueden preguntar si el derecho a la intimidad encuentra tanto desarrollo como para albergar el derecho a la protección de datos o este segundo derecho debe interpretarse independientemente del primeramente mencionado: la cuestión parece no resolver de momento la dicotomía de lo que se puede considerar como un derecho fundamental y la protección que todo ciudadano merece respecto del uso de la Informática. Aunque bien pudiera parecer que esta interpretación frenara el desarrollo dogmático, a la luz de la nueva *Ley de Transparencia L 19/2013* encontramos reconocido que el derecho de acceso de los ciudadanos a la información publica se encuentra recogido como derecho fundamental según el art. 42 de la Carta de Derechos Fundamentales.

La derogada LORTAD ya recogía la excepción de tener que contar con la aprobación del Director de la Agencia de Protección de Datos en el intercambio de datos médicos entre facultativos o instituciones sanitarias , si es en beneficio del tratamiento del afectado o en investigaciones epidemiológicas.

No solicitar la inscripción del fichero de datos de carácter personal en el *Registro de Protección de Datos*, cuando no sea constitutivo de infracción grave será considerado como infracción leve. Así mismo, no atender a una notificación de inclusión en un fichero será considerada infracción grave.

Cuando las infracciones se producen en las Administraciones Públicas, el Director de la Agencia dictará una resolución donde se indicarán las medidas que hay que adoptar para que cesen o se corrigieran los efectos negativos. Podrá proponer medidas disciplinarias , comunicando en su caso, al *Defensor del Pueblo* aquellas actuaciones y resoluciones efectuadas.

El *Registro General de Protección de Datos* responde al *art.39* LOPD en su objeto de inscripción a los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.
Es precisamente a la Agencia de Protección de Datos a la que le corresponde el control de datos nacionales del *Sistema de Información Schengen, SIS*, conforme al *art. 10.* en colaboración con las Fuerzas Armadas, *art. 22*.

Debido a las funciones de Inspección de Datos, *art. 27 a 29 EAP*, esta sección de la Agencia de Protección de Datos realizará auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la Ley. A su vez, el responsable del fichero estará obligado a permitir el acceso a los locales en los que se hallen los ficheros y los equipos informáticos previa exhibición por el funcionario. Cuando dichos locales tuvieran la consideración legal de domicilio, la labor inspectora deberá ajustarse a los principios de intimidad e inviolabilidad.

Respecto del tratamiento de ficheros La Agencia de Protección de Datos conforme a su reglamento Real Decreto 428/1993 y al amparo de *art. 34.1* de la LORTAD se constituye por el Director de la Agencia, un Consejo Consultivo, el Registro General de Protección de Datos, la Inspección de Datos y una Secretaría General.

En relación a los ficheros el Director de la Agencia puede:

- requerir a los ficheros de titularidad privada a que subsanen deficiencias de los Códigos Tipo

- decidir sobre la procedencia o improcedencia de las inscripciones que se deban realizar en el Registro autorizando la entrada en los locales en los que se hallen los ficheros, con el fin de proceder a las inspecciones pertinentes, sin perjuicio de la aplicación de las reglas que garantizan la inviolabilidad del domicilio.

En relación al *Documento de Seguridad* y la Creación de un Fichero bien de titularidad pública o privado se pueden observar los siguientes términos:

- El RLOPD 1720/2007 en relación a las Medidas de Seguridad que sustituye al 994/1999, coincide en señalar que los ficheros de tratamiento con datos de 'salud' exigen una aplicación de Nivel Alto , y aquellos relativos a la comisión de infracciones administrativas o penales a un Nivel Medio, idéntica calificación para los datos de Mutuas, accidentes de trabajo y enfermedades profesionales de la Seguridad Social, y de Entidades Gestoras y de Servicios Comunes y los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización. Recordar que existe una aplicabilidad de Nivel Básico: en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de Discapacidad o la simple Declaración de Invalidez. Se aplicará idénticamente un fichero de nivel alto, para actos derivados de actos de violencia de género

- *existirá un responsable de Seguridad del Fichero cuyas* funciones serán las de coordinar y controlar las funciones embebidas definidas en el Documento sirviendo al mismo tiempo de enlace con el responsable del Fichero, sin que esto suponga una delegación de la responsabilidad que corresponde a este último

- se puede encontrar un documento por cada fichero que requiera de tratamiento, con la posibilidad de refundición en uno único si existieran dos de un mismo

organismo pero pertenecientes a diferentes centros.

- En el 'Documento de Seguridad' se deberá indicar una especificación por cada fichero no automatizado que existiera, así como el Nivel de Seguridad que se le otorgue a cada uno.

- En el caso de la especificación de los controles de acceso la Agencia de Protección de Datos nos sugiere que no resulta obligatorio especificarlo en dicho Documento cuando se trata de una única persona a la que se le permite dicho acceso .

- *Los recursos que por servir de medio directo o indirecto se utilizaran para acceder al Fichero,* deberán ser controlados por esta normativa
- *los centros de tratamiento y locales donde se encuentran ubicados sus ficheros o se* almacenaren los soportes que los contengan

- *los puestos de trabajo, bien locales remotos, desde los que se puede tener acceso al* fichero

- *los servidores, si los hubiese, y el entorno del sistema operativo y de comunicaciones* en el que se encuentra el fichero

- *el administrador del sistema, que mantiene el entorno operativo del Fichero, que pueden* utilizar herramientas de administración que permitan el acceso a los datos protegidos, saltándose las barreras de acceso a la aplicación

- *Usuarios del Fichero: o personal que utiliza el sistema informático de acceso al fichero*

- *Además del personal citado existirá un responsable de Seguridad del Fichero cuyas* funciones serán las de coordinar y controlar las funciones embebidas definidas en el Documento sirviendo al mismo tiempo de enlace con el responsable del Fichero, sin que esto suponga una delegación de la

responsabilidad que corresponde a este último

- *Los administradores del sistema deberán además atenerse a aquellas normas de Tratamiento* de los Respaldos de Seguridad , Normas de Altas de Usuarios y Contraseñas , obligando al cumplimiento en la unidad administrativa a la que pertenece el Fichero.

- *Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una* configuración fija en sus aplicaciones , sistemas operativos que solo podrá ser cambiada bajo la autorización del responsable de seguridad o por administradores autorizados

- El caso contrario, la salida de dichos archivos de un local deberá constar de forma explícita por Procedimiento en el Documento siempre bajo supervisión del responsable del tratamiento. Este tipo de especificación se hará extensible a los accesos a datos de carácter personal a través de Redes de Telecomunicaciones (públicas o no).

- Si se ha contratado la prestación de servicios con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento, se podrá delegar en este '*la llevanza del documento de seguridad*' . *En el contrato celebrado al amparo del a.12 LOPD con especificación de los ficheros* trasladados, el *art.88* se refiere a la delegación de dicha llevanza

- Un proceso de recuperación de datos de carga deberá venir siempre con firma escrita o digital por su responsable. En Niveles Altos, las copias de respaldo y recuperación se realizará como mínimo, cada semana, siendo el responsable del fichero el que verificará semestralmente dichos procedimientos.

  La utilización, validación y conservación de los ficheros de acuse de recibo están contemplados por Orden 3523/2009 de la Agencia Nacional de Datos, persiguiendo un modelo análogo al funcionamiento de Registro Electrónico Común

- Un Informe de Auditoría debe ser emitido por el responsable de seguridad que , a su vez, deberá ser entregado al responsable del fichero y que mediante esta figura quedará a disposición de la Agencia de Protección de Datos o Autoridad de Control de la Comunidad Autónoma

- Se habrá de indicar la relación con otros ficheros proporcionando la ruta especifica en la denominada 'Gestión de la Configuración de Ficheros'

- *En relación al envío de ficheros con datos de carácter personal por e-mail o fax viene* regulada por el *art.92* del Reglamento y debiera ser estudiado por el responsable del sistema y/o de seguridad en función de cómo vaya a repercutir en el reglamento de incidencias, indicándose en cualquier caso en el Documento de Seguridad. El *art.97* exige para un Nivel Medio el conocimiento de la información de envío, y en un Nivel Alto*, art. 101* , el cifrado de los datos

- En relación a las incidencias y entendiendo por 'incidencia' a cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del fichero, entendido bajo sus vertientes de confidencialidad, integridad y disponibilidad de los datos, Las manipulaciones que hayan debido realizarse para dichas recuperaciones deberá dejarse en el registro de incidencias, incluyendo la persona que realizó el proceso y los datos restaurados.

Quedando expresamente prohibida la conexión a redes bajo sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero, quedando constancia de esta modificación en el libro de incidencias y, manteniendo, en cualquier caso, las incidencias registradas de los últimos doce meses restaurados. La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de una *disposición general* publicada en el Boletín Oficial del Estado, *BOE*[81] de modo que la finalidad y usos previstos deberán citar los siguientes requisitos:

81 LOPD, (a.20.2), RD 15/1999, (a.54)

- denominación del fichero
- descripción de su finalidad
- usos previstos
- origen de datos
- procedimientos de recogida
- estructura básica del fichero
- sistema de tratamiento utilizado en su organización
- las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios
- las trasferencias a terceros países , con indicación de los países de destino
- órgano responsable del fichero
- servicios o unidades ante los que cabe el ejercicio del Derecho ARCO
- indicación del Nivel, de acuerdo con el Título VIII del RDLOP

En las notificaciones telemáticas a la Agencia de Protección de Datos, y en su caso, la historia clínica, que precisa de la firma electrónica la no recepción del mensaje de confirmación constituido como acuse de recibo de la Agencia implica que no se ha producido la recepción del mismo. La inscripción de un fichero en el registro únicamente acredita que se ha cumplido con la obligación de notificación dispuesta.

De la misma manera que no resulta factible la identificación del formato digital de cuantos ficheros necesitaran existir y ser controlados y analizados , idénticamente no podrán ser adoptadas de antemano aquellas medidas de seguridad pertinentes para cada fichero que se precisara registrar.

Por otra parte, la elaboración de los *Informes Periódicos de Seguridad* suele considerarse detonante de recogida de datos ya no tan espontánea.

La historia clínica admite juicios observacionales, informaciones venidas desde terceros, justificantes de pruebas, consentimientos informados y voluntades anticipadas. Además de para el ciudadano, una buena recogida de información incide en el área de la docencia y la investigación, y la mejora de la calidad, esto es, en el buen contenido de la e-Administración.

Este nuevo valor añadido que otorga la plataforma de la e-Administración a la Historia Clínica respalda la función asistencial, docente, de investigación, y legal. A ello se le puede añadir la participación de terceros agentes como son los auditores, los gestores y los sistemas sanitarios.

Cuando el protocolo considere que va a producirse una relación multicéntrico, cada uno de ellos, y salvo que se indique lo contrario, deberá declarar un fichero de investigaciones clínicas .

En el escenario de Farmacovigilancia se habrá de declarar un fichero que recoja todos los 'acontecimientos adversos' que se fueran produciendo.

La comunicación de datos personales cuando se realiza en el seno de una empresa se ha de tener en cuenta si ésta se encuentra en un país con protección equiparable a la española o no, e idénticamente se habrá de observar si dicha trasmisión se realiza dentro del Espacio Económico Europeo. Dichas trasferencias internacionales se realizarán conforme a las políticas internas definidas, siempre pretendiendo el control y seguimiento de dichos datos.

Consideraremos Estados que proporcionan un *nivel adecuado de protección* cuando bien la Comisión Europea a través de sus informes, o bien la Agencia de Protección de Datos por medio de sus resoluciones publicadas en el BOE, los hayan declarados en tales términos.

Se deben considerar parte integrante de este grupo de Empresas a aquellas que hubieran adscrito el 'Acuerdo de Puerto Seguro' que se mantiene en consonancia con las Empresas Estadounidenses, espacio donde dicho campo de investigación se contempla y es tratado con un enfoque bien distinto respecto del europeo. Dicho acuerdo fue ratificado por la Comisión Europea en el año 2000. En

cualquier caso, la trasferencia será comunicada al Registro de Protección de Datos.

La relación de Empresas que cumplen estos requisitos puede ser encontrada en la página web de la Agencia de Protección de Datos.

Aquellos *que no cuentan* con el mencionado nivel adecuado de protección de datos necesitan de la aprobación del Director de la Agencia de Protección de Datos, con las siguientes excepciones: por Convenios donde España aparezca como subscriptora, por auxilio judicial internacional o por asistencia sanitaria y, a petición del sujeto desde un Registro Público. Si existiera consentimiento del afectado será discriminatoria la aprobación de dicho acto por parte del Director de la Agencia de Protección de Datos.

Orientado a dicho supuesto, se contempla la inscripción de la trasferencia internacional en el *Registro General de Protección de Datos*.

La principal pregunta que podemos hacernos es si resulta factible la trasferencia de datos con un propósito diferente del que fuera compilado, cuál es el orden de cosas que deberíamos interpretar, qué exigencias legales se deben respetar y, en su caso, el modo de flexibilizar las situaciones no legisladas. Es en este último punto donde las Agencias de Protección de Datos locales intervienen en mayor medida y fundamentalmente en el tratamiento de países denominados no seguros.

Un caso singularmente interesante lo proponen las compañías de investigación de mercados.

Como competencia de este apartado podemos considerar aquellas situaciones donde el flujo y trasferencia de datos, permitidos o no, se puede producir a lo que se han venido en denominar *terceros países*. Un país es considerado tercer país o *third country* cuando la trasferencia de datos no se produce en el seno de la *Unión Europea* ,*EU,* o a uno perteneciente a su área económica, *EEA*, *European Economic Area*. Idénticamente, recibirá el tratamiento de tercer país aquel que no disponga de un adecuado nivel de protección.

Tradicionalmente, la inclusión de cláusulas era manejado por medio de los *Códigos de Conducta* Internacionales hasta la aparición de las denominadas BCR's[82] o *Binding Corporate Rules.*

82 ARTICLE 29 DATA PROTECTION WORKING PARTY WP 133, WP153, WP 154, WP 155, WP 195

Un caso de transferencia de datos en el seno de la misma multinacional y en sus subdivisiones con o sin la inclusión de clausulas es denominado de *Puerto Seguro*.

En una empresa multinacional y siempre que hayan sido definidas unas Normas Vinculantes entre las Empresas del Grupo, *BCRs*, *Corporate Binding Rules*, el Director de la Agencia permitirá dicha transferencia, aun cuando se produjeran en Estados sin el nivel adecuado de protección de datos.

Cuando fuera requerida la especificación de la declaración completa de datos de carácter personal del encargado de un fichero, y existieran varios encargados del mismo , y no pudiendo ser referidos a la vez por diseño del almacenaje de dicha información se indicará a aquel cuya participación sea más prolongada en el tiempo haciendo referencia, así mismo, a la cantidad de datos tratados.

El proveedor o encargado del tratamiento informará a su personal y colaboradores de las obligaciones establecidas en el contrato sobre confidencialidad; de modo que realizará tantas advertencias y subscribirá documentos con sus colaboradores a fin de asegurar el cumplimiento de sus obligaciones.

Ningún proveedor almacenará los datos en dispositivos portátiles ni los tratará fuera de las instalaciones del laboratorio. Recordemos que puede ser una empresa la subcontratada a efectos de ejercer la figura de *encargada de dicho tratamiento*.

Deberá observarse para cada situación y país invocando precisamente aquellas medidas de salvaguarda que sugiere:

- monitoreo, inspección y funciones conectadas conforme al ejercicio de la autoridad nacional competente

- y la protección de datos y de derechos y libertades de otro

En el *Fichero de Vigilancia* se recogerá aquella información estrictamente necesaria que documento cada acontecimiento adverso, encaminado a obtener la mejor información posible sobre la seguridad del producto involucrado.

Cuando se habla de legislación debemos reunir un todo de leyes, reglas y relaciones que pudieran impedir el desarrollo de un contrato. En concreto se estipula que el importador de datos habrá de responder ante el exportador en relación al procesado de trasferencia.

El caso que se se nos puede presentar es el de solicitud por haberse detectado una enfermedad en un país que no es el de residencia habitual del ciudadano y la correspondiente solicitud de datos estrictamente necesarios de su historia clínica con intervención y acuerdo de las propias autoridades.

En ocasiones nos podemos preguntar donde se encuentra el límite en la razón legítima de publicación acerca de la información que se tiene sobre un determinado paciente.

Aceptando los principios extendidos de elaboración de un artículo de divulgación científico a continuación debe surgir la pregunta reflejo de la inquietud acerca de cómo debe ser preparada dicha información.

Respondiendo a esta cuestión se establece en Vancouver en 1978 el primer encuentro de editores de prensa médica 'The Vancouver Group', siendo sus primeras referencias publicadas en 1979. Esto derivó en el *ICMJE*, *International Committee of Medical Journal Editors*, que reunidos una vez al año recopilan principios éticos relacionados con las publicaciones biomédicas resolviendo la cuestión y conocidos con el nombre de *Uniform Requirements for Manuscripts Submitted to Biomedical Journals*.

Bajo la premisa de tratar de encontrar resueltos estos potenciales conflictos de intereses los propietarios de un medio de comunicación no deberán interferir en la evaluación, selección o edición de artículos individuales bien directamente o bien aportando un entorno que determine dichas decisiones.

Más específicamente la legislación estadounidense delimita la definición de la Historia Clínica o HC en un determinado grupo de dieciocho elementos denominado *PHI*, *Personal Health Information* , indicados a continuación y fuera de cuya definición se estará considerando se está incurriendo en una negligencia en relación a la publicación de datos clínicos o de necesidad de reclamar consentimiento informado al paciente:

1. nombres
2. indicativos de la edad del paciente
3. fechas de nacimiento, de muerte, de admisión
4. números de teléfono
5. números de fax
6. direcciones de correo electrónico
7. números de la seguridad social
8. números del récord médico
9. números beneficiarios del plan de salud
10. números de cuentas
11. números de certificados
12. identificadores de vehículos
13. identificadores de dispositivos y números de serie
14. recursos de localizadores web, o URLs
15. direcciones IP
16. identificadores biométricos
17. imágenes faciales
18. cualquier otro código, o caracterización identificativa

Típicamente no se considerará PHI cuando el dato al que nos referimos no está asociado a algún evento del sistema de servicio médico ni cuando el paciente no fuera precisado para ser informado como consecuencia de él. HIPAA se hace cargo de toda comunicación electrónica mientras que su *Privacy Rule* considera que la comunicación puede ser oral, por fax, o manuscrito. En este punto es donde resulta precisa la introducción de este apartado.

4.2.- Sistemas Biométricos

Una introducción histórica acerca del sistema de reconocimiento de huellas dactilares nos permite repercutir sobre sus principios activos e ir observando el modo en que estos variaron:

1.Sir William Hershel, en 1856, empezó a usar las huellas digitales para validar contratos. Su idea era la de que los comerciantes nativos pusieran la huella de su mano derecha detrás del papel del contrato, para evitar que dijeran que la firma no era suya. Después exigió solamente las huellas del dedo índice y del medio. Herschel comenzó a notar que esas huellas eran únicas para cada persona, pese a ser a un convencimiento individual sin apoyo científico.

2.En 1889, D. Henry Faulds, el superintendente británico en el Hospital Tsukiji en Tokio, continuó el estudio de las huellas para identificar las marcas en cerámica antigua. No sólo vio la importancia de las huellas para identificación sino que, además, propuso un método para clasificarlas. Previamente en 1880, había publicado un artículo en <<Nature>> proponiendo que las huellas eran únicas. Su método fue acreditado al ser capaz de descubrir una huella en un frasco de alcohol.

3.Sir Francis Galton en 1880 comenzó sus observaciones para utilizar las huellas como identificadores personales. En 1892 publicó su libro "Fingerprints" en las que decía que las huellas eran únicas y que no cambiaban a lo largo de la vida. También estableció un sistema de clasificar

las huellas.

4.El primer fichero de huellas digitales lo creó en 1891 el policía argentino Juan Vucentin. Al año siguiente logró identificar mediante las huellas dactilares a una mujer apellidada Rojas como la asesina de sus dos hijos

5.En 1901 policías de Gales e Inglaterra establecieron las huellas digitales como sistema de identificación en los delitos. El sistema se basaba en el sistema de Galton, modificado por Sir Edward Richard Henry. El sistema se extendió por todo el mundo.

6.El sistema judicial estadounidense presenta lo que se llama una "audiencia Daubert". En ella es el juez quien examina si hay base real o no para una pretensión "científica". Para ello el juez analiza cinco cosas de las evidencias:

- La teoría y la técnica es testable
- Se ha sometido a revisiones por pares o ha sido publicado
- Se mantienen normas que controlen el uso de la técnica
- Los científicos generalmente aceptan el trabajo
- Se conoce una tasa de error.

7.Lo sorprendente es que en 1999, los abogados de Byron Mitchell, en un caso de robo, denegaron que las huellas parciales encontradas en el tubo de escape de un coche fueran las de su cliente pidiendo una "Audiencia Daubert". Allí quedó claro que no se conocía la *tasa de error* de los emparejamientos hechos con huellas incompletas.

8.Para solucionar el problema, el Departamento de Justicia de Estados

Unidos encargó al FBI y a la empresa Lockheed Martin un estudio que estableciera una tasa de error. Lo hicieron con la base de datos del FBI y en un resumen público se dice que la probabilidad de que un trozo de huella se empareje incorrectamente con otra es de 1 en 10 elevado a 97. Eso es lo mismo que decir que la probabilidad es cero pues en toda la historia de la humanidad no habrá habido más de 10 elevado a 11 huellas.

9.De idéntica forma y en cuanto a *sistemas de reconocimiento de imágenes*, aunque podemos rastrear los antecedentes fotográficos en un amplio elenco de espectáculos visuales basados en ingenios ópticos, tales como los cosmoramas, dioramas, linterna mágica, fantasmagorías, mundonuevos, etc., puestos de moda en el s. XVIII, lo que nos interesa es centrarnos en el invento fotográfico en sí, cuya paternidad hay que atribuirla por igual a Nicephore Niépce y Louis Jacques Mandé Daguerre

10.Nièpce, en 1826, obtendría la primera fotografía, la célebre 'Vista' desde la ventana, y Daguerre, en 1837, conseguiría un autorretrato, siendo a la postre este autor el que se haría con las niveles del éxito tras una campaña publicitaria francesa de hondo calado en los cenáculos académicos.

11.El 10 de noviembre de 1839 se toma en Barcelona un daguerrotipo, y ocho días después se hará otro en Madrid, extendiéndose por la península e islas en poco más de dos o tres años.

12.Según las estadísticas oficiales, se renuevan 6 millones de documentos al año. La historia que empezó en 1944, cuando durante la dictadura se creó el primer DNI como método de control. De hecho, los primeros en obtenerlo fueron los presos y los que estaban en libertad vigilada. En 1951 se extendió a toda la población. Aquel primer modelo incluía información referente al status social, como la profesión y el cargo desempeñado. A partir de 1985 se descartó la inclusión de datos como la profesión, el grupo sanguíneo o el estado civil. En la década de los 90 se iniciaron las técnicas informáticas en

el diseño del DNI.

Conviene tener siempre muy presente que en los procesos judiciales sólo se contemplan tres tipos de pruebas: testificales, documentales y periciales (el reconocimiento judicial y la confesión del *art. 578* de la Ley de Enjuiciamiento Civil hacen referencia a otros elementos del proceso).

La legislación procesal española es muy antigua. Muchos de sus usos, costumbres y normas se remontan al siglo XIX, cuando ni siquiera existía la fotografía.

El derecho, en ciertos casos, devalúa por completo la prueba fotográfica. Incluso hay ocasiones en las que su uso puede ser contraproducente. Debemos llamar la atención sobre la mayor importancia que tiene el reconocimiento del presunto autor de un delito por parte de un testigo, en una "rueda de reconocimiento", que el que pueda realizarse mediante álbumes de fotografías policiales. Si es una de las partes la que muestra antes de la "rueda de reconocimiento" una fotografía del sospechoso, nuestro ordenamiento jurídico entiende que se ha predispuesto al testigo, y puede invalidar tanto la fotografía que tengamos, como el testimonio de quien haya reconocido al sospechoso. Se han conocido juicios perdidos sólo por este error.

Desde verano del 2002, Estados Unidos toma las huellas digitales y la fotografía de todos los ciudadanos que entran en su territorio procedentes de países exentos de visado. A cambio, ya aceptó prolongar un año el plazo para implantar los pasaportes biométricos, que en un primer momento deberían haberse introducido en octubre de 2004. Este refuerzo de las medidas de seguridad se implantaron a raíz de los atentados del 11 de septiembre de 2001 en Nueva York y Washington.

Actualmente los sistemas de almacenamiento de formato digital junto a los Sistemas de Información a Laboratorios son dos de las Infraestructuras relativas a la e-Sanidad existentes en todos los Centros Públicos Sanitarios.

Esta introducción histórica no debe carecer de la implantación en Telemedicina de la Biometría, aunque bien es cierto que no resulta difícil de resolucionar su comienzo imaginándonos la impartición de clases magistrales de Medicina a los alumnos por medio de Teleconferencia.

Se prevé que cuando se alcance un grado de desarrollo de la televisión interactiva la Telemedicina

obtendrá este mayor impacto en el área Sanitaria.

Actualmente se manejan algunos términos en el área de la e-Health:

- *m-Health,* que incorpora la utilización de dispositivos móviles, no sólo para referirse a la atención a distancia sino a la monitorización en Tiempo Real, y envío y recepción de datos clínicos

- *T-Health*[83], aplicado específicamente a la Telemedicina con precedentes en Inglaterra desde el año 2004 en su televisión digital

Un impulso de la aplicación del *Reglamento Sanitario Internacional, RSI-2005*[84], a fin de adaptar sus servicios como garantes de prueba de las Alarmas que se elevaran, influiría positivamente en el impulso de la Telemedicina.

Con la *Declaración de la Haya* de 2004 se produjo un intento de aliviar los problemas que pudieron surgir del uso de las tecnologías biométricas, proporcionando puntos de entrada en materia de seguridad y privacidad.

Se habla de los siguientes métodos de autentificación biométrica:

- la *verificación*: una muestra se chequea contra otra en los controles de acceso

- la *identificación*: la muestra se coteja frente a un conjunto usado en listados de identificación

En cuanto a los dispositivos biométricos podemos distinguir los siguientes:

83 SAINZ DE ABAJO, Beatriz , J.P.C.RODRIGUEZ, Joel , GARCIA SALCINES, Enrique , BURON FERNANDEZ, F.Javier, CORONADO Miguel ,DE CASTRO LOZANO, Carlos. "M-Health y T-Health. La Evolución Natural del E-Health" . Revista e-Salud.com. Vol 7, No 25. Dsiponible en: http://dialnet.unirioja.es/servlet/revista?codigo=14656

84 Organización Mundial de la Salud. Reglamento Sanitario Internacional. 2005 . Segunda Edición. Ginebra 2008 „El reglamento sanitario internacional , RSI o reglamento, fue adaptado por la Asamblea de la Salud en 1969, con el precedente de reglamento Sanitario Internacional, *International Sanitary Regulations*, adoptado por la cuarta asamblea mundial de la Salud. El RSI de 2005 fue adoptado por la 58º asamblea mundial de la salud el 23 de mayo de 2005 y entró en vigor el 15 de junio de 2007". Disponible en: http://www.who.int/ihr/es/index.html

- el *sensor,* que traduce la característica biométrica a una plantilla o template
- el *almacén*:, típicamente una Base de Datos
- el *algoritmo lógico*: que decide positiva o negativamente la verificación o identificación de una muestra
- el *software,* que integra todas estas funciones y permite el intercambio de sistemas

Legalmente, según la *Ley 15/99 de Protección de Datos Personales,* no es posible que una tarjeta electrónica (ya sea pasaporte, visado o DNI) tenga en su chip datos de carácter sensible en general, salvo que se respalde con la acreditación de un consentimiento individual, informado y expreso.

Es el *art. 2.1 de la LOPD* el que establece que dicha ley es de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptible de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, definiendo en su *art. 3. a* los datos de carácter personal, como cualquier información concerniente a personas físicas identificadas o identificables.

Los datos biométricos pueden identificarse con rasgos fisiológicos o del comportamiento de una persona viva, y son considerados por lo tanto datos de carácter personal.

No como anécdota, pero sí como reforzamiento autonómico tenemos en la Comunidad de Madrid el *art. 4.1* de la *Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal*, que establece que la creación de ficheros de datos de carácter personal incluidos en el ámbito de aplicación de la Ley se realizará mediante *disposición* de carácter general que será publicada en el Boletín Oficial de la Comunidad de Madrid o en el Diario Oficial que corresponda. El procedimiento de creación de estos ficheros se encuentra desarrollado en el *Decreto 99/2002, de 13 de junio*, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el *Registro de Ficheros de Datos Personales*.

El Grupo de Trabajo del *art. 29* (de la Directiva 95/46/CE), en los informes y opiniones que viene presentando ante la Comisión en el contexto del debate sobre las transferencias de datos personales a E.E.U.U., remarca y reitera la imposibilidad de que los datos de tipo biométrico (de carácter sensible en general), puedan someterse a tratamientos automatizados fuera de los casos previstos por la

normativa.

En cuanto al proceso penal,

- La intimidad, la imagen, la dignidad y el honor de las personas son bienes que son tutelados en los *art. 197* ss. y *205 ss.* del Código Penal español de 1995

- El *art.301* del nuevo Código Penal español, establece "pena" a quién "convierta o transmita bienes, sabiendo que éstos tienen su origen en un delito grave..."

- La utilización ilícita de tarjetas electromagnéticas y la estafa o fraude informáticos se hallan expresamente previstos en los *arts. 197, 239* y *248.2*

- El *art. 44.3.a* de la citada LOPD, tipifica como infracción grave, proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos sin autorización de disposición general publicada en el BOE o Diario Oficial correspondiente

- Tipificando en su *art. 96.11* como infracción <<muy grave>>, los actos contrarios al respeto de la intimidad y consideración debida a la dignidad de los trabajadores

Toda actuación silenciosa quedaría justificada para el *art. 6.2 de la LOPD* que prevé que no será preciso el consentimiento cuando los datos "se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

Hábeas data es el derecho constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio. Este derecho se fue expandiendo y comenzó a ser reglamentado tanto por leyes de *habeas data* como por normas de protección de datos personales. También se encomendó a agencias estatales el control sobre la

aplicación de estas normas. También se suele exigir un registro del banco de datos para generar transparencia sobre su existencia.

La biometría se define como cualquier característica o rasgo personal automáticamente medible, sólido y distintivo que pueda emplearse para identificar o verificar la identidad de una persona. La biometría empleada para reconocer personas se basa en procesos de '*identificación*' y de '*verificación*'. Aunque el ojo humano no pueda leer las características biométricas, sí pueden hacerlo, y hacer uso de ellas, los instrumentos adecuados, sin límite de tiempo y dondequiera que la persona se encuentre.

Cierto es que es casi imposible que la persona en cuestión pierda los datos biométricos, a diferencia de lo que puede ocurrir con una contraseña o clave. Ofrecen un carácter distintivo casi absoluto, es decir, que cada persona posee una biometría única. Casi nunca cambian a lo largo de la vida de una persona, y ello proporciona permanencia a esas características. Todos tenemos además los mismos «elementos» físicos, lo que da asimismo a la biometría una dimensión de universalidad.

Con todo, es casi imposible la revocación de los datos biométricos: un dedo o un rostro es difícil de cambiar. Estas características positivas desde diversas perspectivas tienen su lado negativo en caso de robo de identidad: el almacenamiento en una base de datos de impresiones dactilares y fotografías vinculadas con un documento de identidad robado podría acarrear problemas importantes y permanentes para el auténtico propietario de esa identidad.

Debería disponerse de unos *procedimientos accesorios* que serían una garantía esencial para la introducción de la biometría, dado que los datos biométricos no son ni accesibles a todos ni del todo exactos. Principal argumento esgrimido en la *Reunión celebrada en Montreal a finales de 2005*.

No obstante, la política actual se asienta sobre la imperceptible integración electrónica que implantaran los Estados miembros desde la adopción del *Sistema de Información de Schengen (SIS)*, la "columna vertebral" del Acuerdo general para abrir las fronteras internas de la UE. El objetivo inicial del SIS era tranquilizar a los Estados miembros en el sentido de que al abrir las fronteras internas no se vería amenazada su seguridad.

A finales de 1996, como resultado de la ampliación de la UE y habida cuenta de que el sistema SIS

original se estaba quedando cada vez más obsoleto, la *Comisión de Schengen* aprobó la sustitución de SIS por SIS II, aumentando así notablemente su capacidad e introduciendo nuevas funciones tecnológicas, en concreto la introducción generalizada de la biometría.

Tanto el SIS como el SIS II son supervisados por organismos nacionales en materia de protección de datos, bajo los auspicios de la Directiva sobre Protección de Datos de 1995 (95/46/EC), que se refiere al procesamiento de datos personales, entre los que figuran los datos biométricos.

Los legisladores tienen que adoptar medidas firmes para garantizar que los sistemas de control biométrico y las bases de datos con las que se vinculan sean transparentes para las personas registradas y estén abiertos a organismos de supervisión independientes.

Precediendo a la creación de infraestructuras supranacionales y legislaciones estatales y regionales así de como de reglamentos de cuerpos de seguridad, en cada espacio identificable contemplado por nuestra tecnología, y aunque no con un cien por cien de convencimiento, se impuso una corriente creciente que intentó categorizar a la ciencia de la biometría como exponente de seguridad en la evitación de otros posibles atentados contra la *ya* población mundial.

Sin embargo, como se puede comprobar en un análisis jurisprudencial de la casuística de los casos habidos entre fronteras se singulariza y pone en evidencia la deficiencia de permeabilidad de esta nueva tendencia en las psicologías de los individuos y su particular interpretación. La *Organización de Aviación Civil Internacional, OACI,* una agencia especializada de las Naciones Unidas, aprobó la adopción de un modelo global y armonizado de datos biométricos en los pasaportes, consistente únicamente en el registro de las facciones conforme a la *27º Conferencia Internacional de Comisarios de Protección de Datos y Privacidad*. El registro de datos adicionales, como huellas dactilares, es una opción que deben sopesar y adoptar los gobiernos nacionales.

4.2.1.- Vía Aérea

La introducción de pasaportes biométricos que cuenten con un chip con la información del rostro y las huellas dactilares de su propietario, es una cuestión controvertida en Alemania. Estados Unidos espera que el gobierno de Berlín, junto con otros 27 países introduzca este tipo de pasaportes paulatinamente. Los nacionales de estos países no requerirían visado al ingresar en Estados Unidos

hasta por 90 días. De no contar con pasaportes biométricos, los ciudadanos tendrían que solicitar una visa aunque sea de tránsito.

Su introducción representa grandes complicaciones técnicas y de logística. Tampoco hay un estándar acordado entre Washington y sus socios europeos, sobre qué clase de datos deberán ser almacenados.

El detonante del 9/11 ha repercutido grandemente en el desarrollo de políticas de seguridad desde EEUU, reavivando el debate sobre la cantidad de información a solicitar por cada nuevo extranjero que llegara a su país por vía aérea, estando anclado el debate en la cantidad de datos de carácter personal que cada parte considera adecuada, y existiendo siempre una desproporción desde la parte estadounidense, existiendo ya casos donde el tratamiento de un dato incorrecto ha limitado el derecho de los ciudadanos europeos.

Existen conexiones directas entre la Organización Mundial de la Salud y la Organización de Aviación Civil Internacional, OACI[85], al deber remitir a esta segunda aquellas modificaciones que se recomienda introducir en la Parte General de la Aeronave, y cuando la OACI haya revisado dicha declaración emite un informe a la *Asamblea de la Salud* y sustituye el texto del Anexo 9 del reglamento Sanitario Internacional por la Parte Sanitaria de la Declaración General de Aeronave revisada por la OACI.

4.2.2.- Vía Marítima

En la Unión Europea, se debate sobre la introducción de la biometría en carnés de identidad, pasaportes, documentos de viaje y visados. Los EEUU van a exigir identificadores biométricos para extranjeros a entrar y salir del país.

El *Convenio OIT nº 108* se modificó en 2003 con objeto de introducir datos biométricos obligatorios para la gente de mar.

85 Organización Mundial de la Salud. WHA 48 .7 . Reglamento Sanitario Internacional. 2005 . Segunda Edición. Ginebra 2008, (pag. 12)

Recogemos los puntos concretos en los que se hace alusión a este tipo de dato de carácter personal:

- *art. 7*. apartados e) donde se alude a aquellas particularidades físicas cuya indicación pueda facilitar la identificación; y f) fotografía digital u original

- *art. 8* apartados a), b), c), d) y e); recordando que se exigirá, además, que al documento de identidad de la gente de mar se incorpore una plantilla u otra representación biométrica del titular

- El anexo I nos recuerda que el material utilizado en la producción del documento, sus dimensiones y la disposición de los datos se ajustarán a las normas de la *Organización de Aviación Civil Internacional* (OACI) aplicables a los pasaportes de lectura mecánica. Su apartado k) indica que la plantilla biométrica corresponderá a una huella dactilar impresa en forma de números en un código de barras, acorde con una norma que se elaborará con posterioridad.

- En cuanto a la tramitación de cada una de sus solicitudes o DIM quedan expresamente declaradas las competencias de los agentes competentes responsables de su manipulación en el Anexo II punto b)

Por otra parte, el desarrollo de nuevos servicios sanitarios en alta mar viene a confirmar el uso que hacemos del concepto de Telemedicina, donde se requiere una colaboración en materia de historia clínica con toda su estructura tecnológica desplegada. Esta faceta supera el perfil de prueba de carga de la HC, elevándola al derecho de todo paciente de ser atendido en el bienestar de su salud.

Por su parte el capitán de la embarcación o el médico de a bordo , si lo hubiere, antes de la llegada al 1º puerto de escala en el territorio de un Estado averiguará cuál es el estado de Salud a bordo[86], y salvo en los casos en que ese *Estado Parte* no lo exiga, cumplimentará y entregará a su llegada, o antes de la llegada, si la embarcación está equipada a ese efecto y el *Estado Parte* exige la entrega por adelantado una *Declaración Marítima de Sanidad*, a la autoridad competente del citado puerto.

86 WHA 48.7. Reglamento Sanitario Internacional. Título VI, (art. 37 : Declaracion Maritima de Sanidad), (pag. 44)

4.2.3.- Protección de Menores[87]

En el marco de la Unión Europea como principal documento se alude a la Resolución sobre *Libro Verde relativo a la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información* (1996), Comisión de las Comunidades Europeas, en "Documentos COM (96)" 483 final.

En este caso contamos como protagonista de dato de carácter personal a las "imágenes" y más concretamente a las relacionadas con menores.

Los recientes desarrollos tecnológicos pueden facilitar nuevas soluciones gracias a un control parental creciente, tanto en la televisión («chip anti violencia» o «v-chip») como en los sistemas en línea. En ambos casos, el etiquetado de los contenidos es un elemento clave del sistema.

En el Convenio Europeo se reconoce el derecho al respeto de la vida privada y familiar (*art. 8*) y, asimismo, el derecho a la libertad de expresión (*art. 10*). No obstante, ambos derechos no son considerados como absolutos e ilimitados, al estar previsto que pueda condicionarse su ejercicio por medidas necesarias, en una sociedad democrática, para garantizar la seguridad, la salud, la moral o los derechos y libertades de los demás (*arts. 8.2 y 10.2*). Este planteamiento normativo ha sido asumido por la *Carta de los Derechos Fundamentales de la Unión Europea* proclamada en Niza en diciembre de 2000. En ella se reconocen también el derecho a la vida privada (*art. 7*) y a la libertad de expresión y de información (*art. 11*) de los ciudadanos europeos. Se declara, asimismo, en este texto la prohibición de un ejercicio abusivo de los derechos y libertades allá reconocidos (*art. 54*).

No en vano la libertad de prestar servicios, también en la esfera de la información y la comunicación, es una de las libertades básicas reconocidas en el Tratado de la Unión.

87 Un ejemplo del trabajo que actualmente se está llevando a cabo en torno a la Privacidad de los Menores , lo encontramos en los *Headlines* de la *newsletter* correspondiente al Organismo I*CO, Information Comisssissioner's Office , UK,* de fecha 3 de setiembre de 2015, que entre otros contiene bajo el título "Concerns about children's privacy online": - International privacy enforcement project taises concerns over children's privacy – The EU regulation, aproachig the home straight – Findings from ICO advisory visits to residential care homes – Personal dara in leaked databases is still personal data – Healthcare Efficiency through tecnology Expo 2015 , etc.

El *Libro Verde* se remite a la jurisprudencia del *Tribunal Europeo de Derechos Humanos (TEDH)* de Estrasburgo para advertir que la libertad de expresión defiende no sólo las ideas e informaciones que no suponen intromisión u ofensa en los valores o derechos ajenos, sino también las susceptibles de ofender, contradecir o perturbar (STEDH, Handyside/Reino Unido, 1976).

El *Libro Verde*, acogiendo la jurisprudencia del TEDH (SS, Handyside/Reino Unido, 1976; The Sunday Times/Reino Unido, 1979; Autronic, 1990; Groppera Radio, 1990; Informationsverein Lentia, 1993), propugna que las restricciones a la libertad de expresión fundadas en la defensa de derechos ajenos, en concreto de los de los menores y la dignidad, se halle condicionada a tres exigencias acumulativas:

- Prohibición de arbitrariedad, lo que implica que cada restricción deba estar prevista por la ley

- Necesidad social imperiosa de garantizar valores y derechos de las sociedades democráticas

- Legitimidad de objetivos, enumerados de forma limitada y entre los que la defensa de la moralidad y la salud públicas se estiman particularmente adecuados para proteger a los menores y la dignidad humana

4.2.4.- Espacio Supranacional(Eurodac, Vis, SIS II)

Fundamentado sobre el *Reglamento nº 407/2002* por el que se establecen determinadas nomas de desarrollo del *Reglamento nº 2725/2000* relativo al sistema <<Eurodac>> para la comparación de las impresiones dactilares.

A partir de marzo de 1996 se empezó a negociar un nuevo convenio sobre la base del Título VI del *Tratado de la Unión Europea* o tercer pilar. En 1998 se juzgó oportuno ampliar el ámbito de aplicación de *Eurodac* al tratamiento de las impresiones dactilares de otra categoría de extranjeros con el fin de facilitar la aplicación de varias obligaciones que se derivaban del *Convenio de Dublín* y

entrando a considerar idénticamente a países como Islandia, Noruega y Suiza.

Debido a la proximidad de la entrada en vigor del *Tratado de Amsterdam*, por el que se modificaban el fundamento jurídico y los procedimientos de la política de asilo, en diciembre de 1998 el Consejo decidió convertir en instrumento comunitario ambos textos; reunió los proyectos de convenio y protocolo basándose en el nuevo Título IV del *Tratado CE* y, especialmente, en su *art. 63.*

Gracias a la comparación de las impresiones dactilares, los Estados miembros pueden comprobar si un solicitante de asilo o un nacional extranjero que se halle ilegalmente en su territorio ya ha formulado una solicitud en otro Estado miembro.

Los datos de los solicitantes de asilo se conservarán durante diez años salvo si la persona obtiene la ciudadanía de uno de los Estados miembros, en cuyo caso se suprimirán en cuanto el solicitante obtenga dicha nacionalidad. Los datos referentes a los nacionales extranjeros detenidos al cruzar ilegalmente la frontera exterior se conservarán durante dos años a partir de la fecha en que se tomaron.

Los datos se borran inmediatamente, antes de la espiración de dos años, cuando:

- el extranjero obtiene un permiso de residencia
- el extranjero abandona el territorio de los Estados miembros

Además de las autoridades nacionales de control, se concibe una autoridad de control común e independiente compuesta como máximo por dos miembros o representantes de las autoridades de control de cada Estado miembro. Dicha autoridad de control se encarga de controlar las actividades de la unidad central para garantizar que se respeten los derechos de las personas afectadas y responder a los problemas de aplicación relacionados con el funcionamiento de *Eurodac*.

Con arreglo al *art. 22* del Reglamento *Eurodac*, el Consejo adoptó disposiciones para garantizar la transmisión y comparación de huellas dactilares y para definir las tareas de la unidad central. La unidad central define las modalidades de transmisión de las huellas por vía electrónica. En caso de fallo técnico, otros medios de transmisión son posibles (CD-ROM, disquete, papel, etc). Un número de referencia permite atribuir las huellas a una persona específica y determinar el Estado miembro que ha transmitido los datos. Este número se compone de una o varias letras y de un código. Para

permitir la comparación de las huellas los Estados miembros garantizan una calidad apropiada de la transmisión. En su caso, la *Unidad Central* establece este nivel de calidad. En general, la unidad central:

- gestiona las solicitudes de comparación en 24 horas (salvo en caso de urgencia) siguiendo el orden de llegada de las solicitudes
- tras cuatro años de actividad debe elaborar estadísticas sobre el número de personas reconocidas como refugiados en varios Estados miembros y número de refugiados que han presentado una nueva solicitud de asilo en otro Estado miembro

Como *anécdotas*, indicar que al menos se debe de contar con catorce años para quedar registrado en este sistema y que en su *art. 7* se puede contemplar la recogida anticipada de datos. Se recogen las huellas dactilares de todos los dedos de la mano.

Este sistema de "libre circulación de personas, asilo e inmigración" tiene una alusión directa en la competencia de datos de carácter temporal según se recoge en un aviso jurídico presentado en su Web:

<<En caso de tratamiento ilícito de datos o comprobación de una acción incompatible con las disposiciones del presente Reglamento, toda persona o Estado miembro perjudicado tiene derecho a pedir la reparación del perjuicio sufrido. No obstante el Estado elegido culpable puede demostrar que el hecho lesivo no le es imputable para verse reconocer una exención parcial o total. Los gastos de las unidades nacionales y el coste de su conexión con la base de datos central y el de transmisión de los datos correrán a cargo de cada Estado miembro.>>

La creación del *Sistema de Información de Visados* (VIS) constituye una parte importante de la política común de visados de la UE y ha sido objeto de diversos instrumentos interrelacionados. Un Estudio de viabilidad de la Comisión Europea en 2003 impulsa su desarrollo adoptando el procedimiento de reglamentación reconocido como la *Decisión Comitológica 1999/468/CE*. El acto definitivo se produce conforme a la *Decisión 2008/602/CE* por la que se establecen la arquitectura física y las características de las interfaces nacionales y de la infraestructura de comunicación entre el Sistema Central de Información de Visados y los interfaces nacionales para la fase de desarrollo.

El VIS se basa en una arquitectura centralizada y consiste en una base de datos central donde se almacenan los archivos de las solicitudes de visado, esto es, el *Sistema Central de Información de Visados* (CSVIS), y en la *Interfaz Nacional* (NI-VIS) en cada Estado miembro. Los Estados miembros designarán una autoridad nacional central que estará conectada a la Interfaz Nacional, a través de la cual podrán acceder al CS-VIS las respectivas autoridades competentes.

La aplicación técnica del VIS y la selección de las tecnologías necesarias se encomienda al comité creado en virtud del *art. 5*, apartado 1 del Reglamento (CE) nº 2424/2001 (LCEur 2001, 4307) sobre el desarrollo del *Sistema de Información de Schengen* de segunda generación (SIS II).
Como principal objetivo se cuenta con la incorporación al nuevo modelo de visado una serie de datos biométricos (imagen facial y dos impresiones dactilares) que irían almacenados en un microchip en la etiqueta adhesiva del visado. El Reglamento prevé, asimismo, la introducción de datos biométricos durante el procedimiento de solicitud y su almacenamiento en la base de datos central.

La finalidad del VIS reviste una importancia crucial, tanto a la luz del *art. 8* del CEDH como del marco general relativo a la protección de los datos. En el *art. 6* de la Directiva 95/46/CE se dispone que sea preciso que los datos personales sean «recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines».

El VIS mejora la gestión de la política común de visados, la cooperación consular y las consultas entre las autoridades consulares centrales al facilitar el intercambio de datos entre los Estados miembros sobre las solicitudes y las decisiones relativas a las mismas.

Introducido por el *Tratado de Ámsterdam*, el *Convenio de Schengen* ratificado en 1985 presenta una segunda fase de instrumentalización, donde aparece el SIS II, *Sistema de Información Centralizado de Schengen*(CS-SIS), renovando su versión I. Incluye las principales leyes desarrolladas hasta el momento en materias de: visados, peticiones de asilo, circulación libre de personas, contando como punto referente el de la inmigración.

La conectividad entre los nodos nacionales (NI-SIS) se realiza desde este dispositivo. Por otra parte, la autoridad SIRENE garantizará el intercambio de alarmas, conectadas a este sistema, pero no almacenadas en él. Esta parte es donde se almacenarán datos de: arrestados, extraditados, individuos en busca y captura, aquellos requeridos por procesos judiciales, aquellos que estén bajo investigación

o los que hubieren perdido o robado pertenencias en las fronteras.

El conjunto de datos definido como "alertas" será lo que permitirá a las autoridades competentes identificar una persona u objeto.
El *Reglamento 45/2001* consigue reducir las víctimas de robo de identidad por estos fines, según su Título IV en base a esa entrada de datos. En su apoyo se suman:

- la *Convención 108 del Consejo de Europa* de 28 de Enero de 1981 en materia de protección de individuos en relación al tratado automático de datos

- la *Directiva 95/46/CE* del Parlamento Europeo de 24 de Octubre de 1995

Más recientemente en la vigesimoséptima Conferencia de Protección de Datos celebrada en Montreal el 16 de Setiembre de 2005 se genera una reflexión más profunda en lo referente a los sistemas europeos que consideran esta materia como son el caso de *Eurodac* y VIS. Llegan a no recomendar el uso de desarrollo de anexos para implementar elaboraciones críticas en relación a la biometría. Este sistema no se propone como único método en casos de identificación. Se refuerza la creación de procedimientos que regulen la corrección de erratas en posibles identificaciones.

Organismos como "Europol" y "Eurojust" tienen acceso a la información contenida en ciertas alertas precisas para el desarrollo de sus funciones. Y hasta tal puto ha de estar definido el acceso al SIS II que deberá existir una relación absolutamente detallada de las personas con este permiso de acceso, contribuyendo al soporte de la autoridad supervisora en una revisión de su *art*. 96. De esta manera queda reforzado el procedimiento que concluirá en una auditoría del propio SIS II.

Aquellas autoridades designadas en cada Estado miembro de acuerdo con la *D 95/46/CE* se responsabilizan de la supervisión de la legalidad del tratamiento de los datos personales del SIS II , velando de que cada cuatro años, al menos, se lleve a cabo una auditoría. Idénticamente, se cuenta con un Plan de Seguridad para el SIS II Central y la infraestructura de comunicación desde la *Decisión 2010/261/UE*, incluyendo ya medidas de seguridad en relación a los recursos humanos mediante la definición de las funciones y responsabilidades del personal con acceso al SIS II Central.

4.2.5.- EL 'Tratado de Prum' acerca de Bases de Datos de ADN

Se concluye el 27 de mayo de 2007 y es un Tratado de Derecho Internacional, adoptado al margen de la Unión Europea, pero relacionado con ella en cuanto a su contenido donde se comenta que tanto la adopción como su iniciativa son similares a lo ocurrido en Schengen.

Durante el Consejo de Justicia y Asuntos de Interior del 15 de febrero de 2007 se acordó integrar partes del tratado en el ordenamiento jurídico de la UE mediante una decisión basada en 3º pilar. El programa de la Haya fija el 1 de enero de 2008 como la fecha a partir de la cual el intercambio entre autoridades de datos se basará en el *Ppo. De Disponibilidad*. De forma que podemos decir que existen algo así como dos partes del conjunto de leyes en relación al *Tratado de Prum*.
Es precisamente el *art.42* del *Tratado de la UE*, en la denominada clausula paralela donde se ofrece la posibilidad de pasar determinados temas del tercer país al pilar comunitario.

De acuerdo con la definición de datos personales que establece la propuesta de Decisión Marco relativa a la protección de datos personales en el Marco del 3º pilar , *art. 2 letra a*, los perfiles de ADN obtenidos a partir de la parte no codificante de ADN relacionado con un nº de referencia constituyen datos personales, puesto que permiten la identificación , aunque sea de forma indirecta de un particular.

Como instrumento de ratificación de España del Convenio relativo a la profundización de la cooperación transfronteriza en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, de 27 de mayo de 2005, en su *art. 2* se aboga por la creación de ficheros nacionales de análisis del ADN para los fines de persecución de delitos, indicando explícitamente que los índices de referencia que no puedan atribuirse a ninguna persona , lo que se viene en denominar huellas abiertas, deberán poder reconocerse como tales. Los índices de referencia no podrán contener datos que permitan identificar a la persona concernida.

Si en el curso de la comparación efectuada con arreglo al apartado 1, una Parte Contratante comprueba que algún perfil de ADN transmitido coincide con los existentes en sus ficheros de análisis del ADN, comunicará sin demora al punto de contacto nacional de la otra Parte Contratante cuáles son los índices de referencia respecto de los cuales se ha encontrado la concordancia, cita su *art. 4*.

Los asesores en materia de documentos enviados por las Partes Contratantes desempeñarán en particular las siguientes funciones: asesoramiento y formación a las representaciones en el extranjero de las Partes Contratantes sobre cuestiones relacionadas con pasaportes y visados, en particular para el reconocimiento de documentos falsos y documentos manipulados, así como otras cuestiones relacionadas con el uso fraudulento de documentos y la migración ilegal.

Cada Parte Contratante garantizará que toda transmisión no automatizada y recepción no automatizada de datos de carácter personal queden documentadas por la autoridad que realice la consulta y la titular del fichero, para el control de la admisibilidad de la transmisión.

La documentación comprenderá los extremos siguientes:

- el motivo de la transmisión,
- los datos transmitidos,
- la fecha de la transmisión y
- la designación o identificación de la instancia que realice la consulta y la titular del fichero.

Los datos del registro únicamente podrán utilizarse para los fines siguientes:

- el control de la protección de los datos
- la garantía de la seguridad de los datos

Un ejemplo de caso sin resolver lo representan desde Islandia de la siguiente forma: En 1948 el Parlamento de Islandia aprobó un proyecto de ley permitiendo la creación de una base de datos centralizada conteniendo la información genealógica, genética y médica personal de todos los

ciudadanos islandeses. Seguidamente, el Parlamento le otorgó un contrato exclusivo a la compañía biomédica.

Mas o menos un año antes del proyecto de ley, *deCODE* firmó un acuerdo con la gigantesca corporación farmacéutica suiza Hoffman-LaRoche, en anticipación del contrato deCODE explicó que estaba investigando genes asociados con más de 30 enfermedades, 12 de las cuales estarán financiadas por Hoffman-LaRoche. Los servicios públicos de salud han mantenido registros médicos detallados de cada individuo desde el año 1915.

Una persona pude solicitar su exclusión de la base de datos en cualquier momento , pero la información a la base de datos no sería removida además la ley no requiera que se le informe a los islandeses qué tipo de investigaciones se están llevando a cabo con sus datos personales.

DeCODE tiene un monopolio sobre los datos debido a que tiene la única licencia. La base de datos pertenece al sistema nacional de salud manejado por el gobierno, pero *deCODE* tiene los derechos de comercializar los datos por 12 años. La legislación hasta le ha asegurado a *deCODE* que el acceso a sus datos no le será dado a nadie si este puede dañar los intereses financieros de la compañía.

Por su parte la *Interpol* mantiene su propia reglamentación al respecto de las *Bases de Datos de ADN* y que como *Sistema Mundial de Comunicación policial 1.24/7* se la conoce como pasarela en Materia de ADN ,creada en 2002, donde puede ampliarse su acceso a ella más allá de las *OCN, Oficina Central Nacional* que mantiene la Interpol en cada uno de sus países miembros, a centros y laboratorios de policía científica si así lo solicitan . Interpol actúa únicamente como conducto para el intercambio y el cotejo de la información, no tiene datos nominales que vinculen un perfil de ADN con una persona y un perfil de ADN es simplemente una lista de números basada en la estructura de ADN de una persona, un código numérico que une para distintos individuos, y no contiene características psicológicas de la persona, ni sobre sus enfermedades o su predisposición a ellas. Interpol nos recuerda que excepto en el caso de los gemelos univitelinos[88], cada persona tiene un ADN único, por lo que los perfiles de ADN resultan útiles para resolver asuntos penales, identificar víctimas de catástrofes y localizar personas desparecidas.

Esta pasarela también es compatible con la *Convención de Prüm* de la Unión Europea (una iniciativa

88 Documento de la Interpol COM/FS/2012-02/FS-01. Disponible en: http://www.interpol.int

surgida en 2005 para simplificar el intercambio de datos entre los países de la UE), y se puede utilizar para la exportación selectiva a escala internacional de perfiles de ADN a los países que utilizan el sistema CODIS (programa de cotejo de perfiles de ADN diseñado por el FBI).

4.3.- Sistemas de Alertas Alimentarias

Aunque en proporción pequeña de información este tipo de sistemas puede incorporar información proveniente de consentimientos informados de pacientes.

Introduciendo la definición de alerta como la gestión que se hace de un determinado riesgo o riesgos asociados a alimentos que no son seguros, se puede observar como la *Organización Mundial del Comercio*, *OMC*, sólo admite barreras al comercio de alimentos por razones sanitarias basadas en la evidencia científica. Los alimentos, por tanto, pueden circular de unos países a otros, en un ámbito internacional, salvo que se demuestren que no son seguros.

Aunque con diferentes niveles de intervención y categorías de acciones a emprender, en EEUU se cuenta con tres agencias federales que se ocupan de las alertas alimentarias:

- la Comisión de Consumidores Estadounidense para la Seguridad de los Productos , *CPSC*
- la Administración para la Alimentación y los Medicamentos, *FDA*
- el Servicio de Inspección y Seguridad Alimentaria , *FSIS* del Dpto. de Agricultura

Cuando una empresa no cumple con lo pactado, se ven obligadas a recurrir a la intervención judicial.

Las tres agencias tienen articulado un procedimiento de comunicación de las alertas a los consumidores, a través de los medios de comunicación, a los gobiernos locales y estatales y a las

organizaciones privadas. La *CPSC*, en su página web incluye lo que se denomina 'Catálogo de Buenas Prácticas', en el que se recogen experiencias de empresas de diferentes sectores que han llevado a cabo iniciativas de comunicación adecuada de problemas relacionados con la seguridad de sus productos.

En la Unión Europea, el sistema de alerta rápida se estableció en 1978, aunque no se legisló hasta 1984. A partir del establecimiento de la Autoridad Europea de Seguridad Alimentaria en el año 2001, el Sistema puede aplicarse tanto a los alimentos de consumo humano como de consumo animal, y recibe el nombre de *Rapid Alert System for Food and Field*, *RASFF*, abarcando a los Estados miembros de la Unión, así como a los países del *Espacio Europeo de Libre Comercio*, EEA-EFTA, y a la Comisión, funcionando en entorno web.

Los países terceros, no miembros de la UE, aun no formando parte de la red de la Comisión se encarga de informarles cuando el alimento problemático ha sido exportado a estos países o cuando es originario de un país tercero, a fin de evitar que el problema se repita.

Comprende tres niveles de información:

- *notificación de alertas*, indicando una necesidad de acción inmediata
- *notificación de información*, sin existir esa necesidad de acción inmediata, servirá para prevenir acciones futuras
- *noticias*, información de interés relacionada con la seguridad de los alimentos para consumo humano o animal

En España existen dos sistemas de alerta alimentaria:

- el de alimentos de *consumo animal*

- el de alimentos de *consumo humano*, que gestiona el Ministerio de Sanidad y Consumo, denominado *Sistema Coordinado de Intercambio Rápido de Información*, *SCIRI*[89]. Se trata de una herramienta de gestión de alertas, basada en un establecimiento de una red de puntos de contacto entre el Ministerio de Sanidad y Consumo, y las autoridades competentes en Seguridad alimentaria de las diecisiete comunidades autónomas , CCAA, así como las ciudades autónomas de Ceuta y Melilla

Este Sistema de ámbito nacional se encuentra enlazado con el RASFF europeo, a través del punto del Ministerio de Sanidad y Consumo.

4.4.- Mercado Interior, IMI

Su objetivo es facilitar la cooperación administrativa y mutua asistencia entre los estados miembros de la Comunidad Europea con el propósito de alegar la funcionalidad en el Mercado Interior y la libre circulación de las personas.

Se realiza gracias a una herramienta de intercambio de información, incluido cierto grado de cantidad de datos de carácter personal entre las administraciones nacionales.

La denominada clausula de privacidad, *The Privacy Statement*[90], cubre la recolección, registro, almacenamiento y borrado de la información personal que no son responsabilidad de cada estado miembro.

Si un ciudadano europeo tiene conocimiento que alguno de sus datos de carácter personal se encuentran en el IMI , podrá ejercer el derecho al ejercicio de los *Derechos ARCO.* Los

89 Red de Alerta Alimentaria. Disponible en: http://www.aesan.msc.es/AESAN/web/alertas/alertas.shtml

90 European Data Protection Supervisor (EDPS), Privacy Statement. Internal Market Information System – Imi(pag. 2): cubre la recolección, registro, almacenamiento, y borrado de la información personal que no son responsabilidad de cada estado miembro". La ley aplicable esta regulada por D 45/2001 CE del Parlamento Europeo. Asegura que está protegido por un número de técnicas con diferentes niveles de acceso a la Base de datos con un sistema similar que el usado en muchos sistemas bancarios. Y también por el protocolo https. Si un ciudadano llega a la conclusión de que tiene sus datos personales en el sistema IMI, puede ejercer aquí los Derechos ARCO."

coordinadores del IMI deben asegurar el establecer contactos con las autoridades en Materia de Protección de Datos de manera que se pueda asistir de la mejor manera y adaptada a la legislación específica de cada país.

El IMI es una herramienta software accesible, desde Internet y diseñada por la Comisión Europea en cooperación con los Estados Miembros. No se trata de una Base de Datos que almacena información, por largos períodos de tiempo, sino más bien un mecanismo centralizado que permite a las administraciones de los Estados Miembros el intercambio de información, siendo esta retenida por pequeños períodos de tiempo.

En concreto, en la *Decisión 2008/49/EC* de la Comisión, que de tiempo en tiempo, será renovada, aparecerán aquellas legislaciones donde será admitido el intercambio.

Los usuarios del IMI son, normalmente, especialistas en sus campos, pero no se espera que lo sean en materia de protección de datos, aunque idénticamente a como ocurre en el campo de seguridad del paciente, se les proveerá de directrices para cubrir estas lagunas así como acerca de las salvaguardas introducidas en el sistema a fin de evitar posibles riesgos, un framework que vendrá a rozar la *Resolución de Madrid*.

Los usuarios del IMI desempeñan tareas en el dominio público en el oficio de su profesión. Claro nos puede resultar el ejemplo de , en el caso , de los trasplantes el carácter de la figura del coordinador en la verificación de que se cumplan las adecuadas medidas sanitarias.

Por otra parte, la ley aplicable a cada usuario depende del tipo de actor o usuario del IMI. Así, para la Comisión se le aplica la Decisión 45/2002/EC mientras que para un usuario normal la ley nacional que ha de estar en conformidad con la Directiva 95/46/CE.

El procesado debe estar directamente relacionado con el ejercicio de una profesión o la provisión de un servicio y de acuerdo con las expectativas de la Directiva. De esta forma las notificaciones de multas no resultan datos relevantes, para la aplicación del citado procedimiento de trasplantes.

Recordemos las exigencias que presenta el *a.10* de la Directiva de protección de datos:

- identificación de los controllers
- propósito del procesado
- contenedores y sus soportes
- ejercicio derechos ARCO
- derecho a *redress* o derecho a obtener una indemnización por perjuicios
- período de tiempo de almacenaje
- medidas de seguridad
- enlaces a documentos y webs, incluidas el IMI

Toda aquella información intercambiada entre las autoridades competentes y procesadas por el IMI se borrarán automáticamente por la Comisión seis meses después del intercambio. Por razones estadísticas, la información permanecerá en el IMI pero de forma anónima.

Alguna autoridad competente involucrada en algún tipo de este intercambio puede exigir el borrado de determinada información, que se llevará a cabo en los diez días siguientes desde el momento de acuerdo con la autoridad competente.

No puede, de ningún modo, ser rechazado el ejercicio de los derechos ARCO, aunque estos se aplicarán conforme a la voluntad de la legislación de cada Estado Miembro.

Si el paciente no se quedara satisfactoriamente tratado, aun puede recurrir a otra autoridad competente.

Estos procedimientos pueden ser iniciados en cualquier momento. En concreto, el controller notificará toda rectificación, borrado o bloqueo a terceras partes, a no ser que esto sea un imposible o apunte a un esfuerzo desproporcionado.

Conviene así mismo indicar que fuera del IMI la información que se hubiera obtenido deberá ser almacenada por autoridades competentes.

El Sistema de Información del *Mercado Interior* , IMI, soporta dos procesos de flujo: uno de intercambio de información y otro de mecanismo de alerta. El acceso a cada uno de ambos flujos se restringe a las autoridades específicamente indicadas para ello. A su vez se distinguen dos procedimientos, el normal y el de urgencia.

Una alerta tan sólo va a ser establecida cuando un potencial serio de daño puede haber sido causado como producto-resultado de una actividad y mientras se encuentre dentro de los límites de la Directiva. Aquellos ámbitos que se encontraran fuera de la Directiva de Servicios, como puede ser motivos de trasporte o de seguridad privada no permitirán la creación de una alerta.

Ejemplos donde sí se pueden crear alertas son los siguientes:

- por haberse producido una emisión de falsa información

- por haber incurrido en una ausencia de medidas de seguridad por parte del proveedor

- por el uso de equipo inadecuado, inseguro o peligroso para la provisión de un servicio. Además, la Directiva de Servicios distingue entre las alertas

enviadas por un Estado Miembro u otros

- cuando lo es por un estado miembro: pueden detectarse dos situaciones a su vez; cuando el estado miembro no tiene la certeza de que las medidas adoptadas son suficientes para detener el riesgo y, cuando se conoce de antemano que la seguridad y sanidad de las personas no se va a poner en peligro en primera instancia, pero se pueden revelar conductas posteriores a las que no de tiempo a afrontar.

- cuando lo es por un estado diferente del de establecimiento

El ciclo de vida de la alerta va del siguiente modo: una autoridad registrada puede generar una alerta desde alguno de los estados miembros del área económica europea, EEA dentro del ámbito de su competencia. La alerta es elevada hasta un coordinador, este la revisa y la difunde a los otros estados miembros. Una vez llegado el mensaje, en la otra parte, el procedimiento se cumple con el mismo esquema.

Cuando el riesgo es eliminado, el coordinador puede desactivar la alerta. En el momento de cierre de una alerta se puede iniciar un pequeño debate en el seno de la autoridad del Estado Miembro hasta efectivamente cerrarla. Se produce, pues una 'Objección', *Objection*.

Las autoridades de alertas son normalmente competencias en el campo de la salud y la seguridad de las personas o en el campo del medioambiente.

En el caso de no obtener una aprobación final, la autoridad iniciada se retiene el derecho a editar o borrar la alerta o bien su información asociada.

La distribución de una alerta permite el añadir información a la misma, indicando, por ejemplo, aquellas medidas que se han ido adoptando.

Como se ha sugerido, es únicamente responsable del cierre del proceso el Estado Miembro donde se encuentra establecido el proveedor. En el período en que se mantiene abierto una propuesta de cierre de una alerta, la propuesta puede ser editada o bien cancelada.

En cualquier momento y punto del ciclo de vida puede ser generados informes y ya se puede observar en su dinámica ciclos como el correspondiente al año 2009 donde IMI fue principalmente utilizado para el desarrollo del sistema de cualificaciones profesionales europeo.

Desde el principio IMI procede con un '*Privacy by Design*'[91] en la implementación de sus sistemas, anteponiendo de principio a fin la privacidad del usuario, concretando la protección de datos del ciudadano en el ámbito de la Sanidad.

Sumándose a este tipo de iniciativas marco, existe una salvaguarda semántica incluso a la hora de

referir al Sistema Informático entre sus usuarios conocida como '*The comitology decision*" . En principio la *Directiva de Servicios* no hace referencia explícita a IMI, por lo que, y de acuerdo con el procedimiento propuesto en la propia Directiva se adoptó una Decisión por la Comisión a fin de concretar que efectivamente esta herramienta iba a ser utilizada en el intercambio de información del Mercado Interior.

La Directiva D 2011/24/CE relativa a la aplicación de los derechos de los pacientes en la asistencia transfonteriza, tiene una repercusión directa en su relación con el ejercicio de ejercer de los profesionales sanitarios que figuran en los registros nacionales locales, pudiendo ponerse a disposición de las autoridades de otros Estados miembros, previa solicitud . El intercambio de información se llevará a cabo a través del Sistema de Información del Mercado Interior.

La Directiva 2011/24/ue relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfonteriza incorpora una importante novedad en relación a este Sistema de Información y el derecho a ejercer de los profesionales sanitarios que figuran en los registros nacionales o locales

91 CAVOUKIAN, Ann. "*Privacy by Design"*. Information and Privacy Commissioner, Ontario, Canada. Information Commissionaries office, ICO. 2008, : refers to the philosophy and approach of embedding privacy into the design specifications of various technologies Disponible en: http://www.ipc.on.ca/images/Resources/privacybydesign.pdf

se ponga a disposición de las autoridades de otros Estados miembros, previa solicitud; produciéndose el intercambio de información a través del Sistema de Información del Mercado Interior y conocido como IMI.

El *IMI*, conforme nos confirma su Clausula de Privacidad recaba básicamente información de contacto de los usuarios de los coordinadores como son nombre, nº tfno. profesional, fax, dirección de correo electrónico, etc., aunque a través de la relación de los formularios de preguntas como es el caso de la *Aplicación de los Derechos de los Pacientes en la Asistencia Sanitaria Transfonteriza*, pueden aparecer otros como el nº de registro de un profesional y, además, tal como expone el *art. 16 de su Reglamento 1024/2012* relativo a la cooperación administrativa a través del Sistema de Información del Mercado Interior y por el que se deroga la *Decisión 2008/49/CE* de la Comisión («Reglamento IMI») , recopilar categorías especiales de datos.

El acceso de los miembros del equipo *IMI* tienen derecho de acceso en conformidad con el *art. 15* de su *Reglamento 2006/3602 de Seguridad de Sistemas Informáticos* usados por la Comisión Europea. Por su parte, los miembros de la Comisión no pueden tener acceso a los datos de quien son objeto de los intercambios de la Comisión salvo que desempeñen alguna función en relación con los vínculos jurídicos contemplados. Por razones técnicas, el personal de la Comisión contará con dicho privilegio en los siguiente casos:

- recuperación, a petición de una autoridad competente, de los datos bloqueados y en relación con los cuales los interesados hayan ejercido su derecho de acceso, rectificación o supresión

- su cancelación antes de que finalice su periodo normal de conservación, en casos concretos y a petición expresa de una autoridad competente participante en el procedimiento de cooperación administrativa, siempre que se cuente con el consentimiento de los interesados

El *IMI* como todo Sistema Informático sujeto a las directrices de Seguridad en materia Informática de la Comisión Europea realiza una invocación a un marco de seguridad que permita la definición de

principios, procedimientos, prioridades y responsabilidades de modo que cada Sistema de Información deberá ser protegido en una relación proporcional al nivel de riesgo al que se encontrara expuesto. Con este criterio realiza una apuesta explícita de la norma internacional ISO 27001, ampliando su ámbito de aplicación al del Teletrabajo, según el *art. 2 del Reglamento*. Contempla, idénticamente el Reglamento la aparición y definición de un nuevo Actor que bien podríamos haber incluido en el apartado 3 del Capítulo II, y correspondiente a la denominación de *LISOS* , *Local Informatics Security Officers*: y, que no siendo parte del Equipo de Gestión del Sistema Informático deberá reportar a su Director o Delegado debiendo garantizar la monitorización e implementación de los Planes de Seguridad; igualmente, el Inventariado deberá mantenerlo actualizado y garantizar su colaboración en la detección de posible de amenazas, así como del análisis de sus posibles impactos.

Sin dejar de olvidar que en lo que respecta a la Protección de Datos por las Instituciones y los Órganos de la Comisión y a su libre circulación, todas las operaciones que competen a la Comisión están reguladas por el *Reglamento (CE) nº 45 /2001.*

En relación a los *Consentimientos de los Interesados*, estos no estarán recabados cuando los tratamientos de datos se realizaran sobre Bases de Disposiciones de las Directivas o Reglamentos, *art. 7 D 95/46/CE, L*a segunda excepción al ejercicio de los Derechos ARCO lo encontramos en la aplicación del art. 24 de la *LOPD, LO 15/1999* y que en lo que respecta a la Defensa Nacional, a la Seguridad Pública o a la persecución de Infracciones Penales no será aplicable a los interesados a los que se soliciten datos personales el derecho a ser previamente informados de modo expreso, preciso e inequívoco de las manifiestas acciones ordenadas:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

4.5.- Sistema Europeo de Alerta y Respuesta Temprana , EWRS

El *Sistema europeo de Alerta y Respuesta Temprana, EWRS*, permite desde 1998 la comunicación en Tiempo Real por medios electrónicos entre los Estados Miembros y la Comisión Europea permite compartir información validada en relación a las amenazas sanitarias y entre los institutos de salud pública nacionales y las autoridades sanitarias.

EL compromiso político se inicia en 2005 con la creación del *Centro Europeo de Prevención y Control de Enfermedades, ECDC*, constituido en torno a tres unidades técnicas:

- Unidad de Vigilancia
- Unidad de Preparación y Respuesta,
- Unidad de Consejo Científico
- Unidad de Comunicación Sanitaria

Se observa, sin embargo, que la aplicación de un valor de añadido en la utilización de estas alertas exige la existencia de sistemas de información que permiten la detección precoz que permitan realizar el seguimiento de los riesgos de salud y su consiguiente categorización y de las consiguientes señales de posibles problemas sanitarios. Esto exige la automatización de procesos de notificación y análisis de datos de vigilancia, junto al desarrollo de métodos estadísticos.

En España, en concreto, se ha iniciado el reconocimiento de la integración básica de datos provenientes del Instituto Nacional de Meteorología con objeto de mejorar la preparación de servicios sanitarios para dar respuesta rápida a los problemas de salud asociados a estos factores.

Por su parte el *CNE-ISCII, Centro Nacional de Epidemiología del Instituto de Salud Carlos III,* como coordinadores de la *Red Nacional de Vigilancia Epidemiológica, RNVE* se constituye como el nodo de comunicaciones entre las comunidades autónomas y los institutos técnicos de los Estado miembros de la UE. Concretamente, el CNE-ISCIII colabora en el desarrollo de herramientas de detección de riesgos mostrando una faceta divulgativa de acceso público.

En Estados Unidos, la garantía de la Interoperabilidad y desde 2005 se coordina desde la *Red de Información de Salud Pública, PHIN*.

4.6.- El Sistema de la Historia Clínica en el Sistema Nacional de Sanidad, SNS

El *Sistema de Historia Clínica Digital del Sistema Nacional de Sanidad, HCDSNS*[92], es considerado como uno de los instrumentos de cohesión del sistema sanitario público español. Forma parte del conjunto de proyectos de Sanidad en Línea convocado dentro del Plan Nacional de Calidad .

El proyecto se fundamenta sobre cinco principios:

- *lógica asistencial*:

  fundamentalmente cuando los ciudadanos se desplazan fuera de la Comunidad Autónoma de origen a fin de que los datos estén accesibles a los profesionales; distingue, por tanto, entre el sistema de historia clínica y la interoperabilidad que se le quiere y precisa otorgar

- *derechos de pacientes* y usuarios

92 L 41/2002 (art.3, art.14, art.15, art.16,), RDL 1093/2010 (art.2, art.3 anexos)

- necesidades y *responsabilidades* de los profesionales

- mandato *legal*

La atención sanitaria de un ciudadano que demanda asistencia puntual precisa de, al menos, los siguientes documentos electrónicos:

- Historia Clínica resumida, HCR, denominada internacionalmente '*Patient Summary*'[93]

- Informe de Atención Primaria

- Informe Clínico de Alta

- Informe Clínico de Consulta Externa de especialidades

- Informe de Cuidados de Enfermería

- Informe de Resultados de Prueba de Laboratorio

- Informe de Resultados de Pruebas de Imagen

- Informe de Resultados de otras Pruebas Diagnósticas

El sistema presenta el contenido del informe como imágenes para su lectura o impresión, aunque no así la edición, la copia parcial o total de su contenido, ni su descarga a dispositivos de

93 Seguridad del Paciente:. Disponible en: http://www.seguridaddelpaciente.es/

almacenamiento.

Al poder realizar el seguimiento de los detalles de los accesos al conjunto de sus datos, el ciudadano puede acceder como auditor externo del sistema, realizando una verificación de la legitimidad de los mismos: observando la fecha y hora en que se realizó la el acceso, el Centro desde el que se realizó el mismo y las características del documento.

La propia aplicación informática contiene salvaguardas que informa al ciudadano de las consecuencias negativas que puede suponerle el elegir la ocultación de un documento condicionando de este modo las decisiones del profesional que le asista o pueda asistir. Idénticamente el profesional de sanidad es informado de esta ocultación por si pudiera obtener el consentimiento informado del paciente y obtener de este modo la desprotección de dicho documento. En estos términos se expresa el documento de requerimientos funcionales del *HCDSNS* que quedan recogidos en un documento denominado 'Análisis de Requerimientos del Sistema' o *ARS*[94].

La participación de la Organización de las Naciones Unidas queda reflejada por la participación de la *International Health Terminology Standards Development Organization*, *IHTSDO*, que ostenta la propiedad intelectual de la Terminología *Snomed Clinical Terms*, *Snomed-CT*[95], que garantiza la interoperabilidad semántica, esto es, el vocabulario sanitario estandarizado que permite la interpretación inequívoca de los contenidos trasmitidos entre sistemas distintos de forma precisa y en idiomas diversos. En 2011 Snomed CT presentaba más de 311 000 conceptos y unas 1 360 000 vínculos, denominados relationships. Creado en Junio de 2002 por el *College of American Pathologists* y el *National Health Service* . Su uso requiere de una licencia[96] con los siguientes posibles modelos:

- una, a cargo de GNP, *Gross National Group* como miembro nacional

94 Ministerio de Sanidad y Política Social. "Analisis de Requerimientos del Sistema, ARS. Historia Clínica Digital del Sistema Nacional de Salud".vs. 2.8.1. 2010

95 Systematized Nomenclature of Medicine, Snomed, that includes: codes, terms, synomyms, definitions covering diseases, findings, procedures, microorganisms substances, etc, in the areas of diseases, symtoms, operations, treatments, devices and drugs. Snomed CT is considered to some to be the most comprhensive multilingual clinical terminology in the world. Disponible en: http://www.ihtsdo.org/fileadmin/user_upload/doc/

96 International Health Terminology Standards Development Organisation. Disponible en: http://www.ihtsdo.org/join-us/affiliate/

- dos, por medio de una licencia comercial

- tres, para propósito de informática médica, o de demostración o de evaluación de modo gratuito

Así mismo, se distribuye acompañado de herramientas específicas como navegadores

El rol del profesional sanitario no está autorizado a almacenar en dispositivo alguno informes, siendo tan sólo autorizado a visualizarlos o imprimirlos el usuario, el que sí podrá realizar dicho almacenaje.

Por su parte, la aplicación permite al usuario a enviar notificaciones de incidencias interpretadas por el sistema como alertas y que son gestionadas por la propia aplicación.

Existe una consideración por parte del sistema de aplicación de un nivel de seguridad avanzado en los siguientes referentes:

- *imagen y vídeo actual*: como datos de exploraciones y telemedicina

- *cuidados de enfermería*: la complejidad de este conjunto de datos no reside en su contenido, sino en el volumen del colectivo profesional que le ha de acceder, y la necesidad de administrar sus permisos con garantía suficiente de autenticidad (certificados electrónicos).

La posibilidad que permite el sistema de detectar los accesos a una determinada historia clínica se extiende a todos los Centros Sanitarios de las diferentes Comunidades Autónomas, CCAA, a través del código SNS del usuario. Por cada nodo de Comunidad Autónoma se crea un *Registro Voluntario de Representados,* que relacionará la identidad de los representantes que voluntariamente que hubieran solicitado la existencia de la tutoría legal explícita o implícita y la caducidad de ésta.

4.7.- El Sistema de Mutuas y Aseguradoras

Presenta este apartado una singular discusión en cuanto a datos únicos extraídos y ya disociados a incorporar en otro tipo de documentación, por ejemplo, de índole de Gestión Económica dígase una factura de venta de material quirúrgico a efectos de control de facturación, por ejemplo. En tal línea se perfila la Directiva en materia de protección de datos que alega que precisamente constituye una 'excepción' a la prohibición general de tratar datos sensibles: cubriendo solamente el tratamiento de datos personales con el propósito específico de proporcionar servicios relacionados a la salud de carácter preventivo, de diagnóstico, terapéutico … y a efectos de la gestión de estos servicios sanitarios, como, por ejemplo, facturación, contabilidad o estadísticas.

En efecto, nos recuerda la Agencia de Protección de datos la prohibición de la transmisión de la información médica obtenida al amparo de lo dispuesto del la *Ley de Protección de Riesgos Laborales* a cualquier tercero[97] distinto del personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores.

Priorizando las disposiciones internacionales consideraremos *disociación* cuando se exija un esfuerzo desproporcionado como para disuadir a quien accede a un dato a que el afectado no resulte determinable.

En el supuesto caso que una Empresa eligiera el método de protección de las contingencias de accidentes de trabajo a través de una Mutua resulta de obligación del empresario la cesión de los datos de sus trabajadores tal vez por medio de la figura del responsable del tratamiento.

La labor fundamental de las Mutuas consiste en la Gestión conjuntamente con la Seguridad Social, esto es, de las contingencias de accidentes de trabajo y enfermedades profesionales.

Un ejemplo de interacción con el Sistema de Información de una Mutua es la realización de una *consulta* que conforme a la definición que nos proporciona la legislación se puede considerar como información concerniente a la salud, presente y futura, física o neutral de un individuo.

El resultado de la consulta conceptualizando el 'parte de accidente' que tradicionalmente se trabaja puede constar de la siguiente información:

97 Informe Jurídico 655/2008, Agencia de protección de datos Disponible en: http://www.agpd.es

- día del accidente
- días probables de baja
- visitas del lesionado
- código lesión

Es precisamente este último dato el que la *Organización Mundial de la salud*, la *OMS*, y conforme a su baremación de tablas sugiere se utilice para su indexación.

Ahora bien, puede ocurrir que tal información como conjunto devenga en la aparición mínima y como dato de salud , por el porcentaje de discapacidad e información genética en algún otro documento como veremos.

Resulta factible el tratamiento de datos de salud realizado sin ejecutar el consentimiento del afectado,

como consecuencia de haber asistido un trabajador a las instalaciones y servicios sanitarios. Ahora bien, en cuanto al personal dedicado a la vigilancia y control de la salud de los trabajadores se llevará a cabo por el personal sanitario con competencia técnica, formación y capacitación acreditada sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador. Independientemente de estos casos, el empresario deberá elaborar y conservar a disposición de la autoridad local la siguiente documentación: la relación de los accidentes de trabajo que hubieran causado al trabajador una incapacidad laboral superior a un día de trabajo. Dicha comunicación no deberá producirse de forma extensiva a todo el historial médico en respeto a la confidencialidad y deberá atenerse a un modelo concreto de notificación[98].

El legislador español no menciona los datos genéticos en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, ni en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica, ni en la ley 14/1986, General de Sanidad.

Por su parte, la recomendación (97) sí que recoge una definición de dato médico. Dicho concepto ha

98 Orden del Ministerio de Trabajo de 1987 , modificada por Orden Tas(2926/2002)

sido aclarado por la *Declaración Internacional de Datos Genéticos*, aprobado por la *32º Sesión de la Conferencia General de la UNESCO* como la información sobre las características hereditarias de las personas obtenidas por análisis de ácidos nucleicos u otros análisis científicos.

Conforme al *art. 7* de la LOPD los datos relativos en la salud o datos médicos en su obtención ha de adecuarse a uno determinados principios de calidad de los datos: ppo. de pertinencia, ppo. de finalidad, ppo. de lealtad y ppo. de seguridad de datos.

El anexo, punto 4.3 de la Recomendación (2002) sobre la protección de datos personales recogidos y tratados a efectos de seguros, señala que los datos personales pueden ser recogidos y tratados en los siguientes supuestos:

- cuando la ley lo prevea

- para la formalización de un contrato de seguro del que el interesado es una parte o para la redacción de una póliza a solicitud del interesado

- cuando el interesado o su representante legal u otra persona u organismo acorde con la ley hayan dado su consentimiento

- cuando los datos sean necesarios para el desarrollo de los intereses legítimos del responsable del tratamiento, siempre que los intereses del afectado no prevalezcan sobre los del representante del tratamiento

En las entidades aseguradoras se obtienen datos de salud de los asegurados bien antes de la conclusión del contrato para la 'valoración del riesgo' por:

- seguro de vida
- invalidez temporal, permanente o muerte
- seguro de accidentes
- seguro de enfermedad

La solicitud de la historia clínica para el abono de determinada asistencia sanitaria prestada o como documento acreditativo de la salud o enfermedad frente a dichas entidades para indemnizar a las personas incluidas en el contrato puede vulnerar de forma directa el derecho a la intimidad del individuo.

Cuando se produzca dicho conflicto, el médico debería abstenerse de informar sobre la salud del cliente que solicita una póliza, ya que su conocimiento del estado de salud del enfermo no deriva sólo del acto de reconocimiento, sino de la información con la que contaba previamente.

La ley del contrato del seguro establece en su articulado un deber del tomador de declarar todas aquellas informaciones susceptibles de influir en el riesgo, dicha obligación no responde a ningún interés general, sino a un interés económico.

La doctrina ha planteado cuál es la forma que requiere el consentimiento expreso, donde la norma legal no establece la necesidad de que ese consentimiento se otorgue por escrito. Sin embargo, parece recomendable tanto para el asegurador como para el asegurado se realice por escrito.

En el *auto 600/1989*, de 11 de diciembre, se había señalado que la comunicación de datos médicos habida cuenta que puede afectar al derecho a la intimidad, sólo es posible tras el otorgamiento del consentimiento de la persona afectada por dicha revelación

El *art. 24.3* párrafo segundo, de la *Ley 30/1995, de 8 de noviembre, de ordenación y supervisión de los seguros privados*, permitió a las entidades aseguradoras la creación de ficheros comunes en los siguientes términos. Las entidades aseguradoras podrán establecer ficheros de datos personales que permitan la colaboración estadístico-actuarial y la prevención del fraude en la selección de riesgos y en la liquidación de siniestro.

La vigente LOPD, a través de su disposición adicional sexta, modificación del *art. 24*, párrafo tercero, de la *Ley de Ordenación y Supervisión de los Seguros Privados* atribuyendo a las entidades aseguradoras la posibilidad de crear ficheros comunes para la liquidación de siniestros y la colaboración estadístico-actuarial cuya inhabilidad sea la de permitir la selección de riesgos, la tarificación o la elaboración de técnica aseguradora y para la prevención de fraude en el seguro.

La LOPD 'exime' a las entidades aseguradoras de requerir el conocimiento previo del afectado, pero

exige la comunicación, en todo caso, al afectado de la posible cesión de sus datos a dichos ficheros para los fines señalados, con expresa indicación del responsable para posibilitar el ejercicio de las facultades del acceso, rectificación y cancelación.

Respecto del segundo tipo de ficheros comunes para prevenir el fraude en el seguro la LOPD establece una excepción genérica al consentimiento del titular de los datos para su introducción en ficheros de prevención del fraude en el seguro.

No obstante, para paliar los posibles efectos negativos de dicha excepción exige la comunicación al afectado de la primera introducción de sus datos, del responsable del fichero de la finalidad del mismo y de las formas de ejercitar los derechos de acceso, rectificación y cancelación.
La amplitud de la denominada clausula *de renuncia al secreto médico* depende del tipo de seguro contratado y de la entidad aseguradora. En unos casos la exoneración de la obligación de secreto profesional se limita únicamente al médico de su compañía aseguradora. En otros, dicha clausula, genéricamente incluida en los seguros de vida, de enfermedad o de accidentes, puede ser más amplia, autorizando al asegurado los médicos que le han tratado, así como a centros asistenciales públicos o privados, a dar toda la información que el asegurador pueda solicitar.

Al margen de la asistencia sanitaria, la *ley 41/2002* , *art. 16* apartado tercero, permite la utilización de datos contenidos en la historia clínica para algunas de estas penalidades jurídicas, epidemiológicas, de salud pública, de investigación y de docencia.

Por su parte, la '*Declaración Internacional sobre los Datos Genéricos Humanos' de 16* de Octubre de 2003, teniendo en cuenta :

- La Declaración Universal de Derechos Humanos de 1948

- Los Pactos Internacionales de las Naciones Unidas referentes a los Derechos Económicos, Sociales y Culturales y a lo Derechos Civiles y Políticos de 1966

- La Convención Internacional de las Naciones Unidas sobre eliminación de

todas las formas de Discriminación Racial de 1965

- La Convención sobre la eliminación de todas las formas de discriminación racial contra la mujer de 1979

- La Convención de las Naciones Unidas sobre Derechos Del Niño de 1989

- Las resoluciones del Consejo Económico y Social de las Naciones Unidas sobre privacidad genérica y no discriminación 2001/39 y 2003/232

- El Convenio OIT sobre las discriminación (empleo y ocupación)de 1958

- La Declaración Universal de la UNESCO sobre la Diversidad Cultural de 2002

- El Acuerdo sobre los derechos de propiedad intelectual relacionados con el Comercio, ADPIC, de 1995

- La Declaración de DOHA relativa al acuerdo sobre los ADPIC y la Salud Pública de 2001

Atendiendo a los imperativos de igualdad, justicia y solidaridad y a la vez prestando la debida consideración a la libertad de pensamiento y expresión, comprendida la libertad de investigación. El *art. 2* nos recuerda las siguientes definiciones:

- *datos asociados* con una persona identificable datos que contienen información como el nombre, la fecha de nacimiento y la dirección, gracias a la cual es posible identificar a la persona a la que se refieren

- *datos disociados* de una persona identificable. Datos no asociados con una

persona identificable por haberse sustituido o desligado toda la información que identifica a la persona utilizando un código

•obtención de *datos cruzados* el hecho de cruzar datos sobre una persona o grupo que consten en distintos archivos constituidos con objetivos diferentes

Cada individuo posee una configuración genética característica, sin embargo, la identidad de una persona no debería reducirse a rasgos genéricos, pues en ella influyen complejos factores educativos, ambientales y personales, así como los lazos afectivos, sociales, espirituales y culturales de esa persona con otros seres humanos y conlleva además una dimensión de libertad, nos recuerda el *art. 3*, en relación a la Identidad de la Persona.

Debería promoverse y crearse C*omités de Ética* independientes, multidisciplinarios y pluralistas en los planos nacionales, regional, local o institucional, de conformidad con lo dispuesto en el *art. 16* de la *Declaración Universal sobre el Genoma Humano y los Derechos Humanos*.
Dichos Comités deberían ser consultados asimismo sobre los temas que no estén contemplados en el derecho interno, según el *art. 6* no sólo debería imponer límites a este principio del consentimiento por razones poderosas al derecho interno compatible en el derecho internacional relativo a los derechos humanos

Nadie debería verse privado de acceso a sus propios derechos de datos genéticos o datos proteínicos a menos que estén irreversiblemente disociados de la persona como fuente identificable de ellos o que el derecho interno imponga límites a dicho acceso por razones de salud u orden públicas o de seguridad nacional.

Los beneficios resultantes de la utilización de datos genéticos humanos, datos proteínicos o muestras biológicas obtenidas con fines de investigación médica y científica deberían ser compartidos con la sociedad en su conjunto y con la comunidad internacional, de conformidad con la legislación o la política internas y con los acuerdos internacionales.

Afinando más nuestra puntería al citar el aún pobre desarrollo de real decreto RD 1841/1997 por el que se establecen los criterios de calidad en medicina nuclear.

Incorporando al ordenamiento jurídico español la *Directiva del Consejo 84/466/EURATOM*, sobre protección radiológica del paciente. Cita que el programa de calidad constará por escrito y estará siempre a disposición de la autoridad sanitaria competente , a los defectos tanto de auditoría como de vigilancia mencionados en los *art.16 y 17*, respectivamente, del citado Real Decreto.

La historia clínica deberá registrar el tipo y actividad en el momento de la administración del radiofármaco, los datos dosimétricos en los casos en que se considere oportuno, aquellas administraciones inadecuadas que se produjeran y los efectos y reacciones adversas de los radiofármacos.

El *Informe Jurídico 0463/2009* nos recuerda que conforme a la *Ley 26/2006 de Mediación de seguros y reaseguros privados* , en su art. 62 y 63 analiza la figura jurídica del corredor de seguros desde el punto de vista de protección de datos de carácter personal. El art. 62 regula la condición de responsable o encargado del tratamiento , que tienen los agentes de seguro, o corredores señalado en su apartado 1.c).

4.8.- Farmacovigilancia[99] e Investigación Clínica

Existe una parte de tratamiento de datos *disociados* y otra no, las prácticas referentes tanto a los Sistemas de Salud Pública como a los Laboratorios privados habrán de diferenciar bien a la información de los pacientes como a los notificadores cuya identidad no coincide con el del consumidor ya identificado.

Además de los tratamientos específicos que algunas unidades de servicio de atención al usuario y por los reglamentos que se van adoptando, cuando una unidad o laboratorio precisa de información adicional en un determinado caso, se establece contacto con el personal que realiza las anotaciones sin disponer de los datos del notificador en cada ocasión. El tratamiento que se hace de los datos, es pues, como datos disociados, aun cuando el procedimiento de seguimiento de la incidencia del estudio requiera de los datos personales tanto del consumidor y/o de su representante legal u otros notificadores.

99 La Farmacovigilancia : garantía de seguridad en el uso de los medicamentos. Perspectivas Políticas de la OMS sobre Medicamentos", WHO/EDM/2004.8. . Octubre 2004. OMS. Ginebra (pag. 44): En 1968 se puso en marcha el programa OMS de Vigilancia Farmaceútica Internacional con la idea de aglutinar los datos existentes sobre las reacciones adversa de los medicamentos . En Octubre de 2004 son 86 los países que participan en el programa.
Real Decreto 1344/2007, de 11 de octubre, que regula la farmacovigilancia de medicamentos de uso humano.

Los formatos de las notificaciones pueden producirse: vía telefónicamente, por e-mail, desde la página web del laboratorio , por correo tradicional o bien por medio del fax.

Se presupone que un laboratorio no participa activamente en la recogida de datos, esto es, sin poder acceder a la historia clínica de los consumidores.

En relación a las Investigaciones Clínicas, un ensayo clínico siempre se inicia con la redacción de un protocolo bajo la responsabilidad de un Promotor aunque es el Director del Laboratorio en última instancia el responsable del estudio científico.

El protocolo conforme a la legislación en materia de ensayos clínicos con medicamentos debe mostrar el objetivo, el diseño , la metodología, las consideraciones estadísticas y la organización de un ensayo, debiendo registrarse la versión inicial, así como sus sucesivas versiones y modificaciones.

La redacción de un protocolo conlleva la identificación única entre el conjunto de protocolos iniciados en el Centro, la denominación del ensayo clínico, el nombre y dirección del promotor, la localización de los centros donde se realizará el ensayo, el método por el cual se realizará la selección de los sujetos prestados voluntariamente al estudio, y un calendario previsto para el ensayo. El protocolo deberá ir acompañado del soporte oportuno que actualmente se le está mostrando al área de *Seguridad del Paciente*, indicando el procedimiento por el que se le va a informar.

De idéntica forma se requiere la conformidad de cada centro donde se celebrará el ensayo clínico, sumándose este escrito a las clausulas legales y económicas a las que se adhiere el ensayo.

Conforme recoge el *Código Tipo de Farmaindustria*[100] el investigador puede recopilar sujetos de estudios de las siguientes situaciones bien diferenciadas:

- por conocimiento directo de sus consultas
- por derivaciones de otros departamentos de los centros participantes
- por decisión expresa y manifiesta del sujeto

100 Agencia de Protección de Datos.Codigos Tipo.Código Tipo de Farmaindustria.
Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php

y , por articulado legal, el promotor puede encontrarse en circunstancias tales que, y aunque ajeno a su voluntad , establezca contacto con datos de carácter personal y que podrán producirse de forma casual o debido a un tratamiento de compensación económica.

En la posibilidad de semejante escenario el promotor habrá de imponer determinadas medidas que le prevengan de tal situación:

- orientándose oportunamente sobre una adecuada prevención de errores
- eligiendo con calidad un adecuado sistema de filtrado de datos
- determinando compensaciones económicas a través de las compañías de seguros
- resolviendo procedimientos de comunicación entre el investigador y el propio promotor

Una vez ocurrida la situación descrita se puede optar por la cancelación de los datos del sujeto o aplicando un nivel de seguridad de nivel categorizado como Alto al fichero donde se le proporciona contenedor.

Considerando el caso de de un *CRO* o participación de empresa a terceros o outsourcing se establecerán las medidas de seguridad decididas en el párrafo anterior y que el proveedor se verá obligado a implementar. Idénticamente se exige el consentimiento informado de aquellas persona cuyos datos serán cedidos a las compañías de grupo a la que pertenecen . Las comunicaciones realizadas a las autoridades sanitarias no precisarán del consentimiento informado cuando se produzca un procedimiento de urgencia, por ejemplo.

4.9.- Soportes

Se aporta la consideración de la perspectiva que proponen el *Esquema Nacional de Seguridad*, el *Esquema Nacional de Interoperabilidad* y la aplicación de un Esquema de Certificación desde una norma internacional ampliamente aceptada en torno a la Seguridad de los Sistemas de Información.

La mayor preocupación en torno al *Esquema Nacional de Seguridad, ENS*, formulado desde el *RD 03/2010* se presenta en torno a la naturaleza del dato y el nivel de seguridad que se le debe aplicar , así como de aquellos documentos que en el seno de la e-Administración quedan repercutidos por su aplicación.

4.9.1- ISO/IEC 27 002

La norma ISO 270001 se considera parte de un conjunto de estándares, denominado ISO/IEC 27000 y desarrollados por *ISO, International Organization for Standardization*, e *IEC , International Electrotechnical Commission* y que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Practicado originariamente como un *Código de Buenas Prácticas* , después de 10 años de existencia y con más de 1 700 Empresas certificadas , en 2005 se publicó con este nombre el Esquema de Certificación ISO 27001[101] por ISO, que establece los requisitos de un sistema de seguridad de la información para ser certificable por una entidad independiente.

La norma ISO 27001 enumera en su Anexo A los objetivos de control y controles que desarrolla la ISO 27002. aun cuando no resulta obligatoria la implementación de la totalidad de dichos controles, la organización deberá argumentar la no aplicabilidad de los mismos.

En 2007 se le reconoce el nombre a la ISO 27 002, aun cuando se mantiene el 2005 como año de edición. Contiene 39 objetivos de control y 133 controles agrupados en 11 dominios. Se trata, como hemos comentado, de una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información y no es certificable.

En la ayuda de expresión de un *requisito* encontramos que podría ser que ninguna violación de la

101 La *BSI, British Standards Institution ,* equivalente a la española AENOR, publica este código de buenas prácticas en 1995. En España esta norma se la conoce conoce como UNE-ISO/IEC 27001

seguridad de la información debe provocar perjuicios económicos graves y/o comprometer a la organización. De forma que el Sistema informático al que continuamente nos remite el estándar sería el *ISMS, Information Security Management System*, que se conforma como aquella parte del *Sistema de Gestión General* basada en un enfoque de riesgo empresarial que se establece para crear, implementar, operar, supervisar, mantener y mejorar la Seguridad de la Información.

Aparece el concepto de *Declaración de Aplicabilidad*, declaración documentada que describe los objetivos de control que son relevantes para el *SGSI, Sistema de Gestión de Seguridad de la Información* (traducción al castellano) y aplicables al mismo. Los objetivos de control y los controles se basan en los resultados y conclusiones de la evaluación de riesgos, en los requisitos legales o reglamentarios, en las obligaciones contractuales y en las necesidades empresariales de la organización en materia de seguridad de la información.

La norma propone que elaborar una *Declaración de Aplicabilidad* deberá incluir:

1.- los controles seleccionados y las justificaciones de su selección

2.- los controles actualmente implementados

3.- la exclusión de cualquier objetivo de control de su Anexo A y la justificación de dicha exclusión

Sus clausulas argumentan sobre un determinado número de categorías de seguridad cuya relación es la siguiente:

a) Política de Seguridad[102]

b) Organización de la Seguridad de la Información

102 RD 03/2010. Anexo IV. Glosario: *Politica de Seguridad* (Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la informaión y los servicios que considera críticos)

c) Gestión de los Activos

d) Seguridad de Recursos Humanos

e) Seguridad Física y Ambiental

f) Gestión de Comunicaciones y Gestiones

g) Control de Acceso

h) Adquisición, Desarrollo y Mantenimiento de *Sistemas de Información*

i) Gestión de Incidentes de Seguridad de la Información

j) Gestión de la Continuidad Comercial

k) Conformidad

A su vez cada Categoría de Seguridad contiene:

a) un objetivo de control que establece lo que se debiera lograr

b) uno o más controles que se pueden aplicar para lograr el objetivo de control

En cada clausula el denominado lineamiento de implementación se produce en relación a la inclusión de una explicación breve de las políticas, principios, estándares y requerimientos de la conformidad de la seguridad de particular importancia para la organización, incluyendo:

1. conformidad con los requerimientos legislativos, reguladores y restricciones
2. educación, capacitación y conocimiento de la seguridad
3. gestión de la continuidad del negocio
4. consecuencias de las violaciones de la política de la seguridad de la información

Los *Acuerdos de Confidencialidad*[103] o no-divulgación debieran tener en cuenta el requerimiento de proteger la información confidencial utilizando términos legalmente ejecutable. Para identificar dichos requerimientos de debieran considerar los siguientes elementos:

a) proceso de notificación y reporte de divulgación no autorizada o incumplimiento del acuerdo de información confidencial

b) condiciones para el entorno o destrucción de la información una vez que se termina el acuerdo

La ISO 27002 incluye la identificación del término *propietario* que se precisa aclarar por encontrar en este texto una acepción particular: en la creación y gestión del SGSI, la identificación de los riesgos promueve la identificación de los activos que están dentro del ámbito de la aplicación del SGSI y a los propietarios de los activos, entendiéndose por el término 'propietario' a un individuo o una entidad al que se ha asignado la responsabilidad administrativa para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término propietario no significa que la persona tenga realmente algún derecho de propiedad sobre el activo.

La seguridad de la información y los niveles de procesamiento de información no debieran ser reducidos por la introducción de productos y servicios de grupos externos. Debiéndose cualquier acceso a los medios de procesamiento de información de la organización realizado, sobre todo, por grupos externos.

103 Lineamiento de implementación de la clausula 6.1.5 ISO 27002

La identificación de los riesgos relacionados con el acceso del grupo externo toma en cuenta los siguientes puntos, conforme al control 6.2.1:

a) los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo

b) el tipo de acceso que tendrá y los medios de procesamiento , dígase: acceso físico, lógico, conectividad de red, o si el acceso se da fuera o dentro del local

c) el valor y la sensibilidad de la información involucrada

d) los controles necesarios para proteger la información que no está destinada a ser accesible por dichos grupos

e) los diferentes medios y controles empleados por el grupo externo cuando almacena, comunica, comparte e intercambia información

f)condiciones para la continuación del acceso en caso de un incidente en la seguridad de la información

Entre sus subclausulas, la nº 6.2.2 aboga por concretar:

a) la protección de activos, incluyendo restricciones sobre el copiado y divulgación de información

b) acuerdos para el reporte , notificación e investigación de las inexactitudes de la información, incidentes de seguridad de fallas en la misma

c) el derecho a monitorear , y revisar, cualquier actividad relacionada con los activos de la organización

d) derechos de propiedad intelectual y la asignación de derechos de autor y protección de cualquier trabajo cooperativo

Proponiendo que resulta el mayor grado de dificultad su Gestión en todos los ámbitos el tratamiento con Grupos Externos o Terceros, encontrará la máxima expresión de desarrollo en torno a los Soportes los ámbitos de Inventariado y Soportes cualesquiera que fuera la naturaleza que se les reconociera.

La subclausula 7.1.1 de la ISO 27002 en la especificación del control afirma que se debieran identificar todos los activos , debiéndose elaborar y mantener un inventario de todos los activos importantes. Los tipos de activos que podemos considerar son:

a) información: bases de datos, controles y acuerdos, documentación del sistema, información de investigaciones, manuales de usuario, procedimientos operaciones o de soporte, acuerdos para contingencias, registros de auditoría e investigación archivada

b) activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades

c)activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo

d)servicios: servicios de computación y comunicación, servicios generales

La información deberá clasificarse en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización.

En el caso de devolución de activos se seguirán procedimientos elaborados a tal fin que refleje dicha transferencia y la oportuna información debidamente borrada. A fin de asegurar su continua disponibilidad e integridad se procederá al adecuado retiro de los derechos de acceso.

Se deberá realizar un continuo chequeo de la 'adherencia' de los acuerdos, monitoreando consecuentemente los *niveles de desempeño* subscritos, revisando especialmente los rastros de auditoría a terceros así como los registros de eventos de seguridad. La organización debiera asegurarse de mantener 'visibilidad' en las actividades de seguridad como la gestión del cambio, identificación de vulnerabilidades y reporte/respuesta de un incidente de seguridad a través de un proceso, formato y estructura de reporte definidos.

El *Marco de la Excelencia a*bordado en el Cap. IV puede ser identificado por la clausula 10.3.1 en relación a la *Gestión de la Capacidad*, de modo que las proyecciones de requerimientos futuros debieran tomar en cuenta los requerimientos de los negocios y sistemas nuevos y las tendencias actuales, proyectados todos ellos en las capacidades de procesamiento de la información de la información.

En relación a la dedicación que le vamos a proporcionar a la *Ingeniería del Software* incorporamos la consideración especial de las clausulas

- 12.4.3 de Control al Código Fuente del Programación

  El personal de soporte no debiera tener acceso irrestricto a las bibliotecas de fuentes de programa

  La actualización de las bibliotecas de fuentes de programa para los programadores sólo se debieran realizar después de haber recibido la apropiada autorización

  Se debiera mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes de programas

- 12.5.3 de Restricciones sobre los cambios en los Paquetes de Software

Si son necesarios cambios , se debiera mantener el software original y se debieran aplicar los cambios en una copia claramente identificada.

Se debiera implementar un proceso de gestión de actualizaciones del software para asegurar que la mayoría de los parches aprobados hasta la fecha y las actualizaciones de la aplicación se instalen para todo el software autorizado. Todos los cambio debieran ser probados y documentados, de manera que puedan reaplicados, si fuera necesario, a las futuras actualizaciones del software. Si fuese requerido, las modificaciones debieran ser probadas y validadas por un organismo de evaluación independiente

4.9.2- Desarrollo Esquema Nacional de Seguridad: RD 03/2010

En respuesta al artículo 42.2 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos y a través del *Esquema Nacional de Seguridad, ENS,* se cumple el objetivo de establecer los principios de una política de seguridad en la utilización de aquellos medios electrónicos que permitan la adecuada protección de los Sistemas de Información.

Reconoce el RD 03/2010 que recoge el Esquema la fuerte imbricación que se está produciendo entre el sector público y privado por dar cobertura a dicho ENS y añadimos que el futuro no viene sino en considerar unos esfuerzos de convergencia en la Interoperabilidad de los Sistemas Informáticos de forma más global, pues ya se vislumbra su debilidad definitoria en torno al dato médico a través de dichas plataformas, con lo que convenimos que el legislador Europeo habrá de ir encontrando el camino para no resultar no sólo confuso sino poco creíble.

Es cierto que de una forma más local se están abriendo canales legislados para ir dando vía y simpatía a dicha apertura, como ocurre con la *Ley de Transparencia*, que viene a considerar tratamientos de la información hasta ese momento oculta y no viable para el ciudadano, y elevando el sustrato legal de las comunicaciones administrativas sobre los que soportar los requerimientos tecnológicos y de seguridad.

Forman parte de la seguridad, como protección de información almacenada y en tránsito, los procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

A fin de dar cumplimiento a los requisitos mínimos de seguridad del ENS reflejados en la *Política de Seguridad* que deberá ser aprobada por el titular del Órgano Superior de la Administración Pública competente:

a) Organización e implantación del proceso de seguridad

b) Análisis y gestión de los riesgos

c) Gestión de personal

d) Profesionalidad

e) Autorización y control de los accesos

f) Protección de las instalaciones

g) Adquisición de productos

h) Seguridad por defecto

i) Integridad y actualización del sistema

j) Protección de la información almacenada y en tránsito

k) Prevención ante otros sistemas de información interconectados

l) Registro de actividad

m) Incidentes de seguridad

n) Continuidad de la actividad

o) Mejora continua del proceso de seguridad

, se aplican Medidas de Seguridad indicadas en su Anexo II, y que pueden pertenecer al marco organizacional, operacional y de protección. Para dar cumplimiento a dichos requisitos mínimos las Administraciones Públicas tienen en cuenta: los activos que constituyen el sistema, la categoría del sistema y aquellas decisiones que se adopten para gestionar los riesgos identificados. Además y sin perjuicio de aplicación del ENS se contempla la legislación en materia de protección de datos de carácter personal , *LO 15/1999*, conocida como *LOPD,* conforme a la naturaleza del dato.

La Seguridad como función diferenciada que delimita el *Esquema Nacional de Seguridad*, ENS, diferenciará en los sistemas de información al:

- responsable de la información
- reponsable del servicio
- responsable de la seguridad

Siendo la *Política de Seguridad* de la organización la que detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

En relación a las líneas de defensa , nos recuerda el art. 8 *RD 03/2010*, el sistema ha de disponer de

una estrategia de protección constituida por múltiples *Capas de Seguridad*, de forma que cuando una de ellas falle se permita reaccionar con tiempos suficiente frente a los incidentes, reducir la probabilidad de que el sistema sea comprometido en su conjunt0 y se minimice el impacto sobre el mismo. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Sean cuales se reconocieran la naturaleza de dichas medidas , la relación seleccionada de las mismas se formalizará en un documento denominado *Declaración de Aplicabilidad* que habrá de ser firmado por el responsable de la seguridad del sistema.

Recordemos, que por su parte deberá existir un *Documento de Seguridad* asociado a la aplicación de Medidas de Seguridad de los Ficheros del Sistemas Informático en consideración a la naturaleza del dato, los Niveles de Seguridad y la Categoría que se hubiera concedido al Sistema.

Las Medidas de Seguridad que se establezcan serán proporcionales a :

a) las *Dimensiones de Seguridad* relevantes: se reconocen como aquellas indicadas en el Anexo IV del real decreto

a.1) *disponibilidad:* propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren

a.2) *autenticidad*: propiedad o característica consistente en que una entidad es quien a de ser o bien que garantiza la fuente de la que proceden los datos

a.3) *integridad*: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada

a.4) *confidencialidad*: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, o entidades o procesos no autorizados

a.5) *trazabilidad*: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad

La determinación del nivel de seguridad adscrito para cada dimensión se lleva a cabo determinado las consecuencias de un incidente de seguridad (siempre de ha de dar por hecho que se produce alguno, para mantener activa su Gestión) sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados:

b.1) Nivel *Bajo*: suponiendo un perjuicio 'limitado'

b.2) Nivel *Medio*: supongan un perjuicio 'grave'

b.3) Nivel *Alto*: supongan un perjuicio 'muy grave'

b) la categoría del sistema resulta algo más compleja de evaluar: si alguna de sus *Dimensiones de Seguridad* alcanzara alguno de los Niveles de Seguridad anteriormente comentados el Sistema de Información obtendrá dicha calificación de Categoría de Sistema

Considerando que estamos contemplando como posible medida de seguridad aquella que operara en un nivel lógico, por tratarse el activo principal de software, podríamos atrevernos a distinguir que la discusión planteada desde el Grupo de Trabajo Gt29 según consta en el Documento WP 195 en torno a la caracterización , responsabilidades, derechos y deberes de un Controlador y un Procesador en materia de protección de datos, podríamos extrapolarla a su establecimiento , en analogía a la consideración de dos Niveles añadidos de Seguridad:

1. Nivel E1: con carácter de orientación de defensa estatal
2. Nivel E2: con carácter de orientación de defensa supranacional

Siendo el anteriormente explicado[104] un Nivel E0.

En esta Tesis y como hilo para condicionar la expresión de una posible propuesta técnica razonada en lenguaje de auditoría vamos a proponer la localización de una infracción categorizada como *grave* , art. 44 . e) y f), LOPD, por impedimento u obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que se solicitara, o bien mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas.

Y, en consideración a la máxima exposición que puede encontrar una falta muy grave, la expresa la Constitución de acuerdo al art. 44.4.e) de la LOPD, la transferencia temporal o definitiva de datos de carácter personal que hubieran sido objeto de tratamiento o fueran recogidos para someterlos a dicho tratamiento, y con destino a países que no proporcionaran un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos. En cualesquiera caso, dichas transferencias deberán ser notificadas al Registro NOTA de notificación de ficheros.

Además, continuando con la consideración de los Niveles de Seguridad, habremos de observar su aplicabilidad la *Certificación de Productos* , según el art. 18, que indica que el *Organismo de*

104 1.- European Data Protection Supervisor. The transfer of personal data to third countries and international organisations by EU institutions and bodies. Julio 2014 : no desdice la Regulación (EC) No 45/2001 en el contexto de las transferencias internacionales, art.5 , estableciendo los diferentes campos en los que la información personal puede ser procesada. Esto implica que antes de que la transferencia tuvieraa lugar, el Controller determinará cual consideración es de aplicación: a) la actividad previa a la transferencia de ser legal (recolección, almacenaje, etc) y b) la transferencia debe ser igualmente legal (en concordancia con el proposito del procesado)
Disponibleen:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf
2.- clausule 7.7.10.3 of Monitoring system use, ISO 27799: In addition to following the guidance given by ISO/IEC 27002, the health information system's audit logging facility should be operational at all times while the health information system being audited is available for use. Health information systems containing personal health information should be provided with facilities for analysing logs and audit trails that: a) allow the identification of all systems users who have accessed or modified by a given subject of care's record(s) over a given period of time b) allow the identification of all subjects of care whose records have been accessed or modified by a givne system user over a given period of time

Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

Del conjunto de Medidas de Seguridad Propuestas por el ENS y a seleccionar para incluir en la *Declaración de Aplicabilidad* la número 4.6.2 denominada *Sistemas de Métricas, op.mon.2*,queda más ampliamente expuesta en el apartado 6 del presente capítulo.

No dejamos sin consideración al Organismo reconocido como centro de excelencia promovido por el Ministerio de Industria, Turismo y Comercio para el desarrollo de la Sociedad del Conocimiento, Instituto Nacional de la Comunicación , INTECO, en observación de los Cursos que publican en su página Web y en un seguimiento mayor que se hace de la consideración y apoyo del Marco de la Excelencia aplicada a la Administración Pública conocido como *CAF, Common Assessment Framework*, para la Solución que se propone, Cap. IV, 2.7.

5.- Evaluación del Impacto en la Protección de Datos Personales, EIDP o PIA, Privacy Impact Assessment

Aun no existiendo, a fecha actual, obligación legal en España de llevar a cabo una evaluación del impacto en el área de la protección de datos, la *Agencia Española de Protección de Datos* sugiere[105] la incorporación de este tipo de evaluaciones como una herramienta madura y cuyo uso puede contribuir a la mejora de políticas y prácticas de protección de datos de la organizaciones que las adopten.

105 Agencia Española de Protección de Datos. "Guía para una Evaluación del Impacto en la Protección de Datos Personales, EIPD". 2014

Considerándose como medida proactiva o instrumento[106] que permite identificar, eliminar o mitigar los riesgos asociados que presenta para la privacidad de las personas todo sistema que trate datos de carácter personal.

Como parte del proceso de una EIDP las organizaciones describirán cómo la información se recolecta, almacena, usa o borra. Debería poder explicar, así mismo, su uso y quién tendrá acceso al mismo. Tan sólo se considerará superado un correcto análisis de los riesgos de este modo. Cada riesgo identificado y su estado´debería apuntar concretamente a una de las siguientes posibilidades:

- su evitación o eliminación
- su mitigación
- su aceptación
- su transferencia

Como instrumento las EIDP pueden integrarse dentro de las metodologías y herramientas de *Gestión de Proyectos* o de *Análisis de Riesgos*. Una EIDP, por tanto, es una herramienta orientada a procesos y no a generar un documento, aunque no se deba descuidar el contenido del mismo, ya que permitirá canalizar el flujo de información destinado a la Dirección.

Entre los riesgos que cita la *Agencia de Protección de Datos* a incluir y derivados de una falta de percepción respecto de la privacidad o de las expectativas de su cumplimiento se cuenta con:

- la aparición o el incremento de los costes de rediseño del sistema e, incluso, la retirada del mismo

106 Information Commissioner's Office, ICO. Conducting Privacy Impact Assessmentes . Code of Practice. Data Protection Act. Version 1.0. February 2014
Parte integral en la aproximación del desarrollo de un *Diseño por la Privacidad*, permitiendo a una organización de forma sistemática analizar como un proyecto particular o sistema puede afectar a la privacidad de los sujetos involucrados. De forma que el desarrollo de una PIA beneficia tanto a la gente afectada por el proyecto como a la organización que desarrolla el proyecto, permitiendo saber al individuo cómo un proyecto le puede afectar. Algunos de las formas por las que puede aflorar un determinado riesgo en relación a una información personal es porque ésta sea: inadecuada, insuficiente o fuera de fecha, excesiva o irrelevante, mantenida por tiempo excesivo, usada de forma inaceptable o no mantenida de forma segura

- la falta de apoyo de actores clave para la viabilidad del proyecto

- la pérdida de reputación e imagen pública

- la posibilidad de acciones de investigación y, en su caso, sancionadoras por parte de la autoridad de protección de datos competente

Un aspecto fundamental en una EIDP resulta la *Verificación de la Conformidad* del proyecto con las diferentes regulaciones existentes en relación a la Privacidad y la protección de Datos. Además y dependiendo del sector en el que se mueva el proyecto pueden existir obligaciones adicionales como es el caso de las legislación sanitaria.

Una forma de llevar a cabo estas revisiones es por medio de auditorías periódicas y que pueden integrarse aunque no confundirse con las establecidas por el desarrollo de la *LOPD, RLOPD RD 1720/2007*.

Recordamos, pues, que una EIDP es una herramienta que va más allá del cumplimiento normativo, aunque su verificación se encuadra dentro de las expectativas que tienen los ciudadanos en todo tratamiento de protección de datos.

Una vez que el proyecto de una EIDP hubiera concluido las auditorías deberían permitir discernir en qué grado fueron superados los riesgos que fueron previstos en ella.

Se considera aconsejable llevar a cabo una Evaluación del Impacto en las siguientes situaciones:

- en nuevas recogidas de datos, o cuando las existentes perfilaran nuevas finalidades, o bien cuando las finalidades resulten más intrusivas o inesperados sus resultados

- en casos significativos de tratamiento de datos de menores, sobre todo cuando fueran menores de catorce años

- cuando se toman medidas que producen efectos jurídicos sobre las personas o que afectan su integridad personal

- ante decisiones que conllevan riesgo de discriminación (económica, social, política, etc)

- ante tecnologías conceptuadas como invasivas como la videovigilancia, técnicas genéticas, geolocalización,..

- en cesiones o comunicaciones de datos personales a terceros

- transferencias a países que no forman parte del Espacio Europeo

- por fines estadísticos, históricos o de investigación científica

- datos especialmente protegidos

- por compromiso con las *Dimensiones de Seguridad* (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad), y especialmente en el uso de Redes de Telecomunicaciones

6.- Orientación a una Propuesta ISO/IEC 27 002- ISO/IEC 27 799

Entre los diferentes modos[107] que existen de representar los requerimientos elegimos aquellos elementos basados en el escenario de modo que el sistema se describe desde el punto de vista del usuario con el empleo de un enfoque basado en este.

Cada elemento que añadimos al modelo de requerimientos, siendo estos requerimientos con representación informática o requerimientos informáticos por encontrarnos en el ámbito de la Solución en el Marco de la *Ingeniería del Software*, se adopta para afrontar inconsistencias, omisiones y ambigüedades; de manera, que podemos otorgarles prioridades y agrupar en paquetes de

107 PRESSMAN, Roger. "Ingeniería del Software: Un Enfoque Práctico". PH. D. 7º de. 2010. University of Connecticut. Cap. 5. : 1. basados en el escenario, 2. basados en clases (cada escenario de uso implica un conjunto de objetos que se manipulan cuando un actor interactúa con el sistema. Estos objetos se clasifican en clases como conjunto de objetos que tienen atributos similares y comportamientos comunes) 3. elementos de comportamiento (que mediante diagramas de estado indican acciones tomadas como consecuencia de un evento particular)

requerimientos cuya representación lógica adopta el de un incremento de software.

Cada actor encuentra su propia operatividad o uso dentro del modelo, de manera que el personal dedicado por vocación y contrato al área del aseguramiento de la Calidad contará con una ayuda en el planteamiento de las Pruebas de Aceptación.

Al nivel del *Análisis del Dominio* que no es otro que la identificación, análisis y especificación de dichos requerimientos localizamos elementos comunes para la solución de un problema y que resulten útiles en todas las aplicaciones dentro del dominio.

El proceso del *Análisis del Dominio* se considera un proceso de aprendizaje del *Ingeniero de Software* en el que descubre patrones de software como mecanismo para capturar conocimiento del dominio, de modo que podrá aplicarse y extrapolarse, por analogía, a otros dominios.

Luego, respetando y considerando los diferentes modelos o *Ciclos de Vida*[108] que se le hubieran concedido a las diferentes soluciones software con la que cuenta nuestro Sistema Informático, debemos recordar que estamos persiguiendo encontrar una nueva funcionalidad resultado de un *Análisis de Riesgos* previos de los *Activos* de la Sección de la e-Administración que nos ocupa (Cap. III y IV).

De detectar la necesidad de implementar una Salvaguarda Técnica como *Medida de Seguridad* y como consecuencia del Análisis al que se va a proceder , probablemente, y debido a la extrema complejidad y amplitud que alcanzará nuestro Sistema Informático, optaremos por definir, implementar e integrar algún componente débilmente acoplado. Los fundamentos de esta *Ingeniería del Software basada en Componentes* es ampliada en la Sección 2.8 del Cap. IV. Con lo que ya se presume se iniciará una discusión acerca de su Certificación[109] y que no desdice sino que confirma alguna obviedad en el *Esquema Nacional de Seguridad* a día de hoy, y que ha de respetar de cualesquiera forma el SNS en el *Marco Nacional de Interoperabilidad*[110].

108 Modelos en Cascada, Evolutivos(Prototipos), basados en Componentes, en Espiral , basados en las transformaciones (métodos formales), Métodos Agiles (Programación Extrema), etc, ..

109 RD 03/2010, art. 18 y Anexo I, op. pl. 5 Componentes Certificados

110 RD 04/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la

La unidad de software independiente en que se constituye un *Componente* puede estar, a su vez, compuesta por otros componentes aun cuando se trata de evitar esta situación.

El Diseño del Componente Software tan sólo se llevará a cabo como consecuencia del reforzamiento de alguna singularidad que vaya entretejiendo el conjunto de capítulos de esta Tesis, y que como se verá es a resultas de sumar los resultados y observaciones originadas desde las Secciones siguientes:

1. Cap. I: reforzamiento de taxonomía
2. Cap. II: no obviedad+no olvido del inicio de los Sistemas Informáticos Europeos

Aun cuando de momento debamos aun introducir un Análisis del *Estado del Art*e en consideración a los *Riesgos Legales* (Cap. III) y practicar algunos Indices de Documentos (Cap. IV), y cuyo trabajo ya se inicia con la norma internacional ISO 27 001 .

En 2008 se publica la ISO 27799 que se trata de un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 27002. A diferencia de las anteriores ISO 27001 e ISO 27002 no la desarrolla el subcomité JTC1/SC27 sino el Comité Técnico TC 215. ISO 27799 explicita directrices para apoyar la interpretación y aplicación en la *salud informática* de la norma ISO 27002 y resulta complemento de la misma.

Se va a considerar la Solución Propuesta como una Medida de Seguridad en relación a la *Política de Seguridad*, elevando el nivel de flujo de información que gestiona la *Unidad de Gestión de Riesgos* y valorándose para cada Actor de la e-Administración reflejado en la Tabla 2, Cap. I su aplicación, que es donde encontramos deficitaria su Defensa Jurídica.

Prestando elevada consideración a la aplicación de un correcto nivel de acceso como consta en los orígenes de los Sistemas Informáticos Europeos y se trata de no perder su orientación en el Artículo 2 del Anexo de esta Tesis.

Administración Electrónica

Elevamos la fórmula de la Propuesta a su discusión práctica en la aplicación de su Esquema de Certificación, Cap. IV , Tabla 6.

La adopción del Esquema P.D.C.A. (Plan, Do, Check, Act) definido en las directrices de la OCDE (2002) es apoyado tanto por la ISO 27001, 27002, 27799 como por la propuesta de Evaluación de Impacto en protección de datos, EIPD, cursada por la Agencia Española de Protección de Datos.

El Modelo del Esquema a seguir a fin de no incurrir en consideraciones mayores sería:

1. la aplicación de un modelo en gestión de riesgos, por ejemplo, la *Metodología en Gestión de Riesgos* propuesta por la Administración Francesa[111]

2. la supervisión del sector sanitario con la ISO 27799

3. la aplicación de un PDCA sobre consideraciones críticas en la norma ISO27002

Un riesgo resulta un escenario que nos describe de qué modo las fuentes de riesgos pueden explotar las vulnerabilidades asociadas a los activos, provocando , como consecuencia de un incidente en el activo e impactos en la privacidad. La Metodología de Riesgos propuesta estima el nivel asociado a un riesgo en término de severidad y probabilidad.

La severidad representa la magnitud de un riesgo; esencialmente depende del nivel de identificación del dato personal y del nivel de las consecuencias del impacto potencial.

La probabilidad representa la facilidad de que un riesgo ocurra; dependerá del nivel de vulnerabilidades de los activos soportados que a su vez dan soporte al nivel de capacidades de las fuentes de riesgo para explotarlas.

111 Metodology for Privacy Risk Management. How to Implement the Data Protection Act. Commission Nationale de l'Informatique et des Libertés, CNIL Edicion 2012

De este modo, estamos afrontando los riesgos a través de medidas proporcionadas. Este nuevo inventario de datos personales debe servirnos como una nueva oportunidad para verificar si cada elemento de datos resulta absolutamente necesario en el procesado de las operaciones y si se ha establecido un periodo adecuado para su almacenaje.

A fin de ayudarnos en la larga cadena de verificaciones que puede suponer la trazabilidad de un riesgo, se identifican los siguientes niveles de identificación de datos personales

- negligible: resulta prácticamente imposible la identificación de un individuo
- limitado:la identificación es difícil
- significante:la identificación es relativamente sencilla
- máximo:la identificación es muy sencilla

En relación a la observación de la ISO 27799 nos recuerda esta norma que la integridad de la información del paciente debe ser protegida a fin de asegurar la Seguridad del Paciente y un importante componente de dicha protección es el asegurar que el ciclo completo de la vida de la aplicación sea auditable.

La norma define la *personal health information* como aquella información existente de la persona y que permite su identificación de la misma relativa a su salud mental o física o bien a la provisión de servicios de salud, y entre las que se incluyen:

a) información sobre su registro para la provisión de los servicios médicos

b) información acerca de pagos o decisiones responsables

c) un número o símbolo asignado para su representación

d) cualesquiera información del individuo recopilada en la provisión de los servicios médicos

e) información derivada de pruebas o exámenes realizados sobre el cuerpo o sustancias del mismo

f) identificación de la persona como proveedor de cuidados médicos

En el contexto de la seguridad de la información en sanidad una activo es cualquier cosa que tenga valor para la organización, incluyendo: la comentada *personal health information*, servicios tecnologicos informático, hardware, software, facilidades de comunicación, lo que se denomina como media, dispositivos médicos para el almacenaje y reporte de los datos.

Reitera la ISO 27799 que existen algunos tipos de información cuya confidencialidad, integridad y disponibilidad debe ser protegida:

a) la *personal health information*

b) datos seudoanónimos e implementados sobre alguna metodología orientada a tal fin

c) datos estadísticos y de investigación, incluyendo los anónimos derivados de borrados

d) conocimiento médico no asociado a atenciones particulares

e) datos de los profesionales de la salud, plantilla y voluntarios

f)datos que permitan la trazabilidad en una auditoría , generados por el sistema de información en sanidad

g) información del sistema de seguridad, incluyendo el acceso de control

De ningún modo se debe adoptar el estándar ISO 27002 como una *checklist*, error muy practicado en el entorno sanitario y consideración que nos lleva a considerar la evidencia de la existencia del soporte a Gestión previo a asegurar su cumplimiento. Esta consideración nos conduce a contar tanto con comunicaciones escritas como verbales a tal fin.

El objetivo de su aplicación debe, así mismo, ser ampliamente propagada a través de la organización, definiendo sus límites en términos de procesos, lugares , plataformas y aplicaciones[112].

ISO 27001 define como componentes del análisis de riesgos y de su gestión[113]:

a) la identificación de los activos, amenazas y vulnerabilidades

b) el impacto sobre los activos

c) la probabilidad y vulnerabilidad de la amenaza

d) determinación de los niveles de riesgo

e) identificación de los controles de seguridad

f) comparación entre controles,que permitan la identificación de áreas de riesgos residuales

g) opciones en el tratamiento de riesgos,incluyendo los de gestión, aceptación del

112 Clausula 6.4.1.6 ISO 27799
113 Clausula 6.4.4.3 ISO 27799

riesgo, permisibilidad, transferencia, etc.

h) planes de tratamientos de riesgos y de los activos

i) registro de aquellos controles que no se considerara vigilar de la ISO 27002

Las revisiones del documento de la Política de la Seguridad del Sistema de Información debería incorporar y reflejar las siguientes consideraciones:

a) la naturaleza cambiante de las operaciones de la organización y los cambios concomitantes sobre el perfil de riesgos detectado y las necesidades de la gestión de riesgos

b) cambios realizados sobre la infraestructura informática y las consecuencias sobre el perfil de riesgos existente

c) cambios identificados en el entorno externo y que provocan un impacto sobre el perfil de riesgos detectado

d) los últimos controles, requerimientos y planes derivados de la aplicación de la legislación y regulaciones surgentes

e) recopilación de de las últimas guías y recomendaciones provenientes de asociaciones y funcionarios de Organismos Reguladores en materia de Datos de carácter personal

f) el resultado de casos defendidos y que establezcan precedentes o prácticas establecidas

g) indicaciones expresas a la Política de Seguridad existente por parte de la plantilla,

proveedores, investigadores y gobierno incluido

De todos los requerimientos relacionados con la seguridad del dato clínico, nos confirma la clausula 7.7.10 de Monitoreo en la ISO 27799, que, entre los más importantes se cuentan con los de:

- auditoría
- logging

Efectivamente, une efectivo traceado de los logs y de sus auditorías puede ayudar a descubrir un mal uso de los sistemas de información. Pudiendo estos procesos idénticamente ayudar al individuo en su defensa contra los abusos de acceso.

De todas formas y aunque apliquemos un PDCA sobre la propuesta no debemos olvidar que en relación a las clausulas de la ISO 27002 y el Servicio Informático Sanitario que consideramos de mayor consideración y a vigilar en esta Tesis son:

1. I*ntercambios de Información*:

   Es importantísimo la determinación de lo que se espera de los empleados cuando se emplean una clara política de seguridad, procedimientos y controles sobre el SGSI.

   En concreto, la clausula o control A. 10.8.2 del estándar requieren de la organización establecer acuerdos formales de forma manual o electrónica, incluidos los datos personales y el software. Estos podrían incluir Acuerdos de *Escrow*[114] a considerar

114 En este caso, se recomienda una tercera parte o agente que preserven el código fuente de la aplicación para satisfacción de las clausulas del acuerdo entre ambas partes. Este agente puede tratarse de un individuo o bien de una nueva firma comercial. Esta parte suele contar con sus propios modelos de contrato que normalmente cada conciliador se encargará de completar según sus requerimientos y circunstancias. De una parte tenemos al creador o creadores de la aplicación y de otra el que compra una licencia de su uso o beneficiario. El agente mantendrá una posición neutral en la transacción respondiendo de cualquier modo del depósito que se haga de la obra. Existen una serie de temas indiscutibles a considerar en el acuerdo, como son: La frecuencia con la que habrá que renovar el depósito

- Las causas por las que habrá que variar esa frecuencia
- Las condiciones en las que se realizará
- Las consideraciones y garantías del mismo

Las clausulas del acuerdo determinarán exactamente el material suministrado al agente, el régimen de su validación

cuando cabe la posibilidad de que se salga alguna de las partes del contrato en algún momento.

El nivel de acuerdo establecido en una Gestión de Riesgos dependerá de la sensibilidad establecida para la información. Dichos acuerdos de información[115] incluyen:

---

y cada cuánto tiempo se producirá su actualización.

Además de la aportación en soporte lógico del software se incluirá documentación de su ciclo de vida. El agente deberá contar por su parte, aunque pudiera de nuevo ser contratada, con la fase de validación del correcto funcionamiento e integridad del código objeto del que fuera depositario libre de virus. Por lo tanto, este actor contará con una licencia limitada del producto mientras la propiedad intelectual perteneciera al depositario. Controlando así, el tratamiento de cada versión release.

Se contemplarán circunstancias de,

- quiebra o insolvencia de la empresa creadora
- modificaciones en tiempos establecidos
- mantenimientos frente a la conclusión del desarrollo de la aplicación
- procedimiento a seguir en caso de tardanza de cobertura de tiempos; aunque en la fase de no continuidad de la implementación de la aplicación en la empresa que ostenta la propiedad intelectual los beneficiarios suelen decantarse por no extender el litigio en el tiempo . De modo que se suelen llegar a acuerdos donde quedan cubiertos a un cincuenta por ciento los gastos surgidos de estos casos
- suspensión de pagos
- concurso de acreedores
- liquidación del programador
- cambio de actividad social de la empresa
- trasmisión de los derechos de propiedad intelectual sobre el programa a un tercero o por sentencia judicial
- caso de existir varias licencias, habrá que ver cómo se recupera el código fuente. Si bien lo más aconsejable sería que se autorizara por parte del depositario la retirada de una copia del código para cada uno de los licenciatarios

En el supuesto caso que la empresa depositaria se viera obligada a ceder parte de su material y código fuente, su titularidad quedará preservada. Algunos van más allá y se ocupan de incluir listas de las empresas que compiten con su producto ante una posible cesión de los derechos de autor.

Sus clausulas deberían ser vigentes aún antes de la concesión de la licencia al beneficiario.

Una relación parcial de los requerimientos del depósito material incluiría,

- copias del código fuente por cada versión release o código objeto en soporte magnético
- toda la documentación técnica, incluidos manuales de usuario
- herramientas de mantenimiento e integradoras con el sistema operativo
- nombres y direcciones de empleados técnicos que cubrieran una subcontratación del software ante cesiones de existencia de la empresa depositaria
- comandos de compilación de forma literaria o multimedia

- identificación de quién es el responsable del control y la notificación de la transmisión , enrutado y recepción en ambas partes del acuerdo

- procedimientos de notificación que aseguren a la otra parte que la información ha sido distribuida o recibida y que los controles técnicos aseguren fudamentalmente la trazabilidad y el no repudio

- la relación de estándares mínima destinada a empaquetamiento y transmisión

- derechos y responsabilidades si los datos se pierden o se producen incidentes de seguridad

- el sistema de etiquetado que asegure que resulta evidente la protección requerida

- donde fuera necesario responsabilidades de propiedad, copyright[116],

Y por parte de la empresa agente van a ser muy importantes el mantenimiento de unas adecuadas condiciones ambientales desde donde prevenir la humedad y oscilaciones de temperatura que eviten daños al material. Se realizará el almacenaje en una cápsula hermética que la prevenga de todo tipo de radiación electromagnética además de los propios planes de cobertura del plan de riesgos laborales de las instalaciones donde se ubique.

115 CALDER, Alan y WATKINGS Steve. IT Governance. A Manager's Guide to Data Security and ISO 27001/ISO 27002. 4th Edition. Cap. 15

116 Pueden acogerse a esta fórmula todos aquellos miembros signatarios del *Convenio de Berna*; se realiza de forma automática, sin coste y este método está universalmente reconocido.

Básicamente, aquel que firma el copyright tiene el derecho de exigir una compensación en el caso de que su código fuera utilizado sin su consentimiento.

Típicamente, una demanda sobre esta forma de protección se resuelve con prontitud en los países europeos.

Se admiten fórmulas de depósitos por terceros con la supervisión de un abogado.

Se constituye o define como una forma de propiedad intelectual que asegura a su propietario el derecho exclusivo para reproducir copias de sus obras bien sea éste literaria, musical, artística, fotográfica, de software o de diseño industrial.

Además de este derecho, se conforman otros: importar o exportar la obra, crear derivados, mostrarla, venderla o asignar estos derechos a terceros.

Cada país ofrece diferentes interpretaciones al respecto del concepto donde aún se esgrime una batalla entre su aspecto patrimonial y el moral.

Su símbolo, una c, encerrada en el interior de un círculo se ha constituido como algo opcional . Su inclusión no tiene

etc. donde competiera, estándares técnicos para la grabación y lectura

- especiales controles tales como la criptografía

2. *Seguridad en el Soporte y Procesos de Desarrollo*:

El responsable de seguridad y el responsable de la información deberían ser los que supervisaran la garantía de accesos lógicos y físicos que practican los proveedores. En cualesquiera caso, esta actividad debería resultar monitorizada.

El control o clausula A.12.5.1 de la ISO 27002 requiere un estricto control de la implementación de los cambios por medio de procedimientos que minimicen el potencial de corrupción de los Sistemas de Información.

El control o clausula A.12.5.5 de la ISO 27002 requiere de la organización la aplicación de controles que harán del desarrollo de software en outsourcing algo seguro. Cuando el software que se precisa no se puede comprar , se debe desarrollar uno propio. Previo a la habilitación del Contrato supervisado por Expertos ISO 27002 sugiere:

- licencias[117] y derechos de propiedad

la obligación de ser adoptada por aquellos países advenidos al *Convenio de Berna*, donde desde el momento de su creación estaría la obra legalmente protegida y el derecho de autor preservado.

Sin embargo, a muchos les resulta psicológicamente útil observar su presencia para prevenir posibles daños.

En la LPI , Ley de Propiedad Intelectual,el *art. 141* posibilita la inclusión de este símbolo para recordar los derechos de explotación.

Como representación oficial de este viejo concepto, intentando proteger estos derechos, más allá del *Convenio de Berna* contamos con la UNESCO donde consultando su web se aclara el estado del caso en cada país desde su Convención en 1952.

117 No lleva implícito un derecho en materia de propiedad intelectual. Pero puede especificar para cada usuario final definido, aquellos términos en que su modificación y utilización quedan determinados.

Su cobertura legal queda dependiente de la Jurisprudencia bajo la que fue comercializada, incrementándose su complejidad para aplicaciones on-line ante la dificultad, en ocasiones, de reconocer una firma digital.Es habitual en muchos ámbitos, y singularmente en el de los programas de ordenador, la utilización de "licencias" . Licencia es prácticamente lo mismo que "autorización". La LPI, Ley de Propiedad Intelectual no distingue claramente entre ambas. Suele incluir las condiciones de distribución de una obra o producción, objeto de derechos de propiedad intelectual. Sin embargo, es la fórmula que, procedente del derecho anglosajón, se viene utilizando para el uso del software.

- certificación de la calidad
- acuerdos de Escrow en caso de fallo financiero
- derechos de acceso de auditoría
- requerimientos contractuales para la calidad del código
- testeo de código malicioso
- fechas de entrega, gestión de control de cambios y medición de los límites

Licencia contractual es la autorización no transmisible dada por un titular de derechos de propiedad intelectual a favor de otra persona para, por una sola vez, reproducir, comunicar públicamente o distribuir las obras o producciones protegidas. Se llama "contractual" porque la autorización se incluye en un contrato o pacto. No es una denominación muy expresiva ni correcta, proviene de las normas de propiedad industrial (marcas y patentes) y de la práctica comercial; la Ley la usa, aunque sin definirla.Es habitual también en el mercado de programas de ordenador que los autores y fabricantes de programas "licencien" al comprador para su uso.

CAPITULO III: ANALISIS DE RIESGOS LEGALES

Abstract :

Around the L 11/2007, traditional and actual implementation of an Auditory in the Management of the Data Field. Supporting on the Standard ISO/IEC 27 001 and its parallel, the ISO/IEC 27 002: legal involvements. Aids to consider the Risk Assessment Plan given as a Table and appreciations grouped to facilitate the assimilation of possible aspects of the 'Security Document'

Claves :

Riesgos, Métricas, Magerit, Precepto Legal, Activo, Certificación, Acreditación, Criterios Comunes, CC, EAL, Salvaguarda, Requisito de Seguridad, Política de Seguridad, Plan de Calidad, Amenaza, Dimensión de Seguridad, Daño, Impacto, Centro Nacional de Inteligencia, CNI, Centro Criptológico Nacional, RD 03/2010, RD 04/2010, Clausula de Confidencialidad, TIC, ENS, Declaración de Aplicabilidad, Arquitectura de Seguridad, ISMS, SOX, ERP, COSO, PCAOB, ISO 27001, ISO 27002, Sistema de Gestión de la Seguridad, Código de Práctica, PDCA, A True International Level, Medida de Seguridad

En el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema. Y con la consideración de que el temor a lo desconocido es el principal origen de la desconfianza, en consecuencia, se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos.

Hemos tomado por definición de Riesgos la proporcionada por la Métrica utilizada en la Administración Pública Española y que ya cuenta con su tercera versión. Nos estamos refiriendo a '*Magerit*'[118].

118 El análisis y gestión de los riesgos es un aspecto clave del Real Decreto 3/2010, de 8 de enero, por el que se

Esta Norma aceptada e introducida en el mundo empresarial de los Servicios Informáticos desde 1997 define el Riesgo como indicación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización'. Aceptando, eso sí, la existencia siempre de un riesgo que debe ser conocido y sometido al *Umbral de Calidad* que se requiere del servicio.

El análisis de riesgos permite tomar decisiones de inversión en tecnología, desde la adquisición de equipos de producción hasta el despliegue de un centro alternativo para asegurar la continuidad de la actividad, pasando por las decisiones de adquisición de salvaguardas técnicas de selección y capacitación del personal.

El análisis de riesgos puede venir requerido por *Precepto Legal*. Tal es el caso del Real Decreto RD 263/1996, de 16 de Febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

El <<activo esencial>> es la información que maneja el sistema; o sea los datos.

El Análisis que se propone tal como recoge la especificación de la Tesis es una propuesta de Análisis de Riesgos Legales[119] deducibles del conjunto de capítulos anteriores y que se presentará a continuación. Aunque hemos recogido previamente algunos conceptos que se han considerado necesario expresar.

---

regula el E*squema Nacional de Seguridad, ENS,* en el ámbito de la Administración Electrónica que tiene la finalidad de poder dar satisfacción al principio de proporcionalidad en el cumplimiento de los principios básicos y requisitos mínimos para la protección adecuada de la información. MAGERIT es un instrumento para facilitar la implantación y aplicación del ENS proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información. La Metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA . Disponible en: http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html

119 Comité de Supervisión Bancaria de Basilea. "Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo". Banco de Pagos Internacionales. Enero 2004

<<Operativa Transfronteriza. 5.Gestión de la Información (a) Mantenimiento de Registros. 52. El banco deberá desarrollar y aplicar reglas claras sobre los registros que deben de mantenerse para documentar la diligencia debida practicada a los clientes y a las transacciones individuales. Si fuera posible, estas reglas deberán tener en cuenta cualquier medida preceptiva en materia de privacidad. Deberán incluir una definición de los tipos de información y documentación que habrán de incluirse en los registros, así como el período de conservación de dichos registros. 53. También deberán mantenerse registros adecuados que documentan el proceso de evaluación relacionado en el Análisis y Seguimiento continuo y con las conclusiones extraídas

>>

Disponible en: http:\www.bis.org

A modo de ejemplo, se puede exponer que una *certificación* dice que un sistema es capaz de proteger unos datos de unas amenazas con una cierta calidad o capacidad de protección. De modo, que detrás de un certificado no hay sino los conceptos de un análisis de riesgos.

Las *acreditaciones* son procesos cuyo objetivo sería legitimar el sistema para formar parte de sistemas más amplios.

*1.- **Criterios Comunes de Evaluación, CC***

La necesidad de evaluar la seguridad de un sistema de información aparece muy temprano de la mano de los procesos de adquisición de equipos del Departamento de Defensa de los EEUU que, en 1983, publica el llamado "Libro Naranja" , TCSEC – *Trusted Computer System Evaluation Criteria*.
El objetivo es especificar sin ambigüedad qué se necesita por parte del comprador y qué se ofrece por parte del vendedor, de forma que no haya malentendidos sino un esquema transparente de evaluación, garantizando la objetividad de las adquisiciones.

La misma necesidad lleva a la aparición de iniciativas europeas como ITSEC, *Information Technology Security Evaluation Criteria.* A mediados de los años 90, existe en el mundo una proliferación de criterios de evaluación que dificulta enormemente el comercio internacional, llegándose a un acuerdo de convergencia que recibe el nombre de *"Common Criteria for Information Technology Security Evaluation",* normalmente conocidos como "Criterios Comunes" o por sus siglas, CC[120].

Los CC, además de la necesidad de un entendimiento universal, capturan la naturaleza cambiante de las tecnologías de la información que, en el período desde 1980, han pasado de estar centradas en los equipos de computación, a englobar sistemas de información mucho más complejos.

Los CC permiten

120 INTECO, Instituto Nacional de Tecnologías de la Comunicación. MAGERIT; "*Metodología de Certificación Common Criteria y Perfiles de Protección del DNIe*". 2012(pag. 15): Este acuerdo internacional de reconocimiento mutuo de certificados está suscrito por las administraciones de 25 países. Se trata de un método de desarrollo seguro y sobre 7 niveles discretos de la gama de esfuerzo, incluyendo la especificación del trabajo de los evaluadores en cada nivel. Los criterios de evaluación se publican como ISO/IEC 15408, y la metodología de evaluación como ISO/IEC 18045. Hay normas nacionales semejantes derivadas de la versión ISO en China y Rusia, pero no estan actualizadas a la última versión del CC, y son utilizadas únicamente en esquemas de certificación nacionales sin reconocimiento internacional.

- definir las funciones de seguridad de los productos y sistemas (en tecnologías de la información)
- determinar los criterios para evaluar la calidad de dichas funciones

Dado que la Calidad de la seguridad requerida de un sistema no es siempre la misma, sino que depende de para qué se quiera emplear, CC permite establece una escala de niveles de aseguramiento, los EAL, *Evaluation Assurance Level*[121]:

EAL0: garantías
EAL1**:** funcionalmente
EAL2**:** estructuralmente
EAL3**:** chequeado metódicamente
EAL4**:** probado y revisado metódicamente
EAL5**:** probado semi-formalmente
EAL6**:** probado y verificado semi-formalmente
EAL7**:** probado y verificado formalmente

Los niveles superiores requieren un mayor esfuerzo de desarrollo y de evaluación.

Ofreciendo a cambio unas grandes garantías a los usuarios. Por ejemplo, en el ámbito de la firma electrónica, los dispositivos seguros de firma suelen certificarse contra un perfil de nivel EAL4+.

En CC las *Salvaguardas* reciben el nombre de *Requisitos de Seguridad* que a su vez se pueden catalogar como funcionales y de garantía.

La legislación española concreta más exactamente en el *art. 18* del RD 03/2010 que respecto de la adquisición de 'productos de seguridad' serán valorados positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición conforme a las

121 '*Evaluation Assurance Level*', EAL son los distintos niveles de seguridad asignados a sistemas y aplicaciones como consecuencia del análisis de medidas de seguridad basadas en los Criterios Comunes, ISO/IEC 15408; "Metodología de Certificación Common Criteria y Perfiles de Protección del DNIe". INTECO, Instituto Nacional de Tecnologías de la Comunicación. 2012. (pag. 21) Las siglas EAL, del inglés, "Evaluation Assurance Level", junto con el cardinal 1-7, fijan el código de referencia que permite consultar en la norma los requisitos de construcción y de evaluación que marcan cada uno de los siete niveles de evaluación (Figura 8. Niveles de evaluación)

disposiciones del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, según establece el RD 421/2004 y la Orden PRE/2740/2007.

El *art. 27* del RD 03/2010 indica en relación a los requisitos mínimos que debe satisfacer un sistema que maneje datos de carácter personal le será aplicable lo dispuesto en la LO 15/1999 sin perjuicio de los requisitos establecidos en el *Esquema Nacional de Seguridad, ENS*.

En relación a los requerimientos técnicos su *art. 32* y en su aplicación a la plataforma de *e-Sanidad*, las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos se realizarán de forma que cumplan, de acuerdo con lo establecido en el presente real decreto, las siguientes exigencias técnicas, asegurando:

- la autenticidad de organismo que lo publique
- la integridad de la información publicada
- se deje constancia de la fecha y hora de la puesta a disposición del interesado de la resolución, así como del acceso a su contenido
- aseguren la autenticidad del destinatario

*2.- **Auditorías***

El RD 03/2010 define en su Anexo IV correspondiente a la Inclusión del Glosario a la Auditoría como aquella revisión y examen independientes de los registros y actividades del Sistema para verificar la idoneidad de los controles del Sistema , asegurando que se cumple la Política de Seguridad y los Procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la Política y de los Procedimientos.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al Reglamento RD 1720/2007, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas, conforme a sus artículos *art. 96 y 110*.

Normalmente la *Política de Seguridad*, que se debe elaborar dentro de la continuidad de un *Plan de Calidad*, incluye la relación de la legislación que afecta a la Operativa de un Negocio. Es absolutamente necesario delimitar el marco legislativo y regulatorio a que debe responderse en cada caso.

Ahora bien, la existencia de datos de carácter personal independientemente de los niveles de seguridad en un sistema precisa como se ha venido exponiendo de un tratamiento específico regulado nacional e internacionalmente, y supervisado por Agencias Gubernamentales que persiguen este idéntico esquema.

Tradicionalmente la aceptación de una clausula *de conformidad* en la interacción con terceras partes, en una Empresa, incluye la aceptación de dicha legislación.

3.- Datos de Carácter Personal

La forma más realista de enfrentarse a los activos de carácter personal es caracterizarlo como tales en el nivel que corresponda, y, además, determinar su valor: el dato que supondría su revelación o alteración indebida. Con esta aproximación, al análisis de impactos y riesgos permitidos los datos tanto por obligación legal[122] como por su propio valor.

Siempre que sea posible conviene partir de datos estándar. En el caso de desastres naturales o accidentes industriales, se puede disponer de series históricas, genéricas o del lugar en el que se

122 *Commission Nationale de l'Informatique et des Libertes, CNIL. Methodology for Privacy Risk Management*:
En el Area de la Privacidad , los únicos riesgos a considerar son aquellos que motivan la Privacidad en el Procesado de Datos Personales. Estos riesgos se componen de algún evento temido y aquellas amenazas que la hacen posible. Se trata de evitar las siguientes situaciones: -no disponiilidad de los procesos legales – cambio en el procesado – acceso ilegítimo en los datos personales – desaparición de datos personales. Para que ocurra una de estas situaciones no deseadas , deberán de exisitir una o más de estas fuentes de riesgo que la causan, pudiendo incluit:

- personas que pertenezcan a la organización: usuario, especialistas en computación
- personas de fuera de la organización: proveedores, terceras personas, organización gubernamental, .
- fuentes no humanas: virus de ordenador, desastres naturales, material inflamable, epidemias,..

ubican los equipos de nuestro sistema de información bajo estudio. Probablemente también se disponga de un historial que informe de lo que es frecuente y de lo que "no pasa nunca".

Cuando se tienen datos de carácter personal, hay que cifrarlos. Cuando los datos son confidenciales, hay que etiquetarlos y cifrarlos.

La clasificación de los datos de carácter personal depende de la legislación aplicable en cada lugar y circunstancia. En el caso de la legislación española, se ajusta a los dispuesto en,

- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal

- Real Decreto 1720/2007 por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal

Esta legislación establece los siguientes criterios:

Nivel básico

Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. LOPD *art. 3*. RD Título VIII Cap. I *art. 81, Cap. III Sección 1º, y Cap. IV Sección 1º.*

Nivel medio

Datos de carácter personal relativos a la comisión de infracciones administrativas o penales, Hacienda Pública o servicios financieros. RD Título VIII Cap. I *art. 81, Cap. III Sección 2º, y Cap. IV Sección 2º.*

Nivel alto

Datos de carácter personal relativos a ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales sin consentimiento de las personas afectadas. RD Título VIII Cap. I *art. 81, Cap. III Sección 3º, y Cap. IV Sección 3º.*

4.- Dimensiones de Seguridad

Del paso de la versión 1 de Magerit a la versión 2 en el año 2010 se ha corregido y ampliado lo que se denominaba *Subestados de Seguridad* dándole el nuevo nombre de *Dimensiones de Seguridad* introduciendo nuevas criterios a fin de medir lo que interesa de los activos. Este concepto se maneja continuamente en el posterior desarrollo de la L 11/2007 en su RD 3/2010 considerándose dicho tratamiento propuesto como un conjunto mínimo de requisitos para todas aquellas plataformas que interaccionen con la e- Administración.

Las *Dimensiones de la Seguridad* se entienden mejor considerando la *negación* de cada una de sus características

- *Disponibilidad*: La carencia de disponibilidad supone una interrupción del servicio

- *Integridad:* Contra la integridad, la información puede aparecer manipulada, corrupta incompleta

- *Confidencialidad:* Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados o que la información llegue solamente a las personas autorizadas

- *Autenticidad:* La autenticidad se dan suplantaciones y engaños que buscan realizar un fraude

5.- Activos

Ya hemos dicho que el activo esencial es la información que maneja el sistema; o sea los datos. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger. El valor puede ser propio, o puede ser acumulado. Se

dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- *degradación*: cuánto de perjudicado resultaría el activo

- *frecuencia***:** cuánto se materializa la amenaza

cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

El impacto *acumulado* se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto *repercutido*, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un *impacto residual*.

- *Impacto*: daño posible

- *Riesgo*: daño probable

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema. Estos activos soportan parte del valor del sistema y están a su vez sujetos a amenazas que pueden perjudicar a los activos de valor.

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

<<Magerit permite modelar directamente la aplicación como un activo>>

Un proceso depende de todos los activos que aparecen en su diagrama. Unos datos dependen de todos los sitios por donde pasen.

Encontrar un activo sin valor acumulado es sinónimo de que las dependencias están mal moderadas o simplemente que el activo es irrelevante.

6.- Gestión de Riesgos

Pueden darse situaciones en las que se requieren un análisis de diferente calado:

- un análisis *urgente* para determinar los activos críticos
- un análisis *global* para determinar las medidas generales
- un análisis de *detalle* para determinar salvaguardas específicas para ciertos elementos del sistema de información
- un análisis de *detalle cuantitativo* para determinar la oportunidad de un gasto elevado

A lo largo de estos procesos se ha de generar una serie de documentos de interés general que desglosados conforme al Esquema de Magerit sería el siguiente para un Proceso de Análisis de Riesgos:

Actividad: Caracterización de los Activos

Tarea 1.1: Identificación de los activos

Tarea 1.2: Dependencias entre activos

Tarea 1.3: Valoración de los activos

Actividad: Caracterización de las Amenazas

Tarea 2.1: Identificación de las amenazas

Tarea 2.2: Valoración de las amenazas

Actividad: Caracterización de las Salvaguardas

Tarea 3.1: Identificación de las salvaguardas existentes

Tarea 3.2: Valoración de las salvaguardas existentes

Actividad: Estimación del estado de Riesgo

Tarea 4.1: Estimación del impacto

Tarea 4.2: Estimación del riesgo

Tarea 4.3: Interpretación de los resultados

Las normas y procedimientos que se derivan en cada proceso van constituyendo el conjunto de normas y procedimientos que se emplearán durante la explotación del sistema.

Resulta relevante el caso donde se cuenta con más de un responsable. Por ejemplo, en caso de datos de carácter personal cabe diferenciarse entre el responsable del dato y el operador que lo manejan:

- *responsables de los datos*, que conocen las consecuencias de la degradación de los datos

- *responsables de sistemas de información y responsables de operación*, que

conocen las consecuencias de un incidente

Independientemente del proceso, en la valoración conviene registrar la siguiente información:

- dimensiones en las que el activo es relevante
- estimación de la valoración en cada dimensión
- explicación de la valoración
- entrevistas realizadas de las que se han deducido las anteriores estimaciones

Se identifican las *amenazas* significativas sobre los activos identificados, tomando en consideración:

- el tipo de activo
- las dimensiones en que el activo es valioso
- la experiencia de la Organización

Para cada amenaza sobre cada activo convendrá registrar la siguiente información:

- explicación del efecto de la amenaza
- entrevistas realizadas de las que se ha deducido la anterior estimación
- antecedentes, si los hubiera, bien en la propia Organización, bien en otras organizaciones que se haya considerado relevantes

sumándose la frecuencia y valoración del daño.

En la caracterización de la salvaguardas se ha de considerar el inventario de procedimientos operativos, inventario de hardware y software de soporte de seguridad, plan de formación, contrato y puestos laborales y acuerdos de externalización.

En cuanto a la valoración de la efectividad de la salvaguarda se observará la idoneidad, calidad, formación de los responsables de configuración y operación.

En cuanto a la orientación que se ofrezca frente a los usuarios se observará si tienen un papel activo, de la existencia de controles de medida de su efectividad, y de la existencia de procedimientos de Revisión Regular.

La interpretación de los Resultados se puede realizar:

- por activos de Mayor Impacto

- por activos de Mayor Riesgo

Asimismo, el Estado de Riesgo puede suponer: el resumen del impacto, la definición del riesgo potencial, y residual de cada activo de dominio.

Por otra parte, de cada riesgo se estudiará si,

- es *crítico* el sentido de que requiere atención urgente

- es *grave* el sentido de que requiere atención

- es *apreciable* el sentido de que pueda ser objeto de estudio para su tratamiento

- es *asumible* el sentido de que no se van a tomar acciones para atajarlo

Durante la fase de especificación se debe evaluar un *dimensionado* de los perfiles de usuario.

Es importante destacar que el alcance de un nivel de seguridad puede requerir modificaciones por parte de los técnicos del sistema; al tiempo que los detalles técnicos puede alterar el análisis.

En cualquier caso, el punto de acuerdo entre los componentes activos y el estado de seguridad (impacto y riesgo) debe ser aprobado por la dirección de la organización.

Finalmente, indicar que en el entorno software de desarrollo se debe de cuidar de la disponibilidad e inventariado de :

- herramientas de tratamiento de la documentación: generación, publicación, control de documentación

- herramientas de tratamiento de código generación, compilación, control de versiones

La utilización de herramientas de soporte deberá permitir:

- Capturar un módulo inicial estudiar y variaciones pasar de lo general a lo concreto, previendo amenazas potenciales y preparando mecanismos de detección y reacción

- revisar periódicamente los cambios que se propongan

7.- Esquema Nacional de Seguridad, ENS

La existencia de datos de carácter personal requiere de un documento de seguridad y la designación de una serie de responsables. Parece natural que estos requisitos se contemplen en la *Política de Seguridad* requerida por el E*squema Nacional de Seguridad*[123], ENS: como conjunto de directrices

123 L 11/2007, (art. 42) , y su consecuente RD 03/2010; Guía CCN-STIC nº 803, (pag. 8)

plasmadas en documento escrito que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Recordemos la legislación que protege este marco de actuación:

- La Ley L 11/2002, reguladora del *Centro Nacional de Inteligencia, CNI*: según *art.4*.e de seguridad de las TIC, y 4.f acerca de la información clasificada

- RD 421/2007, de regulación del centro, CNI

- L 11/2007, según *art.42.2* donde se explícita el Marco de Referencia

El *Centro Criptológico Nacional, CCN*[124], emite unas guías accesibles desde Internet que pueden ser utilizadas como procedimientos por los propios auditores.

El equipo auditor tan sólo tiene la obligación de anticipar al personal auditado de las agendas o disponibilidad de elementos para la ejecución de la prueba.

La auditoría puede ser requerida por más de un órgano: el propio *CCN* y la *APD*, Agencia de Protección de Datos en el caso de que se viere solicitado por regulación su actuación.

Las evidencias que se recojan deben evitar en lo posible, contener datos de carácter personal utilizando algún mecanismo que impidan en lo posible contenerlos utilizando algún mecanismo que impida su divulgación.

En ningún caso los integrantes del equipo auditor deben haber participado o detentado responsabilidades previas a la auditoría al menos en los dos últimos años en el sistema de

124 tiene las competencias en la Administración General del Estado para certificar la seguridad de las tecnologías de la información. Legislación aplicable: Ley 11/2002, RD 421/2004 y ORDEN PRE/2740/2007, por el que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologias de la Información. La certificación es una acto administrativo que a día de hoy no tiene tasas. En España, los certificados que emite el Centro Criptológico Nacional son reconocidos en otros 24 países; RD 421/2004 de regulación del Centro (Serie de Documentos CCN-STIC 801, 802, ..)

información auditado.

Si el Sistema de Información auditado según el *RD 3/2010* tratase datos de carácter personal, el equipo auditor podrá solicitar una copia de la auditoría preceptiva según el RD de protección de datos personales.

Cuando la auditoría es conjunta se rigen por los *art.16* y *art. 110 RD 1720/2007*.

Muchas medidas de seguridad vienen requeridas tanto por el *Esquema Nacional de Seguridad* como por el Reglamento de Protección de Datos de Carácter Personal por lo que su implantación puede ser unificada, sin perjuicio de que en los procesos de auditoría se verifique su idoneidad para proteger tanto los datos de carácter personal como los servicios prestados a los ciudadanos.

Ambas auditorías podrá, concurrir y coincidir en el mismo equipo.

En el *Documento 802* denominado Guía *de Auditoría* precisamente se establecen unas premisas mínimas sin que implique unas limitaciones o esquemas de trabajo.

Cada dos años de forma ordinaria para los Sistemas de categoría Media y Alta conforme al *Anexo RD 3/2010* y con carácter extraordinario postula que deberá realizarse una auditoría cada vez que se produzca una modificación sustancial en las Medidas de Seguridad requeridos.

Antes de la concretación de la auditoría se ha de señalar el Objeto y el Alcance de la misma: precisando hasta donde se audita al considerar que las redes de cada comunicación y sistemas de la administración pública tienen interconexiones con entidades públicas y privadas

- Parte del alcance de la auditoría es el identificar aquellos elementos que entran dentro de éste

- Política de Firma Electrónica y Certificados y Servicios que usan estas técnicas

- Tipos de Dato y Normativa que les sea de aplicación

- Determinación de la Categoría del Sistema

Si la realización de la auditoría ha sido encargada a un equipo externo, los integrantes deberán firmar las preceptivas *Clausulas de Confidencialidad*, incluyendo la de protección de datos. Si la realización de la Auditoría ha sido liderada por un equipo de Auditoría Interna pero con incorporación de expertos independiente estos también deben formar una *Clausula de Confidencialidad* y no debiendo limitarse a una revisión de documentos.

Las pruebas podrán realizarse en base a muestras, pero con el equipo auditor debe sustentar que la muestra de elementos seleccionada para una prueba determinada es suficientemente representativa para garantizar la solvencia de los resultados.

El *Documento 801* en alusión a *Responsables y Funciones* y en terminología del ENS, *Esquema Nacional de Seguridad* determina que el responsable de Seguridad de la Información es la persona que determina los *Niveles de Seguridad de la Información*.

Se recomienda que los criterios de Valoración estén respaldados por la Política de Seguridad. Debe realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo.

Entre las responsabilidades del responsable de Seguridad, se enumeran las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los servicios prestados por los sistemas TIC en su ámbito de responsabilidad

- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de eventos de seguridad y mecanismos de auditoría

implementados en el sistema

- Apoyar y supervisar la investigación de los *Incidentes de Seguridad* desde su notificación hasta su resolución

- Elaborar el *Informe Periódico de Seguridad* para el propietario del sistema, incluyendo los incidentes más relevantes del período

El *art. 10* del ENS, *Esquema Nacional de Seguridad* recoge el principio de la seguridad como función diferenciada y exige que el responsable del sistema no sea la misma persona que el responsable de Seguridad.

El *Informe* resultante deberá mencionar la Metodología utilizada.

Por otra parte, el propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su propietario correspondiente.

En los sistemas de categoría Alta se recomienda que se establezcan indicadores del estado de los riesgos críticos. Estos indicadores entre los que se encuentran los *umbrales de aviso y alarma* en atención urgente estarán a disposición de los auditores.

El Análisis de Riesgos establecido en el Anexo II de esta guía será elaborado por el responsable del sistema que podrá encargar o delegar la función, aprobando el resultando el resultado final. El responsable validará el documento, pudiendo solicitar mejoras del mismo. El documento estará a disposición de los auditores.

Idénticamente estarán a disposición de los auditores la Declaración de Aplicabilidad y la Arquitectura de Seguridad. La normativa de seguridad y los procedimientos de seguridad se han agrupado en esta guía bajo la denominación de *Procedimientos Operativos de Seguridad.* Esta documentación estará a disposición de los auditores además de que debe hacerse llegar a las personas afectadas, que deberán explicitar su conocimiento y adhesión a lo establecido.

EL *Documento 803* o *Guía de Implantación* del ENS, *Esquema Nacional de Seguridad* hace referencia explícita a la norma ISO/IEC 27 002: 2005 y en los siguientes puntos del índice:

- 5.1 Política de Seguridad de la Información

- 15.1.1 Identificación de legislación aplicable

sobre los aspectos que hemos querido resaltar en este capítulo.

8.- ISO / IEC 27 001-27 002

De idéntica forma que se habla de la economía global, podemos referirnos a la economía de la información en convergencia con su gestión.

Se hace precisa la existencia de un marco en materia de Seguridad de la Información que permita a los directores responder al complejo rango de requerimientos de los que deben responder.

El especular en el desarrollo de las Tecnologías de la Información ha contribuido al incremento y la globalización de sus relaciones, pero también a la aparición de peligrosas vulnerabilidades que se hace preciso detectar y de las que hay que prevenirse.

Se potencia la importante conclusión de alinear proyectos tecnológicos con estratégicas metas organizacionales y asegurarse que cumple el valor estimado que deben proporcionar a la organización.

No dejando obviar nunca el presupuesto que un proyecto tecnológico supone una inversión tanto financiera como de recursos.

La Seguridad en materia de datos resulta fundamental en la estrategia web y propuestas de plataformas de comercio electrónico.

Existe un foco interesante de destacar: existen organizaciones en los que los directores depositan particular atención sobre la gestión de riesgos basándose en pasadas experiencias e intereses, concediéndole poca importancia a la necesidad real de objetivos estratégicos.

Esta discusión se hace particularmente interesante sin el complicado entramado que puede hacerse la plataforma tecnológica en su conjunto: extranets, intranets, además de la madeja neurológica de colaboradores, compradores y vendedores.

Este estándar le concede especial importancia a la adopción de las prácticas más adecuadas reconocidas internacionalmente en materia de Seguridad de la Información.

El Sistema de Gestión de Seguridad de la Información, *SGSI*, se puede encontrar geográficamente limitado o restringido a un sector específico (e.g., software de defensa, etc..) ni tampoco dedicado y orientado a un sólo producto.

Ahora bien, las organizaciones deberían siempre asegurarse de que todo proceso que implementen y decidan llevar a buen término resulte apropiado a un entorno, reflejando siempre el estilo y la cultura que lo integrará y aceptará. Asi mismo, dichos procedimientos deberán reflejar los riesgos detectados por el consultor especialista dedicado a la detección y configuración de los mismos.

Recordar que la norma ISO 27 001 debe observarse como un esquema, y no como una garantía de hierro. La certificación no prueba un sistema con una efectividad del 100% en materia de seguridad, sino se debe de considerar como un indicador, especialmente interesante para terceras partes, de que el objetivo en Materia de Seguridad de Datos ha sido perseguido con absoluta voluntad y motivación.

Es un modo no un fin en sí mismo: deben perseguirse los objetivos, no los métodos de obtenerlos.
Una organización con un inadecuado sistema de seguridad de la información se exponen a daño en sus operaciones, a su reputación y a perturbaciones legales.

El primer acuerdo internacional articulado en materia de actividades cibercriminales en las redes computacionales fue firmado en Noviembre del 2001. EEUU lo ratificó en 2006 y se adhirió a él con efectividad en Enero de 2007. Está principalmente orientado a la defensa de sus derechos del ciudadano, colaboradores en la cooperación de investigación de dichos crímenes.

El hecho de que las fuentes de peligro pueden resultar tan diversas y los riesgos se propaguen tan ampliamente nos permite aseverar que resulte insuficiente la implementación de una política antivirus, aunque ésta se presentará de forma continua. Así, la implementación de cortafuegos puede prever de falsos niveles de confort a no ser que existan análisis previos que reflejen una estrategia completa de riesgos.

La Organización será capaz como consecuencia de la adopción del Esquema de demostrar y cotejar que se cubre el Marco Legal y cómo a través del citado análisis. Así mismo, será capaz de protegerse de forma sistemática frente a potenciales peligros.

Dicha implementación, ayudará a mejorar la credibilidad entre la plantilla, clientes y colaboradores, reflejándose todo ello en claras mejoras financieras, en las ventas por ejemplo.

La Ley de *Sarbanes-Oxley , SOX*, presenta importantes implicaciones en aquellos negocios subsidiarios de EEUU. La gestión de esta articulación exige la certificación de los informes financieros de la compañía. Este tipo de reporte depende de la infraestructura tecnológica, la operatividad efectiva de un sistema ERP.

The Sarbanex-Oxley Act se introdujo en EEUU en 2002 después del caso Enron. Se diferencia fundamentalmente del *the Combined Code* y de otros Códigos adscritos en el marco de la OECD en que no se detiene en la mera explicación o exoneración sino que se introduce en la cadena y puede suponer importantes sanciones para directores que actúen de modo individual.

Bajo SOX, la gestión requiere de la certificación de los informes financieros que, por otra parte, están condicionados a toda una infraestructura de e-Administración y anteriormente conceptualizada como ERPs. La conseguida certificación no podrá ser llevada a cabo hasta que se creen e integren los consiguientes controles internos sobre dicha plataforma. Las secciones más críticas de la legislación SOX son la 302 (acts of fraud) , la 404 (changes) y la 409 (monitor).

Existe un entorno de trabajo denominado COSO que garantiza la supervisión de esta ley. Contempla dos importantes grupos de Medidas de Seguridad: las generales y las de aplicación. Los primeros son típicas del esquema ISO 27001. Los segundos se encuentran embebidos en el software a fin de detectar y prevenir o alertar transacciones fraudulentas.

Con el fin de Supervisar la actividad de esta Institución fue creado el PCAOB, *Public Company Accounting Oversight Board*. En su estándar nº 2 de auditoría distingue, sobre todo, dos grupos de salvaguardas: medidas genéricas y medidas de aplicación. Las primeras, son las comunes y presentes en todo Sistema de Gestión de la Información y las segundas se encuentran embebidas en el software a fin de detectar y prevenir transacciones no autorizadas.

El parágrafo 50 en SOX se resume la necesidad del mantenimiento de este entorno de medidas internas incluyendo las observaciones de las secciones 302 , la 404 y la 409. Observar que estas secciones no debieran observarse por igual: así, debieran observarse la 302 por un lado, y la 404 y la 409 por otro (practicando diferentes estructuras organizacionales para el desarrollo de cada conjunto de medidas).

En el parágrafo 52 se observa precisamente que se percibirá un impacto como consecuencia de la implantación de estas medidas en los niveles de proceso, transacción y de nivel de aplicación. El desarrollo de estas medidas afectan a la implementación de las políticas, procedimientos y códigos de conducta que son la misma esencia de la ISO 27002.

Los diferentes Niveles de Seguridad que se adjudicarán a este tipo de controles incluyen políticas, procedimientos y códigos de conducta, que son el corazón de la ISO/IEC 27002.

Un certificado sobre un *Sistema de Gestión de Seguridad* de la Información le trasmite a potenciales clientes que la empresa ha definido y colocado adecuadamente la información relacionada con sus procesos ayudando a crear relaciones de confianza.

Un añadido en la certificación siempre es la mejora continua de sus procesos debido a la aprobación debido a la aprobación externa que esta exige.

Un certificado ISO 27 001 es válido por un período de tres años. ISO 27 001 es el documento frente al cual debe de responder un ISMS. De forma que el responsable de este debería de ser capaz de referirse a él explícitamente y de defender cada una de las etapas que cubren su correspondencia con el estándar.

El movimiento de la ISO 27 001 se originó en 1992 promovido por el Departamento de Comercio e Industria en el Reino Unido; su primera versión BS7799 se generó en 1995 y consistía

fundamentalmente en un Código de Práctica de Gestión de la Seguridad de un Sistema de Información.

Se obtuvo una segunda versión en 1998 dividiéndose el estándar en dos partes: la primera, entendida como un *Código de Práctica* y la segunda como una especificación. Esta segunda parte obtuvo una segunda revisión en 2002. ISO 27 001 se internacionalizó como estándar en 2005. ISO 27 002 alcanzó la misma consideración en 2007.

La serie de estándares 27000 se numeran actualmente de 27000 a 27019 y de 27030 a 27044.

En la clausula 4.2.1 de la norma ISO 27 001 se recogen las pautas para llevar a cabo el P.D.C.A, más concretamente proporciona la definición de la Política de Seguridad que debiera recoger la estrategia A.5.1 y control de objetivos que generan la implementación de un ISMS. Debiendo ser revisada y actualizada periódicamente:

La fase de *Plan (Plan)* comprende:

1. Ámbito del SGSI

2. Política de Seguridad de la Información

3. Valoración de y Criterios de Aceptación de Activos

4. Activos del Sistema

5. Opciones de tratamiento de Riesgos

6. Escenario de Aplicabilidad

La fase de *Hacer* (Do) comprende:

1.Formulación del Plan de Tratamiento de Riesgos incluyendo los procedimientos y la pertinente documentación

2.Implementación del Plan de Tratamiento de Riesgos y salvaguardas planeadas

3.apropiada Formación para la plantilla afectada

4.Gestión de Operaciones y Recursos en línea con el SGSI

5.Implementación de Procedimientos que permitan la detección y respuesta a los Incidentes de Seguridad

La fase de *Revisión* (Check) comprende:

1.Monitorización, Revisión, Testeo y Auditoría

La fase de A*ctuación* (Act) comprende:

1.Mejoras detectadas sobre el SGSI debieran ser identificadas y documentadas, así como ejecutadas

A ISO 27 0001 se le considera consistente con las líneas de la OCDE en materia de privacidad, criptografía y seguridad de la información, aceptándose su implementación en diversos marcos legales y culturales. Esto desde 1998, cuando aun adoptaba el nombre de BS7799.

Luego se está cumpliendo lo que se representa como un nivel internacional aceptado , a *true international level*.

La versión de 2002 persiguió la adopción de un acercamiento al proceso para el diseño y puesta a punto de un SGSI, modelo es conocido como *Plan.Do.Check.Act, PDCA*.

Tanto ISO 27 001 como ISO 27 002 adoptan una metodología de lógica numérica para sus clausulas y subclausulas. Estas se recogen en una hoja aparte.

Muchas organizaciones que intentan adaptarse a la norma ISO 27 001 ya tiene instalado la ISO 9001:2000, el denominado sistema de aseguramiento de calidad.

ISO 27 001 anima a la integración en tal sentido, en particular las clausulas

- 4.3 documentación
- 4.3.2 control de la documentación
- 4.3.3 records

coinciden con las clausulas 4.2.3 y 4.2.4 de la *ISO 9001: 2000*, aunque los primeros van más allá.

En consecuencia, la organización debería adoptar, al menos en cuanto a la documentación los principios a los que se refiere la ISO 9000, haciendo referencia en tal causa la clausula 4.3.1 que indica la mínima documentación que debería acompañar a un SGSI:

- la política de seguridad,
- la estimación de riesgos,
- los objetivos de los controles a garantizar tales situaciones

Se debería prestar, al menos, la misma atención que a otros objetivos del negocio.

Deberá resultar perfectamente identificable la forma que deberá adoptar el resultado y el por qué ese resultado debe resultar esencial.

El equipo que lidere la implementación del SGSI deberá contener una parte funcional, posibilitando que todo el mundo pueda entender y se considere capaz de aplicar este tipo de controles.

Deberá existir, así mismo, una persona encargada de liderar los progresos y de ir mostrándolos.

En ocasiones, suelen presentarse lógicas reticencias a la instauración del SGSI por causas diversas, por ejemplo: el miedo a que el equipo pierda la mística que les ha estado alimentando. Esto puede llegar a provocar cambios en la plantilla tecnológica de forma asertiva o no, y la organización deberá adoptar, en consecuencia, planes de contingencia.

Pese a todo ello, cada miembro de la organización debería percibir que está formando parte de algún tipo de transacción, de forma paralela a la forma de interacción que puedan mantener con la información que se les va proporcionando desde la Internet.

Aunque la ISO 27 002 espera la existencia de un único responsable de la gerencia de todas las actividades relacionadas con la prosecución de la Seguridad de la Información, esto no es un requerimiento específico en la ISO 27 001. Y aunque la selección del especialista técnico que debería llegar a cabo la supervisión e implementación del SGSI debería preceder a la selección del grupo que se ha venido en denominar *fórum*, este grupo sería el que debería considerar la selección de forma democrática, en lo posible, si existiera unanimidad del responsable para la segunda parte.

Puede ser , en este caso, la dirección de la empresa la que no esté de acuerdo en desarrollar este camino, por considerarlo lento. Hablando desde un punto de vista organizacional.

Esta persona seleccionada deberá trabajar siempre en concordancia con el fórum. Por una parte deberá de estar reportando continuamente de la evolución de la implementación del SGSI y comunicarlo, en su caso, al propio grupo. Por otra parte, será el responsable al que se ha de hacer llegar y supervisar la identificación de posibles riesgos, así como de seleccionar aquellas *Medidas de Seguridad* que permita hacerlas frente.

La frecuencia de las reuniones indicará la urgencia y grado de complejidad de la implementación. Aunque realmente no existe la necesidad de los encuentros se produzcan de forma física, podrían llevarse a cabo por videoconferencia.

Aunque la norma ISO 27 001 prescribe la necesidad de mantener contactos con autoridades relevantes, dígase cuerpos legales, asesores técnicos , auditores, cuerpos de la seguridad local, nacional e internacional, esto no afecta para nada la necesidad de la certificación de una plausible auditoría como exigencia del estándar.

Las revisiones sí que se pueden ser llevadas a cabo por auditorías internas. Eso sí, estas normas serán adoctrinadas a tal fin.

Cuando todas estas cuestiones han sido decididas es cuando se puede comenzar.

La política de seguridad debe ser continuamente revisada y actualizada a la vista de las cambiantes circunstancias. Como mínimo la revisión debe resultar anual. La Organización debería ser capaz de mostrar tales documentos en un par de hojas de formato A4 , que debería guiar la implementación de un SGSI.

Conforme a la cláusula Nº 5 de la norma ISO 27 002 estos cambios debieran ser analizados, llevados a la práctica y comunicados a lo largo de la organización siendo estos cambios manifiestos.

Independientemente de la tecnología utilizada, se deben satisfacer los requerimientos de integridad, no repudio, etc.. exigencias que, por definición, deben responder los protocolos de comercio electrónico.

ISO 27 002 minimiza los potenciales daños que puede sufrir la empresa, así como maximiza el retorno de inversiones en infraestructuras y oportunidades de negocio y debe resultar esencial en la línea de la competencia, respuesta legal e imagen comercial.

Tal vez y como respuesta a la exigencia de una determinada Medida de Seguridad, la Organización debe pensar en la creación de unidades dentro de la organización qué organización satisfaga dicho control.

La norma *ISO 27 003: 2005* identifica al menos tres fuentes a la hora de establecer los requerimientos que se ha de exigir al Sistema de Seguridad de la Información: aquellas surgidas de compromiso contractuales en cualesquiera de las jurisprudencias en las que opera; los riesgos que la organización hace frente y todas aquellas que surgan de los objetivos que la Empresa se ha impuesto

en la superación de la línea de negocio.

El *Plan de Gestión de Riesgos* debe responder, de al menos, cinco objetivos:

- la estimación en lo posible de estos
- la reducción en niveles aceptables de aquellos que no puedan ser aceptados
- la coexistencia con ellos, ejecutando con sumo cuidado aquellos controles que los mantiene en un nivel aceptable
- la trasferencia de ellos a alguna otra organización

La forma de aceptar dichos riesgos se debería ajustar, por ejemplo, al principio de que el impacto económico deberá resultar inferior al coste que supone el controlarlos, estableciendo un balanceo entre el grado de costo y el grado de riesgo.

Las metodologías para llevar a cabo el cumplimiento del plan de riesgos se gestionan según *ISO 13 335-3*.

ISO 27 002 adopta desde *ISO Guide 73: 2002* definiciones del concepto riesgo, análisis de riesgo, aseguramiento del riesgo, evaluación del riesgo, gestión y tratamiento del riesgo.

Recordamos que el auditor de la *ISO 27 001* puede requerir documentación como garante de que se cumple la formación requerida y experiencia que se espera de dicho recurso.

- Su clausula A.7.2 especifica que una organización debe contar con un procedimiento de clasificación de la información que asegure que cada uno de sus fines se le otorgue el adecuado nivel de protección
- La clausula 10.3.2 de la *ISO 27 001* proporciona los detalles de un *Contrato*

de Escrow, ampliamente documentado en el Capítulo dedicado a *Escenarios*

- Para nuestro caso, el control A.15 lo podemos considerar como el más importante ya que dicha clausula permite asegurar brechas de irregularidades legales, o entre relaciones laborales, o acerca de requerimientos de seguridad: presenta diez subclausulas

Existe un principio que dice: que si el coste de la implementación y mantenimiento de un control no debiera resultar ser mayor que el coste de su impacto. *CBK, the Common Body of knowledge*, describe entre sus controles:

- *directive controls*: de carácter administrativo, como la creación de políticas
- *controles de detección*: que protegen las vulnerabilidades y que o bien reducen el impacto o lo detienen
- *controles correctivos*: que reducen el efecto de ataque
- *controles de recuperación*: asociados generalmente con la continuidad del negocio

El daño se puede categorizar en tres tipos: orientados hacia la organización (posición competitiva, financiera y de reputación), relaciones contractuales y responsabilidades legales.

Conforme a la A.15.1.1 los requerimientos y sus consiguientes medidas de control deben de responder a los cambios que se produzcan en la marco legal. La clausula A.15.3.2 exige la restricción del acceso a sus herramientas de auditoría.

La Documentación producida por la ISO 27 001 ha de ser considerada como una herramienta y, por

consiguiente, en lugar seguro conforme especifica su clausula *12.1.3*.

En el *legal outsourcing* el tradicional *customer agreement* es sustituido por el *Documento de Seguridad* : La clausula 7.1.2 de la *ISO/27 001* nos dice que cada activo tiene que tener identificado su responsable, aunque no tenga derechos de propiedad sobre el activo. El Inventario de los activos y Módulo especificativo de su mantenimiento invoca el índice art. 7.1.1 o registro de activos. El control art.7.2.2 requiere de la organización la implementación de la clasificación y etiquetado del esquema de información, tanto en formato físico como electrónico, como indica la *ISO27 002.*

La clausula A.8.1.3 requiere un acuerdo de confidencialidad por parte del empleado, así como compromiso y conocimiento de las responsabilidades derivados de participar en un SGSI.

La clausula A.8.2.3 requiere de la organización el seguimiento de las violaciones de la política de privacidad por un procedimiento disciplinario

El paso de la fase de desarrollo de software es un estatus operacional que debe ser definido y documentado. Dicha operación viene definida por el control art.10.1.4 de la *ISO27 002*.

De idéntica forma el control A.10.2.1 considera en contratos de outsourcing o terceras partes las trasformación de cierta parte de la información, debiendo hacerse esto de forma documentada considerando los diferentes niveles de entrega. El consiguiente monitoreo y seguimiento de su labor se pude seguir por el índice A.10.2.2.

9.- Estudio de Viabilidad del Sistema y Gestión del Control del Cambio, Métrica 3

El Ciclo de Vida del Software en la Administración Española está soportado por la metodología *Métrica*, actualmente en su versión 3 y su propiedad intelectual la detenta el *Ministerio de Hacienda y Administraciones Públicas*.

La página Web del Portal de Administración Electrónica, *PAe*, proporciona la relación de Documentos en los que se explicitan las formas de invocación y tratamiento de su Estructura Principal, Interfaces, Técnicas y Participantes.

Referenciando directamente a la exposición del Documento *EVS-Estudio de Viabilidad del Sistema* que es previo a la aplicación de una *Gestión de Proyectos*, se puede apuntar que el *Estudio de Viabilidad del Sistema* es un análisis de un conjunto concreto de necesidades para proponer a corto plazo, teniendo en cuenta las restricciones , y pudiendo ser estas, económicas, técnicas, legales u operativas. Para cada alternativa se valora su impacto en la organización, la inversión a realizar en cada caso y los riesgos asociados, pudiendo seleccionar la más adecuada , estableciendo su planificación.

El EVS plantea el estudio de viabilidad[125] en las siguientes fases, que a su vez se descomponen en tareas a las que se asocian productos de entrada y salida, técnicas y/o prácticas a aplicar y perfil de los participantes aconsejables:

- EVS1, Establecimiento del Alcance del Sistema
- EVS2, Estudio de la Situación Actual
- EVS3, Definición de Requisitos del Sistema
- EVS4, Estudio de Alternativas de Solución
- EVS5, Valoración de las Alternativas
- EVS6, Selección de la Solución

El *Análisis del Sistema de Información* se considerará concluido cuando se cuente con una descripción de la *Situación Actual*, un *Catálogo de Requisitos* y *Objetivos*, una descripción de las Alternativas de la Situación por medio[126] del Contexto del Sistema, su Impacto, su Coste/Beneficio, su *Valoración de Riesgos* y su *Plan de Trabajo* correspondiente. Añadiendo a la lista anterior la exposición de una Solución Propuesta.

Encontramos que lo que resulta más difícil de justificar a la hora de plantear una modificación de

125 De un modo muy similar a como sucede en ISO 27 0001, y por aplicación de un P.D.C.A . podemos encontrar en Métrica v3 alusión directa a su estructura dentro de uno de sus propios elementos, en concreto *GPI 2.2* de *Selección de la Estructura de las Actividades , Tareas y Producto:* para cada proceso se determinan las actividades y tareas a realizar, así como los productos a generar, en función de las características concretas del proyecto

126 Documento de *Técnicas, Métrica 3*

algún subsistema del Sistema de Información es el criterio por el que finalmente, se decidirá su Solución, esto es, en el caso de aplicación de una Medida Legislativa como el inicio de unos nuevos Procedimientos que se deberán de ver plasmados en Producción y que agilicen determinados mecanismos como puede ser el Soporte a la nueva *Ley de Transparencia* puede resultar obvio e incluso imprescindible, sobre todo, si a través de Circulares se comienzan a establecer plazos de los Hitos Informáticos, más si lo que queremos es adelantarnos poquito a poquito en el tiempo a determinadas perspectivas que no justificarían una Inversión apreciable actual, lo que se puede practicar son sucesivos y paulatinos balanceos en relación Coste/Beneficio a una serie de Optimizaciones del Sistema Informático y que, por otra parte, van resultando necesarios.

Sin pretender obviar este apartado de consideración de la exposición a *Métrica* , y salirnos de su Esquema proponiendo uno nuevo, pretendemos incorporar el entendimiento de la Observación de la Tesis a una Solución Concreta sin considerar sus Alternativas, del modo como se expone a continuación y pretendiendo resaltar la consideración de un *Documento de Seguridad* y del *ENS*, *Esquema Nacional de Seguridad*.

De modo que pudiéramos elevar la aplicación de su Esquema, como bien le debe de corresponder, incluso a la valoración de a cuál Ministerio le debe competer la Administración Publica Electrónica o blandiendo su Instrumento decidir si es correcto el Impulso de una determinada estrategia Ministerial, esto es, por ejemplo, ¿se podría justificar una Inversión monetaria de la Fusión de dos Bases de Datos considerando la Naturaleza del Dato (Ministerio) ante una determinada finalidad o más bien permite el Esquema ISO 27 002 aplicado en el Sistema Informático un diálogo óptimo con el criterio fundamental del Impulso de una Ley?

Más sencillo resulta de justificar y defender la Propuesta del Cap. IV en el contexto del actual *Plan de acción de administración electrónica 2011-2015* al promover la reutilización[127] como un concepto

127 AMUTIO, Miguel Angel. "Reutilización de Activos de la Administración", BOLETIC Nº 63. Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas. Fundación ASTIC. Revista de la Asociación Profesional de los Cuerpos Superiores de Tecnologías de la Información en la Administración: << En nuestro ámbito, la Ley 11/2007 ya incidió directamente en la cuestión al establecer en su artículo 45 que las Administraciones Públicas "podrán poner a disposición de cualquier administración sin contraprestación y sin necesidad de convenio aquellas aplicaciones informáticas de las cuales ostenten los derechos de propiedad intelectual" El artículo 46 trata los instrumentos operativos que facilitan lo anterior al establecer que las Administraciones Públicas mantendrán directorios para la libre reutilización de aplicaciones de acuerdo con lo que establezca el Real Decreto 4/2010 (Esquema Nacional de Interoperabilidad)>>

vinculado a la implantación de tecnologías innovadoras y desvinculándonos del complejo mundo de las patentes.

Un bravo ejemplo que ilusionaría a muchos Trabajadores sería una Auditoría de las Bases de Datos conectadas de la Seguridad Social y de Sanidad al objeto de detectar irregularidades que no justifiquen una Defensa de los Derechos del Trabajador al no verse cubierta su Salud , ofreciéndole una baja definitiva ante una dolencia no buscada, incluso cuando la Ley cubriera el caso. Sírvanos esta ilusión aspirada de muchos para determinar su posibilidad dado el contexto actual de Interoperabilidad[128] expuesto por medio de la exposición de dos artículos publicados en España:

- reutilización de Ficheros de la Seguridad Social desde Sanidad[129]

- esquema Completo de Interoperabilidad de la Seguridad Social[130]

Hemos presentado, pues, dos modos de contemplación de la aplicación de *Métrica 3* que eleva su discurso y recupera su tono, como le corresponde a su verdadero origen transcendiendo lo meramente técnico. Es , en consecuencia, el EVS un Instrumento que debe ser respetado en lo máximo por el *Ingeniero de Software* cuando preste su colaboración, de modo que su trascendencia no quede en negligencia y desconocimiento de causa, pues ya vemos el Nivel de Implicación que arrastra si no es bien considerado.

El caso más sencillo y óptimo a plantear resultaría el proveniente de un Análisis Estadístico contrastado con la Situación Actual de los diferentes Subsistemas Informáticos que componen el Sistema Principal.

---

128 COM (2010) 744 final: "Hacia la Interoperabilidad de los Servicios Públicos Europeos". Principios fundamentales de los Servicios Públicos Europeos , 1.- Subsidiaridad y Proporcionalidad 2.- Primacía del Usuario 3.- Inclusión y Accesibilidad 4.- Seguridad e Intimidad 5.- Multilingúismo 6.- Simplificación administrativa 7.- Transparencia 8.- Conservación de la Información 9.- Apertura 10. Reutilizabilidad 11.- Neutralidad y Adaptabilidad Tecnológicas 12.- Efectividad y Eficiencia

129 ANDREE LOPEZ María, G.Benavides Fernando, ALONSO Jordi, ESPALLARGUES Mireia, DURAN Xabier, MARTINEZ Jose Miguel. "La utilidad del uso de datos administrativos en la investigación de salud pública: la Muestra continua de vidas laborales". Gaceta Sanitaria. Vol.28 nº 4.

130 DELGADO Francisco. "Intercambios Internacionacionales de datos". BOLETIC Nº 66. *A*STIC, Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas

Un caso de planteamiento de análisis inverso podríamos retomarlo desde la publicación en el *BOE* de la *Ley de Subvenciones, L 15/2014*, considerando la *Ley de racionalización del Sector Público* como precursora e introductora de la consideración de índices en la Gestión de la e-Administración del Sector Público.

Habrá que entender la extensión de la exposición de la que hemos querido participar en el apartado 10.42 del Cap. III al considerarse y apreciarse como un inicio y no un indicio de lo que puede suponer el Marco del que Forma parte la Propuesta de la Tesis.

De manera que en el Esquema *Métrica* vamos a resaltar aquellas acciones que consideraremos mínimamente útiles que proponga un Cambio en el Sistema de Información global.

En el contexto de *Métrica V3, Incidencias* son aquellos hechos inesperados y anómalos que se presentan durante la realización de las actividades y tareas del proyecto y que producen desviaciones de la planificación. Los cambios de requisitos son un tipo especial de incidencia que exigen un tratamiento especial. Todos los cambios de requisitos que se produzcan durante el desarrollo de un proyecto se mantendrán debidamente clasificados en un documento específico , el *Registro de Cambios*, indicando para cada cambio la información que se ha hecho constar en su apartado.

Igualmente, el resto de las Tares de *Gestión de Proyectos* se encontrarían a la espera de la Evolución acerca del Estudio de Viabilidad del Cambio.

GESTION DE PROYECTOS

GP3: Seguimiento de Tareas /Gestión de Cambios en los Requisitos

	Producto de Entrada	Producto de Salida
GPS5.1, Registro de la Petición del Cambio de los Requisitos	Notificación de la necesidad de cambio	Formulario de petición de Cambios
GPS6.1, Estudio de la Petición del Cambio de los Requisitos	Formulario de petición de Cambios	Catálogo de Necesidades
GPS6.2, Impacto de la Petición del Cambio de los Requisitos		Análisis Funcional del Cambio Diseño Técnico
GPS6.3, Propuesta de la Solución	Formulario de Petición de Cambios Catálogo de Necesidades Análisis Funcional del Cambio Diseño Técnico	Propuesta de la Solución

Tabla 3. Metrica-Gestión de Proyectos

Como consecuencia de una nueva *Planificación del Sistema de Información, PSI*, surge la necesidad de proceder a generar la Fase de un *EVS*, cuyo principal comportamiento registrable frente a una nueva Ley, puede corresponderse con el trazado siguiente, sin desdecir el resto de actividades y/o tareas del esquema del *EVS*:

1.- debemos poder conceptualizar los diferentes 'niveles' en los que está hablando la modificación planteada, tanto desde el punto de vista físico como del lógico, si esto es posible, y lo podemos obtener en la *Descripción General del Sistema*, especificando su *Contexto*, *Estructura Organizativa*, y, sobre todo, el *Catálogo de Requisitos* relativo a restricciones o dependencias con otros proyectos. Dígase, por ejemplo, una integración específica de colaboración de dos Bases de Datos Ministeriales (naturalezas del dato), siendo necesario para ello , al menos, un *Diagrama de Flujo de Datos* y un *Diagrama de Descomposición Funcional*.

2.- Las condiciones del subsistema no pueden venir mejor definidas que por un *Catálogo de Usuarios*, siendo conveniente la subdivisión del Sistema en Subsistemas identificando las posibles mejoras y/o problemas existentes. El *Catálogo de Usuarios* deberá responder a un

Escenario que perfile un Índice *de Revisión* correspondiente al momento desde el que se deberá presumir si la Medida Legislativa a aplicar se encuentra próxima(existe plazo vigente), es previsiblemente virtual, o es real (aunque no exista plazo preciso)

3.- A continuación,y respetando la aplicación de la *Política de Seguridad* dentro de la cual se cuenta con el *Documento de Seguridad* en lo que respecta a la protección de los datos personales, debemos poder identificar las medidas correspondientes al *RD 03/2010* relacionadas, o las nuevas a generar independientemente de que se trate de una *Salvaguarda Técnica* propiamente dicha: distinguiendo, en cualquier caso, las *Dimensiones de Seguridad* afectadas a fin de poder dar respuesta satisfactoria al *Plan de Riesgos* establecido y a la *Gestión del Plan de Calidad*

4.- El Grado de Refinamiento de la previsión del Ciclo de Vida interno de la Propuesta, puede llegar a la *Especificación* del propio *Requisito* dentro del *Catálogo de Requisitos* facilitando de este modo su *Trazabilidad* y el *Impacto del Cambio*. Si como propone la Técnica de *Catalogación* de Métrica v3, las características asociadas a los mismos fueran: identificador del requisito, autor, tipo de requisito (funcional, no funcional, implantación, formación, documentación), descripción, prioridad(alta, media, baja), estado(aprobado, implantado, aplazado), fecha de creación, fecha de revisión, la propia característica que define el estado podría indicar si depende o no de la aparición de una ley, o de la observación de un plazo

ESTUDIO DE VIABILIDAD DEL SISTEMA-EVS

EVS1: ESTABLECIMIENTO DEL ALCANCE DEL SISTEMA

	Producto de Entrada	Producto de Salida
EVS1.2, Identificación del Alcance del Sistema		Descripción General del Sistema(Contexto del Sistema, Estructura Organizativa) Catálogo de Requisitos(relativos a restricciones o dependencias con otros proyectos)

EVS2: ESTUDIO DE LA SITUACION ACTUAL		
	Producto de Entrada	Producto de Salida
EVS 2.1, Valoración del Estudio de la Situación Actual		Descripción de la Situación Actual(descripción de los Sistemas de Información Actuales)
EVS 2.2, Identificación de los Usuarios Participantes en el Estudio de la Situación Actual		Catálogo de usuarios

EVS3: DEFINICION DE REQUISITOS DEL SISTEMA		
	Producto de Entrada	Producto de Salida
EVS 3.1, Identificación de las Directrices Técnicas y de Gestión	Catálogo de Normas del PSI Recopilación de Directrices Técnicas y de Gestión	Catálogo de Normas
EVS 3..3, Catalogación de Requisitos	Identificación de Requisitos Catálogo de Requisitos	Catálogo de Requisitos

Tabla 4. Métrica-EVS

Y, con la elaboración y completación de estas Fases de *Métrica*, aun cuando la Solución resultara pospuesta, podría ser retomada o replanteada ante nuevas necesidades, nunca como información obsoleta.

Y, cuidado con observar que la Solución es planteada de manera global que puede y deberá llevar aparejada medidas de Salvaguarda, ya que, aunque se tratara de una medida de dichas características no se encuentra desligada del resto del *Plan de Seguridad del Sistema de Información*.

*10.- **Diccionario[131] del Análisis de Riesgos***

Tanto los *Activos* como los motivadores de la *Gestión del Cambio* registrado en un *Documento de Seguridad* deben estar documentados mínimamente pudiendo, así mismo, ser actualizables si así se considerara para su comprensión.

Recordemos que en el caso de los *Activos*, unos pueden depender de otros dentro de un orden jerárquico de dependencias

Activos Legales vigentes en nuestra legislación por extracción semántica y orden alfabético:

al.1. *Accesos*: [a.85, a.91, a. 103, a. 113 RD 1720/2007]

a1.2.*Alquiler y Préstamo de Bases de Datos*: [D 92/100/CE]

al.3.*Asiento Electrónico*: [Orden PRE/3523/2009, RD 04/2010]

al.4.*Atención al Cliente*: [a.4 L 3/2014]

al.5.*Auditorías del Sistema Informático:* [a.27, a.28, a.29 Regl. APD], [a.8, a.33 RD 1736/1998], [a.96, a.110 RD 1720/2007]

al.6.*Autenticación*: [a.93, art. 98 RD 1720/2007]

131 En un Sistema Informático, SI, los Activos se definen como Requisitos y que se equiparan , como indicamos en el Capítulo II con los Requisitos Informados a los que se les otorga carácter legal y validez jurídica, siendo penalizable su omisión. En la Tarea de ordenar y gestionar dichos Requisitos se cuenta con una Herramienta dentro del SI, denominado *Diccionario de Datos o de Requisitos*, y donde bien sea de forma descriptiva o como definiciones que identifican los elementos de Diseño del SI, se incluyen a fin de facilitar en nuestro caso una Gestión del Cambio (Cap.III, apartado 9) dentro del EVS y , precisando, cuando manejemos el Documento de Seguridad.
El Sistema de Gestión de Seguridad de la Información, SGSI, es también un SI, y la Administración Electrónica del Documento de Seguridad se puede considerar parte de él, en lo que respecta a la Privacidad del Tratamiento de Datos de Carácter Personal observable tanto desde el Esquema Nacional de Seguridad como desde la norma internacional ISO 27002

al.7.*BBDD en Línea, Prestación de Servicios*: [D 96/9/CE Motivos] [a.36 RDL 1/1996]

al.8.*Calidad de los Datos*: [a.5 Convenio 108], [a.4, a.8, a.32 LOPD], [a.6 D 95/46/CE]

al.9.*Cifrado*: [a.35, a.39 L 32/2003]

al.10.*Código de Conducta*: [a.31 LOPD], [a.16 D 31/2000/CE]

al.11.*Consentimientos*: [a.10 D 95/46/CE], [a.6 LOPD], [a.3, a.8 L 41/2002], [a.6.2 RD 223/2002], [a.22 L 11/2007]

al.12.*Consumidores y Usuarios:* [a.38 L 32/2003], [a.102 y sgtes. RD 424/2005], [L 3/2014]

al.13.*Derechos ARCO*: [a.53, a.105 CE], [a.5, a.11. a.14, a.15, a.16, a.17,a.23 LOPD], [a.12, a.14. D 95/46/], [a.18 L 41/2002], [a.1.d L 56/2007]

al.15.*Datos de Carácter Personal*: [a.13 L 30/1984], [a.50 L 11/1998], [a. 3, a.6 LOPD], [a.34 L 32/2003], [a.17 L 59/2003], [a.3 RD 223/2004], [a.17 L 59/2003], [a.3 RD 223/2004], [a.62, a.65, a.70 RD 424/2005], [a.1.5 L 56/2007]

al.16. *Derecho 'Sui Generis'*: [a.134, a.135 L 5/1988], [a.7, a.9.b, a.9.c, a.10 D 96/9/CE], [.31.1 RDL 1/1996]

al.17. *Dimensiones de Seguridad*: [L 11/2007 Motivos] [RD 3/2010 Motivos]

al.18. *Documento de Seguridad:* [art. 81, 82, 84, 86 y Titulo VIII Cap. II y por Niveles de Seguridad Cap. III RD 1720/2007]

al.19. *Esquema Nacional de Seguridad y Sistema Nacional de Salud*: [a.42 L 11/2007]

al.20.*Ficheros*: [a.20, a.25, a.39 LOPD], [a.2 D 95/46/CE]

al.21.*Ficheros de Acuse de Recibo*: [a.13, a.16 RD 4/2009]

al.22. *Información Contrato Electrónico*: [a.10 D 31/2000/CE]

al.23. *Infracciones Agencia Protección de Datos*: [a.53.z y a.54.r L 32/2004]

al.24. *Logs*[132]: [a.23 RD 3/2010]

al.25. *Medidas de Protección de Programas de Ordenador*: [a.36.3, a.103, a. 137.3 RDL 1/1996]

al.26.*Necesidades Estadísticas*: [a.9.b D 96/9/CE], [a.9.b L 32/2003]

al.27.*Niveles de Protección*: [a.33 LOPD], [a.80, 81, Titulo VIII Cap. IV RD 1720/2007]

al.28. *Normas Técnicas*: [a.13 D 97/66/CE], [a.15 L 32/2003], [a.26.2, a.26.3 L 59/2003], [a.25 RD 1720/2007], [a.6, a.11 RD 4/2010]

al.29. *Patentes Programas de Ordenador*: [a.96, a.99 RD 1/1996]

al.30. *Procedimientos de Recuperación*: [a.94, art. 102 y art. 112 RD 1720/2007]

al.31. *Protección de la Intimidad*: [a.18, a.20 CE], [a. 1902 Código Civil], [a.8 Convenio 108], [a.12 DUDH], [a.34 L 34/2002], [a.7 L 41/2002], [a.3 L 11/2007], [a.4.2 L 56/2007]

al.32. *Protección de la Salud*: [a.43 , a.152 CE], [a.1 LO 3/1986]

132 *MAGERIT*.v.3.0. Metodología de Analisis y Gestión de Riesgos de los Sistemas de Información . (Libro II. Catálogo de Elementos: 5.3.3 Errores de Monitorización (Log); 5.4.1: Manipulación de los Registros de Actividad) *UDA. Utilidades de Desarrollo de Aplicaciones* v.1.0 Guía de Desarrollo . Eusko Jaurlaritzaren Informatika Elkartea, EJIE. Servicios Informáticos del Gobierno Vasco. Administración Electrónica del País Vasco 06/06/2011. (apartado 12.5. Logs de Aplicación e Incidencia , pag. 156)

al.33. *Prueba Documental*: [a.24 L 34/2002], [a. 38 L 59/2003]

al.34. *Receta Electrónica y Ordenes de Dispensación*: [RD 1718/2010]

al.35. *Recuperación de Documentación*: [a.21 RD 4/2010]

al.36. *Requerimientos Informados*: [a.9, a.53, a.55 L 32/2003]

al.37. *Reutilización de Bases de Datos*: [a.7.3 D 96/9/CE], [a. 133.1, 2 LPI],[[a.46, a.48 RDL 1/1996]

al..38. *Parámetros de Calidad*: [a.8 RD 1736/1998], [a.79, a.80 L 32/2003]

al.39.*Secreto*: [L 9/1968], [a. 18.3, a.55.2 CE], [a.6.2, a.7.6, a.10 LOPD], [a.33 L 32/2003], [a.8 L 59/2003], [a.70 RD 424/2005]

al.40.Seguridad de los Pacientes: [a.47 L 16/2003]

al.41.*Tarjeta Sanitaria*: [a.57 , cap. v L 16/2003]

En el caso de los *Motivadores del Cambio* en un *Documento de Seguridad,* el índice 15 de la norma I*SO 27 001* corresponde a la parte de la Auditoría Legal; a continuación se recuerda este esquema previo a proponer una posible influencia:

15 **CUMPLIMIENTO**

15.1 Cumplimiento de los requisitos legales

15.1.1 Identificación de la legislación aplicable

15.1.2 Derechos de propiedad intelectual (DPI)

15.1.3 Protección de los documentos de la organización

15.1.4 Protección de datos y privacidad de la información personal

15.1.6 Regulación de los controles criptográficos

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

15.2.1 Cumplimiento de las políticas y normas de seguridad

15.2.2. Comprobación del cumplimiento técnico

15.3 Consideraciones de las auditorías de los sistemas de información

15.3.1 Controles de auditoría de los sistemas de información

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Lo que se propone , aprovechando el Indice 15.1.1 de la ISO 27002 es completar el Diccionario del SGSI, no sólo a efectos de Documentación que debe de acompañar a una *Política de Seguridad*, o bien como *Anexo* a un *Documento de Seguridad* (en ambos casos se recomienda), sino de caras a dar Soporte a la *Gestión del Cambio* que puede ocurrir sobre un determinado *Documento de Seguridad*, debiendo reflejar un *Registro* de dicho cambio y exponiendo la aproximación más directa que provoca dicho cambio, recordando así mismo que nos podemos mover en el campo de lo hipotético o futuro, de una regla no observada(por sanción), o bien por actualización de legislación. El texto que acompaña a cada unidad legislativa descriptiva, reconocida como Ley, Orden o Real Decreto deberá resultar claro en su exposición.

Este apoyo a un 'Control de Registros' se alinea directamente con la clausula *nº 4.3.3* denominada *Control de Registros* en la ISO/IEC 27001. Eso sí, deberemos evitar tal y como indica el apartado *4.3.2.i de Control de Documentos* prevenir el uso no intencionado de documentos obsoletos.

Apuntamos las posibles *Categorías* de los *Motivadores de la Gestión del Cambio*:

- Invocación de Principios Fundamentales Universales
- Marco de Interoperabilidad
- Convergencia Jurisprudencial

- Incorporación Legislación Europea
- Actualización Parámetros Técnico Operadoras Telecomunicaciones
- Desarrollo de la personalidad jurídica
- Reglamento Medidas Seguridad
- Seguridad del Paciente
- Protección del Ingeniero de Software en la e-HC
- Defensa del Consumidor
- Estructura Organizacional del SNS
- Procesos de Certificaciones
- Estructura Tecnológica del e-SNS
- Tarjeta Sanitaria
- Procesos de Auditoría
- Procesos Transparencia
- Reutilización de la Información en el Sector Público
- Procedimientos Legales
- Aplicación Norma Internacional
- Soporte a Autoridad en materia de Seguridad

- Procesos de Migración de Entornos
- Monitorización Dimensión de Seguridad
- Desarrollo del ENS
- Actualización Especificación BBDD

La forma de *Introducción* del *Requisito Informado Legal* que se convierte en *Motivador de la Gestión del Cambio* debería resultar "parcial", en el sentido que cada *Nota* asociada a una *Categoría* de *Motivador* deba ser escueta en la especificación de su origen. No todas las Categorías deben aparecer correspondidas en la relación legislativa que hemos considerado denotar, aunque para aparecer citada la legislación correspondiente desde el *Diccionario* deberá existir alguna correspondencia con las Categorías establecidas pudiendo existir *Borradores de Notas* destinados a una 'Discusión de Categorías' del Equipo de *Analistas* del *Diccionario del SGSI.*

Decidimos, por tanto la inclusión de alguna de estas *Notas*, en base a los siguientes criterios

- destacar de otro modo más técnico, que no sea el meramente discursivo, algún *Requerimiento Informado,o Requisito Legal*
- observación no forzada del discurso de las posibles *Categorías*
- recuperar desde un par de ejemplos la aplicación del *Diccionario*
- recordarnos que no sólo la tecnología es mejorable, también la legislación y, sin embargo,siempre podemos mejorar nuestro *SGSI*, independientemente del estado del arte en el que se encuentren ambos ámbitos

En el apartado *Cap. IV, 2.2.1*, y concretamente en la citación del Cap. III encontraremos una especificación de la *Gestión del Cambio del EVS* y la indicación de los posibles vínculos legislativos en relación a la Categoría de 'Defensa del Consumidor'.

Podemos, de inicio establecer aquellas correspondencias con la *Categoría* denominada: 'Estructura Tecnológica del e-SNS' conforme a nuestras *Notas*:

- L 16/2003
- RD 183/2004
- D 97/66/CE
- L 34/2002
- L 16/2724003
- L 32/2003
- RD 183/204
- L 223/2004
- RD 424/2005
- D 2006/24/CE
- L 1030/2006
- L 11/2007
- L 56/2007
- RD 1720/2007
- D 2009/140/CE
- RD1671/2009

- RD 03/2010
- RD 04/2010
- RD 1093/2010
- RD 1718/2010
- D 2011/24/CE

Debiendo, en cualquier caso, existir flexibilidad en el Mantenimiento y Modificación del Diccionario.

mot.1.-Convenio 108 de Estrasburgo

> Su art. 5 alude directamente a la *Calidad de los Datos* indicándose que los datos de carácter personal que sean objeto de un tratamiento automatizado serán <<adecuados, pertinentes y no excesivos>> en relación con las finalidades para las cuales se hayan registrado. Así mismo serán necesarios y si fuera necesario puestos al día. Prohibiéndose la recogida de datos por medios fraudulentos.

mot.2.-Convenio de Schengen

> Se genera el llamado *Sistema de Información de Schengen , SIS*, estableciendo la libre circulación por medio de un visado. El SIS ya en su versión II consiste en la creación y mantenimiento de un sistema de información común, con una parte nacional y de una parte de apoyo técnico. La regulación de la utilización de los datos de carácter personal del SIS viene determinado por el *art. 126.3* de su reglamento en dos aspectos : a quien atribuir la responsabilidad por posibles daños y aquellas medidas que se deban adoptar en el tratamiento automatizado de datos. Cada estado participante ha de respetar una serie de condiciones entre la que se encuentra el *Control de Introducción,* de manera que pueda verificarse a posteriori qué datos de carácter personal se han introducido, en qué

momento y por qué persona.

mot.3.-Constitución de 1978

Teniendo en cuenta en particular el art. *10.2* de la C.E. , sobre el contenido de los acuerdos internacionales que obligan a España y el art. *18.4* de la CE de 1978 que postula que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Luego, existe en la Constitución otra garantía por el *art. 105* según la cual se regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la Seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas. Y aunque no se hace mención al uso de la informática no excluye en principio soporte alguno que pueda contenerlos.

mot.4.-Ley Orgánica LO 1/1982
, de protección civil del derecho al honor, a la intimidad personal y familiar,y a la propia imagen

Su art. 7 recoge la consideración de 'intromisión ilegítima' en el ámbito de protección delimitado por su *art. 2* citándola en su apartado 4 como aquella revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela. Las acciones de protección frente a intromisiones ilegítimas caducarán transcurridos cuatro años desde que el legitimado pudo ejercitarlas.

mot.5.-D 95/46/CE
, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Pretende superar las diferentes categorizaciones que se hagan de los *Niveles de Seguridad* asignados a los datos de carácter personal en plataformas similares como consecuencia de la disparidad de las disposiciones de los Estados miembros.

El *art. 18.4* de la Constitución Española de 1978 en el que se quiso fundar el nuevo derecho de *autodeterminación informativa* no estableció ningún nuevo derecho, sino un

límite a una facultad (“el uso de la informática”) derivable del derecho general de la libertad (art. 17.1 CE) o de la libertad específica de comunicación (art. 20.1 CE) sobre la base de derechos expresamente consagrados en la Constitución (“el honor y la intimidad personal y familiar”, art. 18.1. CE). Se trata pues de una clausula que establece límites expresos en el ejercicio de derechos fundamentales.

mot.6.-D 96/9/CEE
, sobre la protección jurídica de las bases de datos

Su art. 7 hace referencia al citado derecho '*sui generis*' reiterando los conceptos de extracción o reutilización, concretándose en que el préstamo público no constituya un acto de tales ejecuciones.

La mas importante diferencia geográfica de conceptualización[133] entre los cuerpos de definición de *Bases de Datos* aparece esbozada en la dicotomía D 96/9/CEE vs. RDL 1/1996, dentro del ámbito de la Comunidad Europea expresando:

- en la primera, tiene la consideración de base de datos las recopilaciones de obras, de datos o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma

- en la segunda, también son objeto de propiedad intelectual las colecciones de obras ajenas, como las antologías, u las de otros elementos o datos que por la selección o disposición de las materias constituyan creaciones intelectuales, sin prejuicio, en su caso de los derechos de los autores de las obras originales

Por otra parte, al respecto de la doble protección se detecta un plazo común de protección: *art. 10 D* y *art. 136 LPI*; al respecto de la reutilización de su contenido puede producirse cuando se transfiera el derecho o por contrato de cesión conforme al *art. 7.3 D* y *art. 2 LPI*

133 *Exposición de motivos de la D 96/9/CEE*: referencia de la palabra 'compilación' usada en el ámbito estadounidense; Exposición de motivos de la *L 5/1998:* la *Copyright Act* define la compilación como una colección de datos seleccionados de tal forma que el conjunto de ellos pueda ser observado como de original autoría

mot.7.-RDL 1/1996
, por el que se aprueba el texto refundido de la Propiedad Intelectual o LPI

El objetivo fundamental de la protección del asalariado en función de sus obligaciones se recoge en el *art. 51.5*.

Los programas que permitan la posterior utilización de las bases de de datos se encuentran protegidos en la sucesión de los *art. 95 a 104*.

En referencia a transferencias a terceros países se produce la exclusión de supuestos de protección para aquellos fabricantes que sólo pertenecen nominalmente a la Unión Europea pero que sus actividades se desarrollan en otros países ajenos . Se considera dicha protección en los *art. 10 D y art. 11.3 LPI*.

La *Comisión de Propiedad intelectual* se crea adscrita al *Ministerio de Educación, Cultura y Deporte*, como órgano colegiado de ámbito nacional. Su actuación garantiza la salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los responsables de servicios de la sociedad de información en los términos previstos en los art. 8 y concordantes de la *Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico*.

El requerimiento previo podrá considerarse , a efectos de la generación del conocimiento efectivo en los términos establecidos en los *art. 16 y 17* de la *Ley 34/2002*, siempre y cuando identifique exactamente la obra o prestación, al titular de los derechos correspondientes y, al menos, una ubicación donde la obra o prestación es ofrecida en el servicio de la sociedad de la información.

Por otra parte, las funciones de inspección, vigilancia y control de las entidades de gestión de derechos de propiedad intelectual, incluido el ejercicio de la potestad sancionadora, corresponderán a la *Comunidad Autónoma* en cuyo territorio desarrolle principalmente su actividad ordinaria.

mot.8.-Convenio de Oviedo

, de 1997, para la protección de los Derechos Humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina

Propuesto por el Consejo de Europa establece en su art. 5 que una intervención en el ámbito de la sanidad tan sólo podrá efectuarse después de que que la persona afectada haya emitido su expreso consentimiento, consentimiento que por otra parte podrá ser retirado en cualquier momento. Es el primer instrumento internacional con carácter *público vinculante* para los países que lo subscriben. De manera que, el derecho a la protección a la salud queda reforzado en el terreno de la documentación clínica.

mot.9.-D 97/66/CE

, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones

Se reparte en 16 artículos y un anexo. Los servicios deberán ser seguros y confidenciales. Se impedirán las escuchas, grabaciones u otras intercepciones no autorizadas o ilegales. La excepción supondría la autorización del usuario o supuesto de seguridad de Estado.

En relación a las características técnicas y normalización su art. 13 en los apartados siguientes presentan las siguientes singularidades:

2.Cuando las disposiciones de la presente Directiva sólo puedan aplicarse mediante la implantación de características técnicas específicas, los Estados miembros informarán a la Comisión de conformidad con los procedimientos establecidos en la D 83/189/CEE del Consejo, de 28 de marzo de 1983, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas

3. Cuando proceda, la Comisión garantizará la elaboración de normas europeas comunes para la aplicación de las características técnicas específicas, de conformidad con la legislación comunitaria en materia de aproximación de la legislación de los Estados miembros relativa al equipo

terminal de telecomunicaciones, incluido el reconocimiento mutuo de su conformidad, y con la Decisión 87/95/CEE del Consejo, de 22 de diciembre de 1986, relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones

mot.10.-L 5/1998

, de incorporación al Derecho español de la Directiva 96/9/CE sobre la protección jurídica de las bases de datos

Añadiéndole la excepción de no originalidad [134] respecto de la Directiva sobre una posible extracción parcial o reutillización en la que se ha aplicado una inversión sustancial reconocida en una obtención, verificación, y presentación aparece el derecho *sui generis*.

mot.11.-LOPDAT

, Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal

La evitación de una destrucción accidental de datos ha sido regulada por RD 994/1999 por el que se aprueba el *Reglamento de Medidas de Seguridad* de los ficheros automatizados que contengan datos de carácter personal, dando en su momento cumplimiento al *art. 9* de la derogada LORTAD, y manteniéndola vigente la LOPDAT en tanto el Gobierno no lo modifique o sustituya.

Acerca de los *Códigos Tipo* la LOPDAT en su art. 31 establece que mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular *códigos tipo* que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo. Los citados códigos podrán contener o no reglas operacionales detallada de cada sistema en particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporaran directamente al código,

134 Caso no considerado tradicionalmente por las Cortes Estadounidenses: si imaginamos la BBDD de artículos de Derecho, la localización en Internet o Url de cada uno de ellos, no goza en principio de derecho, pero su compilación sí, de manera que si fueran copiadas el conjunto de estas URLs este hecho sería protegido por la *Ley de Copyright, 17 U Code 101*

las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquel. Debiendo ser depositados o inscritos en el *Registro General de Protección de Datos* pudiendo el Director de la misma llamar a correcciones.

mot.12.-D 31/2000/CEE
, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior

Limitándonos en este apartado a una mera técnica de inserción de parte de su texto, en el *art. 152* del *Tratado de la Comunidad Económica Europea*, se cita que la protección de la salud es un componente esencial de las demás políticas comunitarias.

Un prestador de servicios puede beneficiarse de las exenciones por mera transmisión (*mere conduit*) y por la forma de almacenamiento automático, provisional y temporal, denominada "memoria tampón" (*caching*) cuando no tenga participación alguna en el contenido de los datos transmitidos; esto requiere, entre otras cosas, que no modifique los datos que transmite. Este requisito no abarca las manipulaciones de carácter técnico que tienen lugar en el transcurso de la transmisión, puesto que no alteran la integridad de los datos contenidos en la misma.

En relación a la memoria tampon o caching, los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, el prestador del servicio no pueda ser considerado responsable del almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de éstos, a condición de que:

- el prestador de servicios no modifique la información
- el prestador de servicios cumpla las condiciones de acceso a la información
- el prestador de servicios cumpla las normas relativas a la actualización de la información, especificadas de manera ampliamente reconocida y utilizada

por el sector

- el prestador de servicios no interfiera en la utilización lícita de tecnología , con el fin de obtener datos sobre la utilización de la información el prestador de servicios y actúe con prontitud para retirar la información que haya almacenado, o hacer que el acceso a ella sea imposible, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en que se encontraba inicialmente; de que se ha imposibilitado el acceso a dicha información; o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir que se acceda a ella.

mot.13.-Ley 34/2002

, de servicios de la sociedad de la información y de comercio electrónico

Su art. 7 fundamenta el principio de libre prestación de servicios para aquellos que sin ser residentes en España prestan servicio de la *Sociedad de la Información* a través de un establecimiento permanente en España, quedando la salud pública especialmente indicada en el previsto a observar por el prestador de servicios. La <<ubicación de los medios tecnológicos>> no bastan por sí solos para determinar el establecimiento del prestador.

En el caso de ejercer una profesión regulada el prestador de servicios deberá indicar si se adhiere a algún *Código Tipo de Conducta* y la manera de consultarlo electrónicamente. En la elaboración de los Códigos se ha de garantizar la participación de las asociaciones de consumidores y usuarios.

La 'acción de cesación' expresada en el *art. 30* puede ser interpuesta por personas físicas o jurídicas, grupos o asociaciones de consumidores, el Ministerio Fiscal, el *Instituto Nacional de Consumo* y organismos reconocidos por la Comunidad Europea.

mot.14.-Ley 41/2002

, básica reguladora de autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Los pacientes tienen la obligación de facilitar los datos sobre su estado físico. Cada profesional que intervenga en la actividad asistencial está obligado al respeto de las decisiones adoptadas libre y voluntariamente por el paciente en su *art. 2.6*. Idénticamente se reconoce el derecho del ciudadano a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual.

mot.15.- Ley 16/2003
, de cohesión y calidad del Sistema Nacional de Salud

Con el objeto de desarrollar el código de identificación único, el *Ministerio de Sanidad y Consumo* desarrolla una Base de Datos que permite la depuración de titulares de tarjetas. Las tarjetas sanitarias individuales deberán adaptarse a la normalización que pueda establecerse para el conjunto de las Administraciones públicas y en el seno de la Unión Europea. Idénticamente se concretan los elementos que configuran lo que se denomina infraestructura de la calidad y seguridad.

mot.16.-La Comisión del Mercado de las Telecomunicaciones, CMT

Las actividades y funciones de la Comisión del Mercado de las Telecomunicaciones se encuentran integradas en la nueva Comisión Nacional de los Mercados y la Competencia , CNMC, que ha entrado en funcionamiento el 7 de octubre de 2013, agrupando las funciones destinadas a garantizar y promover el correcto funcionamiento, la transparencia y la existencia de una competencia efectiva en todos los mercados y sectores productivos.

La Ley General de Telecomunicaciones contempla la necesidad de proteger los datos de carácter personal en el sector de las telecomunicaciones en su *art. 50* conforme a la LOPD en las normas dictadas para su desarrollo y en las normas reglamentarias de carácter técnico, cuya aprobación exija la normativa comunitaria en materia de protección de datos personales.

Uno de los objetivos a reforzar con objetivo de disfrutar de un mercado único de redes y servicios de comunicaciones electrónicas, desde la supervisión por la Comisión de las

soluciones aplicadas por la *Autoridades Nacionales de Regulación*, ANRs consiste en la modificación de las Directivas marco en materia de protección de datos de carácter personal, según consta en la COM(2007) 689 final, siendo reguladas por la D 90/398/CE. Constituye doctrina pacífica y consolidada del *Tribunal Supremo* que la CMT tiene atribuida *potestad normativa* ejercitada a través de las *circulares*; ahora bien, se reconoce la innecesariedad de dar audiencia a las asociaciones de consumidores y usuarios en el procedimiento de elaboración de circulares. Acerca de dicha legalidad se cita la SAN de 31 de marzo de 2006.

La *Declaración de Confidencialidad* regulada por disposición adicional cuarta de la Ley 32/2003 no afecta tan sólo a la recogida de requerimientos sino a toda la información aportada como consecuencia de cualquier procedimiento y actuación tramitada por la CMT. Se la puede calificar como acto de trámite cualificado en cuanto se definen los actos de trámite doctrinal y jurisprudencialmente como aquellas que se adoptan dentro de un procedimiento para impulsarlo y ordenarlo y que hacen posible la decisión con la que finaliza un acto administrativo.

En relación al secreto comercial o industrial configurado en el *art. 37.5* de la *LRJPAC*, L 30/1992, *de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común,* se afirma que no existe en el ordenamiento jurídico español una normativa que expresamente identifique cuáles son los datos o informaciones que puedan ser declarados 'confidenciales.' La Comisión Europea en la comunicación COM(139)2004 en el apartado 17.3.2 indica que se concederá acceso tan sólo a un resumen o parte de la información. Asimismo, en los puntos 23 y 24 se indica que cuando la información haya perdido su 'importancia comercial', ya no podrá considerarse confidencial. O aquellas que hablen sobre datos de mercado y que hayan superado los cinco años habrán dejado de ser confidenciales.

El Reglamento *AJ 2012/593* de Régimen Interior de la Comisión del Mercado de las Telecomunicaciones , *RRI*, incorpora las modificaciones que provocan un nuevo texto refundido a resultas de la aplicación surgidas como consecuencia de la aplicación de la Creación del Organismo reguladores Europeos de Comunicaciones , Reglamento CE nº 1211/2009, y que conforme a su Título I, Capitulo III(art. 8 a 26) conforma a la CMT bajo su régimen jurídico.

Dicho Reglamento, *RRI*, en aplicación del art. 12 *LES, Ley de Economía Sostenible , L 2/2011* consensuando el régimen de transparencia y de reserva de información establece para el adecuado funcionamiento de la Comisión los siguientes servicios, art. 11 bajo la Jefatura del Secretario: Direcciones de Asesoría Jurídica, de Administración y de Sistemas de Información, y así mismo adscritos a la Direccción General de Instrucción: las Direcciones de Análisis Económicos y de Mercados, de Estudios , Estadísticas y Recursos Documentales, de Regulación de Operadores, Dirección Técnica y Dirección de Internacional.

Concreta, en la modificación de su art. 15 y en relación a las Sesiones, que en las reuniones del Consejo podrá asistir con voz, pero sin voto, le personal directivo, y cualquier persona del personal no directivo, que determine el Presidente , de acuerdo a los criterios generales que acuerde el Consejo, y no pudiendo asistir a las reuniones los miembros del Gobierno ni los altos cargos de las Administraciones Públicas.

mot.17.-Ley 32/2003
, General de Telecomunicaciones

Su art. 7 indica la creación del *Registro de Operadores* dependiente de la *Comisión del Mercado de las Telecomunicaciones*.

Por otra parte, y de acuerdo con los principios de objetividad y de proporcionalidad, el Gobierno podrá modificar las condiciones impuestas previa audiencia de los interesados, del *Consejo de Consumidores* y usuarios e informe de la *Comisión*, siendo la modificación llevada a cabo por Real Decreto

mot.18.-Ley L 59/2003
, de 19 de diciembre , de firma electrónica

El documento electrónico es soporte tanto de documentos públicos como privados. En concreto, el *art. 3.8* nos recuerda que dicho soporte será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica, con la que

se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del art. 326 de la *Ley de Enjuiciamiento Civil*.

En relación con el *Documento de Seguridad* y las consiguientes *Medidas de Seguridad* propuestas:

- ***art. 18***, el 'mantenimiento de un Directorio' actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida

- ***art. 19***, la 'Declaración de Prácticas de Certificación', donde cada prestador de servicios formulará una declaración de prácticas de certificación en la que se detallarán las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados , las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados.

- ***art.27***, en los procedimientos de certificación se utilizarán las normas técnicas cuyos 'Números de Referencia' hayan sido publicado en el <<Diario Oficial de la Unión Europea>> y excepcionalmente por las aprobadas por el Ministerio de Ciencia y Tecnología que se publicaran en la dirección de Internet de este Ministerio.

mot.19.-RD 183/2004

, por el que se regula la tarjeta sanitaria individual[135]

135 Aunque no se le ha dedicado una especial atención a lo largo de la Tesis, a la infraestructuta de la Receta Electrónica, no queremos dejar de hacer observar la enorme carga que se le supone de trabajo al tener de trasponer los requerimientos técnicos extrapolándolos de los legales (ejemplos en el Cap. IV) que implican idénticamente la relación siguiente de legislación no visible en este apartado:

- L 29/2006, de garantías y uso racional de los medicamentos sanitarios
- RD 1302/2006, por la que se establecen las Bases del Procedimiento para la designación y acreditación de los centros, servicios, y unidades de refrencia del Sistema Nacional de Salud

A efectos de desarrollo del Sistema Informático , el *art. 5* , constituye la Base de Datos de datos de población protegida del *Sistema Nacional de Salud, SNS*, que que recoge la información básica de los usuarios del *SNS*, así como el fichero histórico de las situaciones de aseguramiento y de la adscripción de la persona, en su caso, a diferentes Administraciones sanitarias a lo largo de su vida. Esta BBDD incorporará información del sistema de *Seguridad Social* y del mutualismo administrativo, con el fin de suministrar a las Administraciones sanitarias datos permanentemente actualizados que permitan la correcta gestión de las situaciones de las personas respecto a altas, bajas, cobertura de prestaciones y movilidad de pacientes en la *Unión Europea*, de acuerdo con los reglamentos comunitarios vigentes en esta materia. El plan de explotación estadística de la base de datos será acordado por el *Consejo Interterritorial del Sistema Nacional de Salud*, y la información obtenida se pondrá a disposición de las Administraciones sanitarias. En todo caso, la información que se facilite a estos fines será previamente objeto de disociación.

La BBDD se diseña técnicamente en torno al código de identificación personal que incorpora la tarjeta sanitaria individual y que, a su vez, deberá incorporar los datos básicos comunes1 de forma normalizada y visible.

En relación a las medidas de seguridad a adoptar será el *Consejo Interterritorial del Sistema Nacional de Salud* el que determinará la relación de agentes del sistema sanitario autorizados para el acceso a la base de datos y sus capacidades de operación. También, en caso de considerar necesaria la cesión de los datos de esta base, recabará la asistencia de la *Agencia Española de Protección de Datos*, a fin de que por ésta se determinen los supuestos bajo los que podrá efectuarse la cesión a terceros. Dicha cesión se atendrá, en todo caso, a la normativa vigente en materia de protección de datos personales

- RD 1039/2011, por el que se establecen los criterios marco para garantizar un tiempo máximo de acceso a las prestaciones sanitarias del Sistema Nacional de Salud
- RD 640/2014, por el que se regula el Registro Estatal de Profesiones Sanitarias

No obstante, aconsejamos en tal respecto la lectura de SIMARRO Escribano Jose Manuel. "Los Sistemas de Información de Registro de Medicamentos". I+S Informática y Salud. Nº 106 . Setiembre 2014.

mot.20.-Ley 223/2004

, por el que se regulan los ensayos clínicos con medicamentos

En ella aparecen las principales definiciones y actores que se manejan en el *Capítulo de Escenarios*. Garantiza la salvaguarda de la integridad física y mental del sujeto, así como su intimidad y la protección de sus datos, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

mot.21.-RD 424/2005

, por el que se aprueba el Reglamento de las condiciones para la prestación de servicios de comunicaciones electrónicas, el Servicio Universal[136] y la protección de los usuarios

Los operadores deberán notificar a la *Comisión del Mercado de las Telecomunicacione*s cada tres años, contados desde la notificación inicial, su intención de continuar con la prestación o explotación de la red o servicio.

Según su *art. 5* el interesado en prestar estos servicios deberá incluir la siguiente información, junto con la documentación que acredite su autenticidad:

- Breve descripción de la ingeniería y diseño de red, en su caso
- Tipo de tecnología o tecnologías empleadas
- Descripción de las medidas de seguridad y confidencialidad que se prevén implantar en la red, en su caso
- Descripción funcional de los servicios
- Oferta de servicios y su descripción comercial

136 Se define el S*ervicio Universal* como el conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una calidad determinada y a un precio asequible. En relación a la aplicación de los niveles de servicio al conjunto de los usuarios, el Ministerio de Industria, Turismo y Comercio podrá establecer ámbitos de análisis mas restringidos y fijar para dichos ámbitos niveles mínimos de calidad de servicio. Dichos niveles de calidad y aquellos métodos y procedimientos de control están regulados por la *Orden TIC/912/2006* incluyéndose la especificación de la obligación de publicar los parámetros de calidad del servicio.
art. 22 L 32/2003; D 2002/22/CE, L 56/2007, RD 424/2005, ORDEN ITC/912/2006, ORDEN PRE/531/2007

- La fecha prevista para el inicio de la actividad

Las definiciones y métodos de medida de los *Parámetros de Calidad de Servicio*, los requerimientos relativos a la remisión periódica de los datos a la Administración, las condiciones orientadas a garantizar la fiabilidad y la posibilidad de comparación de los datos y las demás condiciones relativas a la medida y seguimiento de los niveles de calidad de servicio serán las establecidas mediante orden ministerial.

Los parámetros que se establezcan en dicha orden incluirán los que figuran en la norma del *Instituto Europeo de Normas de Telecomunicación ETSI* EG 201 769-1 y el desglose regional será, como mínimo, por Comunidad Autónoma.

mot.22.-D 2006/24/CE

, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE

La Directiva lista y especifica para cada procedimiento los datos necesarios a incorporar, dígase en:

- la identificación del origen de datos
- la identificación del destino de las comunicaciones
- la identificación de la fecha, hora y duración de una comunicación
- la identificación del tipo de comunicación
- la identificación del equipo de comunicación: IMSI (identidad internacional del abonado móvil) e IMEI (identidad internacional del equipo móvil)
- la identificación de la localización del equipo de comunicación móvil

mot.23.-Ley 1030/2006

, por la que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el procedimiento para su actualización

Por invocación expresa del art. *43* de la *Constitución Española*, donde se reconoce el derecho a la protección de la salud y establece que compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios, el *art. 10* de la Ley dedica los Servicios de información a los usuarios del *Sistema Nacional de Salud, SNS*, en los términos siguientes: tendrán derecho a la información y, en su caso, tramitación de los procedimientos administrativos necesarios para garantizar la continuidad de la atención sanitaria; a la expedición de los partes de baja, confirmación, alta y demás informes o documentos clínicos para la valoración de la incapacidad u otros efectos; la documentación o certificación médica de nacimiento, defunción y demás extremos para el Registro Civil.

Y con dedicación al *art. 45* de la *Ley General de Sanidad*, recordando las prestaciones que comprenderá el Catálogo, concretará en el art. de la Ley la Cartera de servicios complementaria de las comunidades autónomas apoyándose en el Consejo Interterritorial del Sistema Nacional de Salud que conocerá, debatirá y, en su caso, emitirá recomendaciones, sobre el establecimiento por parte de las comunidades autónomas de prestaciones sanitarias complementarias a las prestaciones comunes del Sistema. Idénticamente y en la otra dirección, las comunidades autónomas pondrán en conocimiento del Ministerio de Sanidad y Consumo los servicios complementarios no contemplados en la cartera de servicios comunes del Sistema Nacional de Salud

mot.24.-Ley 11/2007,
de 22 de Junio , de acceso electrónico de los ciudadanos a los Servicios Públicos

Por primera vez cita esta ley lo que en un real decreto posterior RD 3/2004 se ha venido en denominar *Dimensiones de la Seguridad*: asegurando el acceso, la integridad, la autenticidad, la disponibilidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

El art. 41 da entrada al *Esquema Nacional de Interoperabilidad* y el *Esquema Nacional de Seguridad* que serán aprobados por real decreto de Gobierno.

mot.25.-Ley 37/2007
, sobre reutilización de la información en el sector público

Adoptando la *D/2003/98/CE*, puede poseer un gran interés para determinadas empresas en los ámbitos de su operación y para los ciudadanos en la aplicación de la transparencia. Serán las Administraciones y los Organismos Públicos los que los que decidan o no autorizar o no la reutilización de los *Documentos*[137] o Categoría de Documentos conservados con fines comerciales o no comerciales, aportando un valor añadido al derecho de acceso .

La ley no será aplicable en los supuestos siguientes: para aquellos documentos para los que se exiga ser un titular de derecho, sobre los que existan derechos de propiedad intelectual o industrial por parte de terceros, los conservados por instituciones educativas y de investigación, tales como los centros de investigación, con inclusión de organizaciones creadas para la transferencia de los resultados de la investigación, aunque

137 Artículo 3. *Ámbito objetivo de aplicación*
Se entiende por documento toda información cualquiera que sea su soporte material o electrónico así como su forma de expresión gráfica, sonora o en imagen utilizada. A estos efectos no se considerarán documentos los programas informáticos que estén protegidos por la legislación específica aplicable a los mismos.3. La presente ley no será aplicable a los siguientes documentos que obren en las Administraciones y organismos del sector público previstos en el artículo 2: a) Los documentos sobre los que existan prohibiciones o limitaciones en el derecho de acceso en virtud de lo previsto en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y las demás normas que regulan el derecho de acceso o la publicidad registral con carácter específico. b) Los documentos que afecten a la defensa nacional, la seguridad del Estado, la protección de la seguridad pública, así como los sometidos al secreto estadístico y a la confidencialidad comercial y, en general, los documentos relacionados con actuaciones sometidas por una norma al deber de reserva, secreto o confidencialidad. c) Los documentos para cuyo acceso se requiera ser titular de un derecho o interés legítimo. d) Los documentos que obran en las Administraciones y organismos del sector público para finalidades ajenas a las funciones de servicio público que tengan atribuidas definidas con arreglo a la normativa vigente. e) Los documentos sobre los que existan derechos de propiedad intelectual o industrial por parte de terceros. No obstante, la presente ley no afecta a la existencia de derechos de propiedad intelectual de las Administraciones y organismos del sector público ni a su posesión por éstos, ni restringe el ejercicio de esos derechos fuera de los límites establecidos por la presente ley. El ejercicio de los derechos de propiedad intelectual de las Administraciones y organismos del sector público deberá realizarse de forma que se facilite su reutilización. que gestionen los servicios esenciales de radiodifusión sonora y televisiva y sus filiales. g) Los documentos conservados por instituciones educativas y de investigación, tales como centros escolares, universidades, archivos, bibliotecas y centros de investigación, con inclusión de organizaciones creadas para la transferencia de los resultados de la investigación. h) los documentos conservados por instituciones culturales tales como museos, bibliotecas, archivos históricos, orquestas, óperas, ballets y teatros. 4. Lo previsto en esta ley no restringirá las previsiones más favorables que sobre acceso o reutilización se establezcan en las leyes sectoriales.

pudiendo prever los acuerdos sectoriales.

La ley encuentra su desarrollo en el real decreto *Real Decreto 1495/2011*. El régimen administrativo de la reutilización considera los supuestos de: sujeción a condiciones de licencias-tipo, previa solicitud o sin condiciones.

En cualquier caso, el ejercicio de los derechos de propiedad intelectual de las Administraciones y organismos del sector público deberá realizarse de forma que se facilite su reutilización. Observar que en el desarrollo de esta Tesis y previo a su finalización hemos incluido esta última actualización de Octubre de 2014.

Con fundamento, perfila la existencia de *Sistemas de Gestión Documental* que facilite a los ciudadanos su adecuada recuperación. El *art. 8* de la Ley establece las condiciones de reutilización en los términos siguientes: que el contenido de la información no sea alterado, que no se desnaturalice el sentido de la información y que se cite la fuente.

mot.26.-Ley 56/2007
, de Medidas de Impulso de la Sociedad de la Información

El *art. 11.3* garantiza que en la adopción y cumplimiento de las medidas a que se refieren se respetarán, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección a los datos personales, a la libertad de expresión o a la libertad de información, cuando estos términos pudieran resultar afectados. El *art. 12* dice textualmente que los destinatarios y prestadores de Servicios de la Sociedad de la información podrán dirigirse a cualesquiera órganos competentes en materia de la Sociedad de la información, Sanidad y Consumo de las Administraciones Públicas, para:

a) conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica

b) informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos

c) obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica

Redefine la firma electrónica en su *art. 5.1* considerando como tal la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. Continuando siendo adoptado como prueba documental el soporte en que se hallaren firmados electrónicamente los datos en un juicio.

mot.27.-RD 1720/2007

, Reglamento de desarrollo de la LO 15/1999, de protección de datos de carácter personal, sustituye al RD 1720/2007

En el apartado de Definiciones, su *art. 5.g.* nos recuerda que el dato de carácter personal relacionado con la salud se refiere, en cualquier caso, a aquellas informaciones concernientes a la salud pasada, presente y futura, física y mental, de un individuo, y en particular, se considerarán datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética. Por su parte el apartado 5.h. en relación al destinatario o cesionario, nos recuerda que se trata de aquella persona física o jurídica, pública o privada u órgano administrativo, al que se revelaran los datos; pudiendo ser idénticamente destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

La Agencia Española de Protección de Datos garantizará un Nivel adecuado de protección en las Transferencias a Estados, recordándonos el *art. 66* que es el que rige su Autorización y Notificación produciéndose su consiguiente inscripción en el Registro General de Protección de Datos y pudiéndose producirse la suspensión temporal de las mismas.

En relación a las operaciones de outsourcing o de posibilidad de subcontratación de servicios, el art. 21 se llega a observar , inclusive, el hecho de dicha posibilidad cuando no hubiera sido prevista la circunstancia previamente en contrato, debiendo someterse al responsable del tratamiento y el subcontratista ser considerado encargado del tratamiento siéndole de aplicación el art. 20.3. Además, se respetará escrupulosamente el hecho de que el encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiere encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello.

El responsable del fichero como primera obligación tiene la elaboración de un *Documento de Seguridad* que deberá observar en cualquiera caso el personal que tenga acceso a los datos automatizados de carácter personal y a los sistemas de información, con lo que al menos se contemplarían las siguientes consideraciones:

- medidas, normas, procedimientos, reglas y estándares que garanticen el nivel de seguridad exigible

- estructura de los ficheros protegidos y descripción de los sistemas de información que tratan

- procedimiento de realización de copias de respaldo y de recuperación de datos teniendo dicho responsable la obligación de actualizar dicho documento, en función de los cambios relevantes que se produzcan en el sistema o su organización y, por supuesto para ajustarse a los cambios de legislación vigente; dicho documento deberá registrar la identidad de aquellas personas que estén autorizadas para conceder, cambiar o anular las autorizaciones.

mot.28.-D 2009/136/CE

, de 25 de Noviembre, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) Nº 2006/2004 sobre la cooperación en materia de protección de los consumidores

Esta Directiva incluyendo la definición de “violación de los datos personales” como aquella violación de la seguridad que provoque la destrucción accidental ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados de datos personales transmitidos , almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad, nos recuerda que resulta necesario garantizar que todos los consumidores y los usuarios gocen del mismo nivel de protección de la intimidad y de sus datos personales, independientemente de la tecnología utilizada para prestar un determinado servicio.

Puesto que dicha violación conlleva el fraude o usurpación de identidad, daños materiales, humillación grave o daño para la reputación, el abonado o afectado negativamente deberá recibir notificación inmediata a fin de que se puedan adoptar las precauciones necesarias, incluyéndose información sobre las medidas adoptadas por el proveedor para atajar la violación, así como recomendaciones para el abonado o particular afectado.

A la hora de determinar las medidas de ejecución sobre la seguridad del tratamiento se contará con todas aquellas autoridades y organizaciones europeas tales como la Agencia Europea de Seguridad de las Redes y de la Información, ENISA, el Supervisor Europeo de Protección de Datos y el Grupo de Trabajo en materia de protección de datos personales.

Como novedades e invocando futuros servicios relativos a la Telemedicina se cuenta con el número único europeo de llamada de emergencia “112” y el correspondiente para dar parte de la desaparición de niños “116000”.

mot.29.-D 2009/140/CE

, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/21/CEE relativa a un marco regulador común de las redes de comunicaciones electrónicas , la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas

Cuenta con la importante expresión de la definición de "acceso" o la puesta a disposición de otra empresa, en condiciones definidas y sobre una base exclusiva o no, de recursos o servicios con fines de prestación de servicios de comunicaciones electrónicas, incluyendo cuando se utilicen para el suministro de servicios de la sociedad de la información o de servicios de contenidos de radiodifusión. El término abarca, así mismo, otros aspectos como los siguientes: el acceso a elementos de redes y recursos asociados que pueden requerir la conexión de equipos por medios fijos y no fijos, el acceso a infraestructuras físicas, como edificios, conductos y mástiles, el acceso a sistemas informáticos incluyendo los sistemas de apoyo operativo; el acceso a sistema de información de bases de datos para prepedidos, suministros, pedidos, solicitudes de mantenimiento y reparación y facturación; el acceso a la conversión del número de llamada o a sistemas con una funcionalidad equivalente; el acceso a redes fijas y móviles, y el acceso a sistemas de acceso condicional para servicios de televisión digital y el acceso a servicios de redes virtuales.

Se promueve la aplicación de normas o recomendaciones internacionales aprobadas por la *Unión Internacional de Telecomunicaciones, UIT, la Conferencia Europea de Administraciones de Correos y Telecomunicaciones, CEPT, la Organización Internacional de Normalización, ISO y la Comisión Electrotécnica Internacional, CEI.*
Resolviendo , en cualquier caso, los litigios transfonterizos mediante el derecho de consulta al *ORECE*[138], pudiendo este Órgano emitir dictámenes que idénticamente deberán tener en cuenta las autoridades nacionales de reglamentación.

mot.30.-RD 1671/2009

, de 6 de Noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

Dejando aparte el Desarrollo del *Punto Neutro Judicial* que resulta más orientado al

138 Reglamento (CE) Nº 1211/2009 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por el que se establece el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) y la Oficina. La función principal del ORECE consiste en asesorar y asistir a la Comisión Europea en el desarrollo del mercado interior, creando a la vez un vínculo entre las Autoridades Reguladoras Nacionales (ARN) y la Comisión. Además, el ORECE debe servir como órgano de reflexión, debate y asesoramiento para el Parlamento Europeo, el Consejo y la Comisión en el ámbito de las comunicaciones electrónicas. Por tanto, el ORECE debe prestar asesoramiento al Parlamento Europeo, al Consejo y a la Comisión, bien a petición de estos o bien por propia iniciativa. El consejo tiene como misión principal la de adoptar todas las decisiones relativas al ejercicio de las funciones del ORECE y ejecutar las tareas del ORECE, entre las que figuran: atender consultas sobre proyectos de medidas relativas al acceso efectivo al número de llamada de urgencia 112 y a la aplicación efectiva de los números 116

Facultativo que participa del Órgano Judicial aun cuando pretenda integrar Accesos a Sedes Electrónicas que aún no han encontrado su limitación en número, este Real Decreto está íntegramente orientado al Usuario en cuanto de Acceso a Registros y Sedes Electrónicos, de momento parcial o de forma individual por Sectores de Actividad o Ministerios.

Nos recuerda su *art. 3. 2* que las sedes electrónicas se crearán mediante orden del Ministro correspondiente o resolución del titular del organismo público, que deberá publicarse en el «Boletín Oficial del Estado», con el siguiente contenido mínimo:

> a) Ámbito de aplicación de la sede, que podrá ser la totalidad del Ministerio u organismo público, o uno o varios de sus órganos con rango, al menos, de dirección general.
>
> b) Identificación de la dirección electrónica de referencia de la sede.
>
> c) Identificación de su titular, así como del órgano u órganos encargados de la gestión y de los servicios puestos a disposición de los ciudadanos en la misma.
>
> d) Identificación de los canales de acceso a los servicios disponibles en la sede, con expresión, en su caso, de los teléfonos y oficinas a través de los cuales también puede accederse a los mismos.
>
> e) Medios disponibles para la formulación de sugerencias y quejas.
>
> f) Cualquier otra circunstancia que se considere conveniente para la correcta identificación de la sede y su fiabilidad.

mot.31.-Resolución De Madrid

, Estándares internacionales sobre Protección de Datos Personales y Privacidad

Bajo la premisa de la Trasferencia Internacional de Datos propone como medidas proactivas el establecimiento de procedimientos destinados a prevenir y detectar infracciones, que podrán basarse en modelos estandarizados de gobierno y/o gestión de la seguridad de la información, y la puesta en práctica de estudios de impacto sobre la privacidad previos a la implementación de nuevos sistemas y/o tecnologías de información destinados al tratamiento de datos de carácter personal.

Define un conjunto de principios y derechos que garanticen dicha protección:

- de lealtad y legalidad
- de finalidad
- de proporcionalidad
- de calidad
- de transparencia
- de responsabilidad
- de legitimación

Para el presente caso, se mantiene la consideración de datos de carácter personal a aquel que afecta a la esfera más íntima del interesado con el añadido de sensible a los datos relativos a la salud o a la sexualidad.

La Conferencia resuelve que la Propuesta para Redacción de Estándares Internacionales para la Protección de la Privacidad demuestra la viabilidad de tales estándares como un nuevo paso hacia la elaboración , en el momento oportuno, de un instrumento internacional vinculable. Aprobada entre los días 4 y 6 de noviembre de 2009 con motivo

de la celebración de la "Privacy Conference" en su 31ª edición.

mot.32.-RD 3/2010

, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

El *Esquema Nacional de Seguridad* se crea con objeto de dar respuesta del *art. 42* de la *Ley 11/2007*, de acceso electrónico de los ciudadanos de los servicios públicos.

Dicho nivel de confianza alude a la resistencia mostrada frente a los accidentes o acciones ilícitas o malintencionadas que comprometan las denominadas *Dimensiones de la Seguridad* que recoge su Anexo I, a saber: la Disponibilidad, Autenticidad, Integridad y Confidencialidad, de los datos almacenados o transmitidos y, por otra parte, de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

El primer objeto de esta norma es determinar la Política de Seguridad que se ha aplicar, teniendo que ser aplicado por las Administraciones Públicas para asegurar las mencionadas *Dimensiones de Seguridad*.

El *art. 6* defiende y postula un equilibrio entre la naturaleza de los datos y los tratamientos que recibe.

mot.33.-RD 4/2010

, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

A tener en cuenta para futuras actuaciones legislativas se atiene al *Marco Europeo de Interoperabilidad*, y a la *Decisión 922/2009* relativa a las soluciones de interoperabilidad para las administraciones públicas europeas, a los planes de acción sobre administración electrónica en materia de interoperabilidad y de aspectos relacionados, particularmente, con la política comunitaria de compartir, reutilizar y colaborar.

Reconocido dicho protagonismo se reitera que debe ser abordado por la regulación del

Estado, y en concreto haciendo alusión a la *Ley 11/2007*:

- *art. 4*, de impulso de la Administración electrónica o e-Administración
- *art. 40*, de cooperación entre AAPPs
- *art. 41*, en relación a la aplicación de Medidas de Seguridad
- *art. 42.1*, donde se crea el Esquema Nacional de Interoperabilidad

Se establecerá y mantendrá actualizada la *Relación de Modelos de Datos de Intercambio*, siendo las definiciones y codificaciones empleadas en los modelos de datos tendrán en cuenta lo dispuesto de la *Ley 12/1989*, de la *Función Estadística Pública*.

El patrón nacional de Tiempo será sincronizado con la fecha y hora del *Real Instituto y Observatorio de la Armada* conforme *RD 1308/1992*.

Por el *art. 17* se enlazarán los directorios de aplicaciones para su libre reutilización a los que se refiere el *art. 46* de la *Ley 11/2007* entre sí.

mot.34.-RD 207/2010

, por el que se establecen las condiciones del uso tutelado de técnicas,tecnologías y procedimientos sanitarios, y se modifica el RD 1207/2006 por el que se regula la gestión del Fondo de Cohesión Sanitaria

Por modificación del real decreto *RD 1207/2006*, por el que se regula la gestión del Fondo de Cohesión Sanitaria, la asistencia sanitaria referida es la que contempla el catálogo de prestaciones del Sistema Nacional de Salud, definido en la *L 16/2004* y desarrollada por real decreto *RD 1030/2006* por la que se establece la *Cartera de Servicios comunes del Sistema Nacional de Salud* y el procedimiento para su actualización.

Con carácter previo a la puesta en marcha del 'uso tutelado'[139] se deberá elaborar un protocolo de selección y seguimiento de los pacientes, constatando y usando idénticas palabras que el expone el real decreto, que en el consentimiento informado de los pacientes a los que se les aplicara la técnica,tecnología o procedimiento se explicite se les indique que está sometido a uso tutelado.

Durante el período de uso tutelado, se recogerá y procesará la información que desarrolla la *Cartera de Servicios Centrales del SNS*.

Por su parte, el Órgano *Evaluador Tutelador* elaborará un Protocolo de Uso Tutelado que recopilará, entre otras cosas, los resultados y las complicaciones a corto, medio y largo plazo imprescindibles para la toma de decisiones, el procedimiento de recogida de información y de seguimiento del cumplimiento del protocolo del estudio.

El Órgano *Evaluador Tutelador* tienen por obligación velar por el cumplimiento de la *Ley de Protección de Datos L 15/1999*, y la *L 41/2002* reguladora de la autonomía del paciente y de derech

mot.35.-RD 1093/2010

, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud

Permite mediante una relación de Anexos detallados en su art. 3 los modelos de Datos completo con cuya especificación deben estar definidas las Bases de Datos del *SNS*:

- informe clínico de alta
- informe clínico de consulta externa
- informe clínico de urgencias

139 mecanismo para determinar el grado de seguridad, eficacia, efectividad o eficiencia de una técnica, tecnología o procedimiento, en los casos en los que no exista suficiente información que lo avale, antes de decidir sobre la conveniencia o necesidad de actualizar la cartera de servicios regulada mediante el Real Decreto 1030/2006, de 15 de septiembre, por el que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el procedimiento para su actualización.

- informe clínico de atención primaria
- informe de resultados de pruebas de laboratorio
- informe de resultados de pruebas de imagen
- informe de cuidados de enfermería
- historia clínica resumida

Pudiendo las Comunidades Autónomas establecer sus respectivos modelos, siendo su extensión a la *Mutualidad General de Funcionarios Civiles del Estado*, MUFACE, el *Instituto Social de las Fuerzas Armadas*, ISFAS, y la *Mutualidad General Judicial* , MUGEJU en virtud de los conciertos que éstas subscribieran.

mot.36.-RD 1718/2010
, sobre receta médica y órdenes de dispensación

Le dedica el Capítulo VIII a la custodia y protección de datos, siendo el ar. 11 el que nos recuerda que en relación a la confidencialidad de datos el sistema de receta electrónica garantizará .-la seguridad en el acceso y trasmisión de la información, implementándose medidas de seguridad de nivel alto, de modo que dicha información solo será accesible desde la oficina de farmacia a efectos de dispensación, residiendo de forma permanente en los sistemas informáticos no pudiéndose ser almacenada en los repositorios o servidores ajenos y no gestionados por las Administraciones sanitarias establecidos para efectuar la facturación.

Posibles implicaciones para el modelo de datos se constatan en la definición de formatos y datos comunes tanto para la receta pública como la privada, distinguiéndose los bloques correspondientes al prescriptor, el paciente y la receta propiamente dicha en los art. 3, 4 y 5.

Por redacción formal de parte de este último , consta que:

1.- el Ministerio de Sanidad, Política Social e Igualdad facilita el acceso al resto de las Administraciones Sanitarias, incluidas las mutualidades de funcionarios, a sus sistemas electrónicos provisores del código identificador unívoco del usuario del Sistema Nacional de Salud y del Nomenclator oficial de productos farmacéuticos de dicho Sistema en el que figuran los códigos de identificación inequívoca de los medicamentos y productos sanitarios, sus formas farmacéuticas, vías y unidades de dosificación, así como el contenido de los envases comerciales y sus condiciones de financiación en el Sistema Nacional de Salud y además su posible dispensación en unidades concretas. Se facilitará el acceso a otras bases de datos del Ministerio de Sanidad, Política Social e Igualdad que ofrecen información sobre los medicamentos y productos sanitarios autorizados.

2.- a fin de garantizar la interoperabilidad entre los diferentes servicios de salud, las recetas médicas electrónicas de cada una de las Administraciones sanitaria deberán incorporara el código identificador unívoco de usuarios del Sistema Nacional de salud y el código de identificación del medicamento o del producto sanitario y del resto de parámetros de definición del tratamiento prescrito que figuren en el nomenclátor oficial de productos farmacéuticos del Sistema Nacional de Salud

3.- El Sistema de receta médica electrónica de cada una de las Administraciones del Sistema Nacional de Salud posibilitará la identificación del régimen de pertenencia del paciente, a efectos de cobro de la aportación que en cada caso corresponda, y la realización de la facturación de las oficinas de farmacia a la correspondiente

Administración sanitaria por medios telemáticos con las necesarias medidas de seguridad y control que garanticen su correspondencia con las dispensaciones realizadas.

En las recetas médicas de la Red Sanitaria Militar de las Fuerzas Armadas en lugar del número del colegiado podrá consignarse el número de Tarjeta Militar de Identidad del facultativo; así mismo se hará constar , en su caso, la especialidad oficialmente acreditada que ejerza.

mot.37.-Directiva 2011/24/CE

, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza

La condición de asegurado no se asegura en un estado Miembro mientras que la estancia de una persona en territorio de Estado miembro no sea conforme al de la legislación de dicho Estado o de estancia en su territorio. De todas formas, se presenta un marco para la coordinación de los sistemas de seguridad social que obvia la asistencia a la hora de realizar tareas rutinarias y diarias, la asignación de órganos y el acceso a los mismos con fines de trasplante y los programas de vacunación pública.

Existe una repercusión directa sobre el caso de la telemedicina, que se considerá asistencia sanitaria prestada en el Estado miembro donde esté establecido el prestador.

El artículo 6 garantiza los Puntos Nacionales de Contacto, pudiendo ser estos uno o varios, poniendo la Comisión esta información a disposición del público , consultando estos puntos a las organizaciones de pacientes, los prestadores de asistencia sanitaria y los organismos de seguros sanitarios.

Los gastos de la asistencia sanitaria transfronteriza serán reembolsados o abonados directamente pro el Estado miembro de afiliación hasta la cuantía que habría asumido dicho Estado si la asistencia sanitaria se hubiera prestado en su territorio,sin exceder del coste real de la asistencia sanitaria prestada.

El art. 9 permite garantizar que los procedimientos administrativos relativos al disfrute de asistencia sanitaria y el reembolso de los gastos sanitarios se basen en criterios objetivos y no discriminatorios, que sean necesarios y proporcionados al objetivo a lograr. Estas decisiones individuales podrán ser impugnadas en procedimientos judiciales, lo que incluye la adopción de medidas cautelares.

En relación a nuestra Tesis la presente Directiva se aplicará sin perjuicio de lo establecido en la D 95/46/ce y la D 2002/58/CE relativas al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, e idénticamente sobre el reglamento (CE) nº 1338/2008 sobre estadística comunitarias de salud pública y de salud y seguridad en el trabajo.

A fin de garantizar la continuidad de la atención los pacientes que hubieran recibido tratamiento tendrán derecho a obtener en papel o en forma electrónica la historia clínica de dicho tratamiento y como mínimo una copia del mismo.

El objetivo de la red de evaluación de las tecnologías sanitarias que se propone sea voluntaria tratará de evitar la duplicación de las evaluaciones. Esta nueva red de Sanidad electrónica intentará prolongar las existentes de dispensación de Receta Electrónica. En

cualquier caso, sea cual fuera la recepción en Farmacia de la Receta podrá ser denegada mientras sea discriminatoria o existieran dudas legítimas y justificadas sobre la autenticidad, el contenido o la inteligibilidad de una receta determinada.

mot.38.-RD 1495/2011

, por el que se desarrolla la Ley 37/2007, sobre reutilización de la información del sector público para el ámbito del sector público estatal

Los documentos reutilizables en formato no electrónico serán puestos a disposición del público previa solicitud. En respuesta al *Esquema Nacional de Interoperabilidad* en el ámbito de la Administración Electrónica los documentos en formato electrónico

reutilizables podrán incluir entre sus metadatos una indicación de su última fecha de actualización y una referencia a las condiciones de reutilización aplicables en cada momento.

Se considerará una 'ubicación única' en la que los órganos de la Administración General del Estado y los demás organismos y entidades informarán de manera estructurada y usable sobre qué documentación es susceptible de ser reutilizada, los formatos en que se encuentra disponible, las condiciones aplicables a su reutilización, indicando la fecha de la última actualización de los documentos reutilizables.

Su Capítulo IV expone el régimen aplicable a documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales, configurándose esta información como suficiente conjuntamente con la edición por el entonces *Ministerio de Hacienda y Administraciones Públicas* de la *Guía de Aplicación del Real Decreto 1495/11*2 con indicaciones precisas del tipo de recurso humano a dedicar a Soporte en la labor de Reutilización y la aplicación de Formatos y observación de la reglamentación en materia de protección de datos.

mot.39.-Orden HAP/566/2013
, por la que se regula el Registro Electrónico Común

Y siendo la presente Orden sometida al previo Informe de la Agencia de Protección de Datos de conformidad a lo dispuesto en el art. 37 párrafo h) de la Ley Orgánica 15/1999, y conocida como LOPD.

La sede electrónica del *Punto de Acceso General* regulado por el *art. 9* del *RD 1671/2009* contendrá la información que facilite a los interesados la utilización de los procedimientos de identificación y firma electrónica admitidos, o el enlace con la dirección en que dicha información se contenga. Asimismo, incluirá información detallada sobre la utilización, validación y conservación de los ficheros de acuse de recibo entregados como consecuencia de la presentación de cualquier tipo de documento ante el *Registro Electrónico Común*.

Se aconseja prestar atención a la diversidad de expresión semántica expresada entre la derogada PRE/3523/2009 y en relación a las Dimensiones de Seguridad y la Orden que la sustituye:

- el art.5 de la derogada nos transmite que los sistemas de información que soporten las sedes electrónicas deberán garantizar la confidencialidad, disponibilidad e integridad de las informaciones que manejan. El *Esquema Nacional de Interoperabilidad* y el *Esquema Nacional de Seguridad* establecerán las previsiones necesarias para ello.

- El art. 5 de la sustituta y en relación al acceso del Registro Electrónico Común confirma que incluirá información detallada sobre la utilización, validación y conservación de los ficheros de acuses de recibo , integrados como consecuencia de la presentación de cualquier tipo de documento ante el Registro Electrónico Común. Por su parte, y en relación y en relación a los Documentos Admisibles el art.6 indica que los documentos admitidos se ajustarán a lo establecido en el RD 04/2010.

- En cada Administración Pública existirá, al menos, un sistema de registros electrónico suficiente para recibir todo tipo de solicitudes , escritos y comunicaciones dirigidas a la Administración Pública, fundamentado sobre el art. 31 RD 1671/2009 que establece la creación, naturaleza y fundamento del Registro Electrónico Común.

Dicho Registro emitirá automáticamente por el mismo medio un recibo electrónico firmado mediante alguno de los sistemas de firma previstos en el art. 18 de la L 11/2007 con, al menos, el siguiente contenido: número o código de registro individualizado, fecha y hora de presentación , copia autenticada del escrito, enumeración y denominación de los documentos adjunto, y en el caso de la inscripción a proceso selectivos, el plazo establecido para su resolución y notificación del procedimiento.

Su Anexo III, especifica la definición del Nombre de sus Fichero, REC, siéndole de

aplicación un Nivel de Seguridad Básico, conforme al esquema de aplicación de Medidas de Seguridad.

La clausula aplicable de *no incremento de gasto público*, derivada de su art. 3 y disposición adicional tercera, concreta que aun cuando la medidas contenidas en esta orden se atenderán con los medios personales y materiales existentes en el Ministerio de Hacienda y Administraciones Públicas, que actuando como registro específico para la inscripción y pago de la correspondiente tasa en las convocatorias de procesos selectivos en relación con el ingreso en Cuerpos o Escalas de personal funcionario o en plazas de personal laboral adscritos a la Administración General del Estado y sus Órganos Públicos vinculados o dependientes asiste un acuerdo de gestión entre el órgano convocante y el Ministerio de Hacienda y Administraciones públicas por el cual se encomienda a este último la gestión de inscripción y pago, por vía telemática.

mot.40.-Ley 19/2013
, de transparencia, acceso a la información pública y buen gobierno

En lo que se refiere a entidades sujetas a Derecho Administrativo , incluidas las organizaciones sindicales, la ley se aplicará a determinadas entidades que por su condición de perceptores de fondos públicos (sociedades mercantiles en cuyo capital social la participación pública sea superior al 50%, considerando mínima la cantidad de 5. 000 euros cuando la percepción pública ha supuesto el 40% de sus ingresos anuales) se ven en obligación de publicar aquella información que sea de solicitud de acceso.

En relación a los datos de carácter personal, art. 15, se van a señalar como distinguibles dos tipos de derecho: el denominado 'de acceso' y relacionado con la autoridad pública y aquellos para los que se precisa el consentimiento informado del titular por tratarse de datos 'especialmente protegidos', art.5, y considerándose el medio de la *disociación*[140].

En ningún momento deberá obviarse la función de la labor estadística que vela por la valoración del grado de cumplimiento y calidad de los servicios públicos, art. 8.

140 Agencia de Informática y Comunicaciones de la Comunidad de Madrid, ICM. Unidad de Arquitectura y Soporte de Aplicaciones. "Proceso de disociación de datos personales. LOPD. Versión 2.0.".2011

Por su parte, un *Portal de Transparencia* irá recogiendo , art. 10, conforme se vaya estableciendo reglamentariamente aquella información del Estado cuyo acceso se solicite con mayor frecuencia. En cuanto a los principios técnicos que deben regir su construcción y desarrollo art. 11, deben priorizarse la accesibilidad, la interoperabilidad y el concepto de reutilización.

Su artículo veintiuno es un fiel reflejo del grado de complejidad que deberán alcanzar los Sistemas Informáticos en la Administración Pública al poder incluir ya aquellas Unidades de Información que permitan entre otras tareas: recibir y difundir y dar tramitación a las solicitudes de acceso a la información; realizar los trámites internos para dar acceso a la información solicitada; realizar el seguimiento y control de su tramitación; llevanza del registro de solicitudes; aseguramiento de la disponibilidad en la correspondiente sede electrónica; mantener actualizado el mapa de contenidos de los diferentes tipos de información del Órgano.

Por último, reseñar que existirá una *Comisión de la Transparencia y Buen Gobierno*, art. 36, de la que participa la *Agencia de Protección de Datos* con un representante y cuyas funciones, de percepción análogas nos recuerda a las observadas desde la *CMT* y ella misma, art. 38, y que además de las de formación y sensibilización, elaboración de recomendaciones y de directrices y normas de desarrollo de buenas prácticas en materia de transparencia, evaluará el grado de aplicación de la Ley, informando , en cualquier caso, de los proyectos normativos de carácter estatal que desarrollen esta Ley o que estuvieran relacionados con su objeto.

Constituyendo el grupo de leyes relacionadas con la Sociedad de la Formación y Salvaguardas Técnicas su Disposición adicional segunda precisa con toda claridad
la elaboración de un *Plan de Calidad y Simplificación Normativa* que se encargará de coordinar el proceso de revisión y su simplificación normativa respecto del resto de Departamentos ministeriales coordinando su actividad con los órganos competentes de las Comunidades Autónomas.

Garantizando la información, formación y educación de los consumidores y usuarios, y un régimen de comprobación y servicios de atención al cliente. Las oficinas y servicios de información y atención al cliente que las empresas pongan a disposición del consumidor deberán asegurar que ésta tenga constancia de sus quejas y reclamaciones. Si tales servicios utilizan la atención telefónica o electrónica para llevar a cabo sus funciones deberán garantizar una atención personal directa, más allá de la posibilidad de utilizar complementariamente otros medios a su alcance.

Dirigida a reforzar la seguridad jurídica, tanto de los consumidores como de los usuarios como de los empresarios prevee eliminar disparidades existentes en la legislación europea de los contratos de consumo que crean obstáculos significativos en el mercado interior, y en atención a la Recomendación 2001/310/CE de la Comisión relativa a los principios aplicable a los órganos extrajudiciales de resolución consensual de litigios en materia de consumo o normativa que resulte de aplicación y a la Recomendación 98/257/CE de la Comisión, relativa a los principios aplicables a los órganos extrajudiciales de resolución consensual de litigios en materia de consumo. Pudiendo, en consecuencia la regulación sectorial elevar el nivel de protección conferida por la ley siempre que se respetan las disposiciones de derecho de la Unión Europea.

A través de definiciones concretas como las del consumidor , usuario, empresario,contrato de venta, contrato de servicios, contrato complementario, establecimiento mercantil, servicio financiero, subasta pública, contenido digital, garantía comercial, la ley converge el establecer el derecho de desistimiento en un plazo de catorce días naturales.

Y aunque desarrolla la aplicación del consentimiento del usuario, art. 101, incluso por la consideración de *Códigos Tipo* y *Códigos de Conducta* el derecho incluye la importante excepción de aplicación del Título a los contratos relacionados con la salud, prestados por un profesional sanitario a pacientes para evaluar, mantener o restablecer sus estado de

salud, incluidos la receta, dispensación y provisión de medicamentos y productos sanitarios, con independencia de que dichos servicios se prestaran en instalaciones sanitarias.

En consideración al importante esfuerzo que hace la Ley en relación a los servicios prestados con contenidos digitales, añadimos el anuncio por parte del Ministro de Economía y Competitividad, en fecha de 09 de mayo de 2014 en rueda de prensa posterior al Consejo de Ministros[141] de la novedad de acompañar a cada nueva ley de un informe sobre su Incidencia en el Mercado. Pronosticando la creación de un *Consejo de Unidad de Mercado* a fin de avanzar en el desarrollo y aplicación de la ley.

mot.42.-Ley 15/2014

, de racionalización del sector público y otras medidas de reforma administrativa

Tras la emisión del Informe CORA, Comisión para la Reforma de las Administraciones, con propuestas de medidas que dotaran a la Administración de aquel tamaño, eficiencia y flexibilidad que se extrae demandan los ciudadanos y la economía del país ,y por Real Decreto 479/2013, se crea la Oficina para la reforma de la Administración, como órgano encargado de la ejecución coordinada, seguimiento e impulso de las medidas incluidas en el mismo, con la principal orientación dirigida hacia la Administración electrónica.

Por lo que respecta al Sistema Nacional de Salud, SNS, nos recuerda el real decreto que es el Observatorio de Salud el que deber proporcionar un análisis permanente del SNS en su conjunto y que funcionar en secciones en función de los temas a tratar.

Por su parte, en lo referido al Tribunal de Cuentas y por modificación de la Ley 7/1988, en las Administraciones que no tuvieran establecido *Órgano de Control Externo, OCX,* el Tribunal de Cuentas podrá establecer secciones territoriales del mismo para el cumplimiento de las funciones propias, entre las que se añade proporcionarán informe ante los anteproyectos de ley y los de disposiciones reglamentarias en relación a su

141 MURCIA Jorge. "Las nuevas leyes deberán pasar el test de la unidad de mercado". El Correo. Sábado 10.05.14 , (pag. 49)

régimen jurídico o sobre el ejercicio de sus funciones fiscalizadora o jurisdiccional. En el caso de Anteproyectos de Ley el Gobierno remitir dicho informe a las Cortes Generales.

Como mención especial en relación a la protección de datos y a la aplicación y vigilancia de la transparencia, el art. 30 de la Ley establece que la *Base de Datos Nacional de Subvenciones, BDNS*, funcionar como *Sistema Nacional de Publicidad de Subvenciones*, debiendo los beneficiarios deberán dar publicidad de las subvenciones y ayudas percibidas en los términos y condiciones establecidos en la Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno.

- Transparencia: por modificación de la de Subvenciones, L 38/2003, art. 20, la *BDNS* tiene por finalidades promover la transparencia, servir como instrumento para la planificación de las políticas publicas, mejorar la gestión y colaborar en la lucha contra el fraude de subvenciones y ayudas públicas

  Garantizar el derecho de los ciudadanos a conocer todas las subvenciones convocadas en cada momento y para contribuir a los principios de publicidad y transparencia, la Intervención General de la Administración del Estado publicar en su página web el contenido de las convocatorias de subvenciones

- Protección de datos: la Intervención General de la Administración del Estado es el órgano responsable de la administración y custodia de la *BDNS* y adoptar las medidas necesarias para garantizar la confidencialidad y seguridad de la información. La cesión de datos de carácter personal debe efectuarse a la Intervención General de la Administración del Estado no requerir el consentimiento del afectado. En este ámbito no ser de aplicación lo dispuesto en el apartado del art. 21 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

La información incluida en la BDNS tendrá carácter reservado, sin que pueda ser cedida o comunicada a terceros, salvo que la cesión tenga por objeto la colaboración especificada en la sección Tres del art. 30. En estos casos, la 'cesión de datos' ser realizada preferentemente mediante la utilización de medios electrónicos, debiendo garantizar la identificación de los destinatarios y la adecuada motivación de su acceso.

As mismo, no serán publicadas las subvenciones concedidas cuando la publicación de los datos del beneficiario en razón del objeto de la subvención pueda ser contraria al respeto y salvaguarda del honor, a la intimidad personal o familiar de las personas físicas en virtud de lo establecido en la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y haya sido previsto en su normativa reguladora.

En tal orientación y con la mirada puesta en el ciudadano, corroborando el *Informe CORA* se establece el Tablón edictal único tomando este forma en el *Boletín Oficial del Estado, BOE*, teniendo conocimiento de todos los anuncios que le puedan afectar independientemente de cual sea el órgano que los realiza o la materia sobre la que versen.

Con objetivo dirigido concretamente a la afianzación de los *Soportes* ya existentes en la e-Administración y por modificación de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos se exige que las Administraciones Publicas deberán admitir todos los certificados reconocidos incluidos en la Lista de Confianza de prestadores de servicios de certificación establecidos en España y publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo.

mot.43.-RD 806/2014

, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos

La nueva gobernanza TIC encuentra en los siguientes organismos su representación:

a) la creación de la *Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado*, por *Real Decreto 695/2013* , y que por el presente se adscribe al *Ministerio de Hacienda y Administraciones Públicas*, establecerá un *Catálogo de Servicios Comunes* del que formarán parte los medios y servicios compartidos, entendiéndose por tales todas las actividades, infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos que dan soporte a los sistemas de información, art. 10

b) En la *Comisión de Estrategia TIC*, la <<Estrategia TIC>>, será aprobada por el Gobierno de acuerdo con lo previsto en el *art. 9* de este Real Decreto. Entre sus funciones cuenta con fijar las líneas estratégicas, de acuerdo con la política establecida por el Gobierno en materia de tecnologías de la información y las comunicaciones, la aprobación de la propuesta para su elevación al Consejo de Ministros por los titulares de los departamentos de Hacienda y Administraciones Públicas y de la Presidencia, informar los anteproyectos de ley, los proyectos de disposiciones reglamentarias y otras normas de ámbito general que le sean sometidos por los órganos proponentes, la declaración de los proyectos de 'interés prioritario'[142], en los términos establecidos en el *art. 11*, a propuesta de los ministerios y sus organismos públicos adscritos previo informe de la *Dirección de Tecnologías de la Información y las Comunicaciones,* la elevación anualmente de un Informe al Consejo de Ministros, en el que se recogerá el estado de la transformación digital de la Administración en la Administración General del Estado y sus organismos públicos. La *Comisión de Estrategia TIC* es el órgano colegiado encargado de la definición y supervisión de la aplicación de la Estrategia sobre Tecnologías de la Información y las Comunicaciones de la Administración General del Estado y sus organismos públicos, *art.3*

142 Se considerarán proyectos de interés prioritario aquellos que por sus especiales características sean fundamentales para la mejora de la prestación de servicios al ciudadano.
Artículo 11. *Proyectos de interés prioritario.*
El Comité de Estrategia TIC podrá declarar como proyectos de interés prioritario aquellos que tengan una singular relevancia y, especialmente, aquellos que tengan como objetivo la colaboración y cooperación con las comunidades autónomas y los entes que integran la Administración local y la Unión Europea en materia de Administración digital. La declaración de proyecto de interés prioritario se trasladará como recomendación al Ministerio de Hacienda y Administraciones Públicas y a la Comisión de Políticas de Gasto para que, en su caso, sea tenida en cuenta en la elaboración de los Presupuestos Generales del Estado

c) las *Comisiones Ministeriales de Administración Digital, CMAD*, como órganos colegiados encargados de impulsar la transformación digital de la Administración valorarán las posibles vías de actuación, priorizándolas, y propondrán su desarrollo, todo ello evitando que se generen duplicidades, conforme al principio de racionalización, y promoviendo la compartición de infraestructuras y servicios comunes, art. 7

d) *Unidades TIC* de la Administración General del Estado y sus Organismos Públicos, son en el ámbito departamental responsables del impulso y de la coordinación interna en cada departamento en materia de Administración digital, y serán los órganos de enlace con la Dirección de Tecnologías de la Información y las Comunicaciones. Tienen como función la provisión de servicios en materia de Tecnologías de la Información y Comunicaciones a sí mismas o a otras unidades administrativas, entendiéndose como provisión de servicios TIC la realización de una o varias de las siguientes funciones: Soporte, operación, implementación y/o gestión de sistemas informáticos corporativos o de redes de telecomunicaciones.; Desarrollo de aplicativos informáticos en entornos multiusuario; Consultoría informática; Seguridad de sistemas de información; Atención técnica a usuarios; Innovación en el ámbito de las TIC; Administración digital; Conformar la voluntad de adquisición de bienes o servicios en el ámbito de las tecnologías de la información y las comunicaciones

11.- Elaboración del Documento de Seguridad

En relación a la elaboración del Documento de Seguridad es factible reorganizar las indicaciones proporcionadas desde la propia Agencia de Protección de Datos en relación a algunos conceptos importantes que nos pueden hacer dudar sobre exactamente cómo y en qué sección situar y aplicar las motivaciones[143] que se le presuponen asociados. De este modo, podemos esbozar los apartados ordenados que a continuación se exponen, conforme a los criterios que de forma aproximativa en la

143 *LOPD, (art. 32)* que estudia si existe ámbito alguno de los Código Tipo; *RLOPD , (art.24)* para realizar el informe mensual sobre los registros de accesos; RD 03/2010 teniendo en cuenta los requerimientos mínimos de la Política de Seguridad además del *art.29* acerca de las Guías de Seguridad del CCN y del art.39 en relación al Ciclo de Vida de los Servicios y Sistemas

definición de sus rótulos resultan más propios de la *Ingeniería del Software*, capítulo de que sucede al que nos encontramos y que complementa la perspectiva técnica que esta Tesis precisa:

1.Forma que adopta el Documento

2.Características Técnicas del Registro de Acceso

3.Soportes

4.Indicación de Normas de Etiquetado

5.Procedimientos
{accesos, altas, auditoría interna/externa, contra accesos indebidos, de cifrado, de incidencias(notificaciones, recuperaciones)}

6.Ficheros
{ámbitos definidos desde los Códigos Tipo, indicación de los Niveles de Seguridad, Leyes o regulaciones que le pueden afectar, indicación de los Niveles de Seguridad de Datos del Fichero, Especificación de la Unidad de Atención de los Derechos ARCO, ruta de acceso del archivo, delegaciones de responsabilidades, recuperaciones, indicación de accesos remotos }

7.Informes Periódicos

8.Observación : si el esquema es modificado por aplicación de la ISO/IEC 27002

9.Llevanza del Documento de Seguridad

10.Auditorías

Dichas secciones pueden encontrar convergencias con las medidas adoptadas desde la propia legislación y así mismo ayudarnos en el devenir futuro en el desarrollo y derivación que van encontrándose idénticamente desde la legislación y las normas o estándares.

Cada una de las citadas secciones puede encontrar el siguiente contenido:

11.1.- Documento de Seguridad: su redacción y formato

Conforme al *RD 03/2010* podría auditarse conforme a los marcos organizativo, operacional y de protección.

Ahora bien, si priorizamos el Modelo Organizativo, tal vez estemos concediendo mayor valor a una norma o estándar que a los principios legislativos.

Por ello, se reincide en las conclusiones que se puedan llegar a obtener en el Marco de Privacidad que pretende desarrollar la *Resolución de Madrid*.

Por su parte, la existencia del *Documento de Seguridad* se sostiene sobre la de la Figura del Responsable de Seguridad sugerida por el *art.9 LO 15/1999*. Sin embargo, no es de obligada existencia hasta que aparezca reconocido un Nivel Medio, responsabilizándose entonces de coordinar y controlar las Medidas definidas en el Documento.

Sin embargo, y pese a esta pequeña posibilidad, cada Unidad Pública o Privada conectada su actividad a la e-Administración deberá responder a una auditoría a través de la Supervisión de dicho Documento y que tiene registrados sus movimientos conforme al *art.82* .. *art.88* RLOPD. EL siguiente Nivel de Supervisión lo indica la *Agencia de Protección de Datos*.

Recordar también que al *Documento de Seguridad* se le acompañará de los Informes de Auditorías Anteriores.

Algunas de las consideraciones que pueden condicionar el Formato del Documento de Seguridad pueden ser los siguientes:

1.por aplicación de Niveles , a.8.e

2.por aplicación de Medidas de Seguridad, complejidad o sucesividad

3.documento por cada Fichero

4.documento genérico, adjuntando un documento por cada fichero que requiera de tratamiento

Algo realmente importante, conforme al *art.47* debe de ser el registro de la constancia en el Documento de la imposibilidad de cumplir con las obligaciones establecidas sobre identificación, inventariado y acceso a los soportes dados.

Las incidencias perpetradas serán mantenidas, *art. 35* por doce meses al menos.

11.2.- Políticas de Acceso: registros

Independientemente del tipo de organismo de la e-Administración en el que nos encontremos operando, cabe el serio análisis y aplicación de una *Política de Accesos*, donde además se diferencie precisamente el Nivel dentro del Organigrama que nos encontramos; De este modo, no será lo mismo referirse a un único individuo que accede a un fichero para una empresa subcontratada a terceros en régimen de outsourcing que al mismo *IMI*, cuando se está realizando la auditoría de una determinada alarma[144].

Por tanto, además de la importancia de la Implementación de una buena Política de Accesos, reconociendo la coyuntura contractual y social, podemos distinguir el uso de determinadas tecnologías como el uso de la Biometría.

De este modo, por ejemplo, se aconseja el balanceo del estudio de los cambios de procedimiento de identificaciones, con prioridades orientadas al establecimiento de sus periodicidades del cambio.

Nos resulta un tanto indistinto la distinción de los registros de accesos, pudiendo ser de indistinta aplicabilidad en cualesquiera Nivel de Seguridad:

<<fecha, hora, nombre del fichero, tipo de acceso, autorizado o denegado, registro accedido>>

144 Agencia Española de Seguridad Alimentaria y Nutrición, AESAN http://aesan.msssi.gob.es/AESAN/web/notas_prensa/alerta_pepinos.shtml

Existe la excepción legal de permitir una ausencia de registro de acceso, cuando así consta en el Documento de Seguridad, y tan sólo accede una persona.

La supervisión de los accesos de usuarios autorizados se llevará a cabo por el responsable del fichero con periodicidad semestral.

Los accesos remotos deben ocupar un lugar privilegiado dentro de la Política establecida, es entonces cuando podremos hacer verificaciones del tipo: ¿se ha prohibido al encargado de tratamiento la incorporación de datos a sistemas o soportes distintos de los del responsable? ¿consta dicho registro en el Documento de Seguridad?

No se debe olvidar el inventariado de los dispositivos que verifican los accesos y sus comportamientos.

Para finalizar y participando de la aplicación del *RD 03/2010* se ha de permitir el camino entre el punto de equilibrio entre las comodidades de uso y la protección de la información, que nos recuerda el *art. 4.2* con el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pudiera o no, acceder a un recurso del sistema.

11.3.- Soportes: selección y albergue

Han de constar en los registros de accesos al menos las entradas y salidas de los soportes a los que se le haya concedido un Nivel Alto y/o Medio. Los Bajos, no.

Consecuencia de la aplicación del *art.33* correspondiente al *RD 03/2010*, que afirma que <<la política de firma electrónica y de certificación concretará los procesos de generación, validación y conservación de firma electrónica, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas: el envío de ficheros por e-mail o fax, regulado por el *art. 92* del *RD 03/2010*, debe de ser cuidadosamente estudiado por el responsable del sistema en función a repercutir en el Reglamento de Incidencias, indicándose, en cualquier caso, en el Documento de Seguridad, *art.97*, exigiendo en un Nivel Medio el conocimiento de la información de envío , y en un Nivel Alto, *art.101*, el cifrado de datos.

Los accesos de datos de carácter personal a través de Redes de Telecomunicaciones (públicas o privadas) garantizan:

- mecanismos de cifrado para impedir la manipulación por terceros
- relación de usuarios autorizados a realizarla
- salidas y entradas de soportes correspondientes a ficheros de Nivel Alto y Medio

Se deberán guardar aquellas correos electrónicos que involucren entradas o salidas de datos de ficheros, en directorios protegidos y bajo el control del responsable , al menos, durante dos años.

Deben de ser evitados las 'tierras de nadie' en la interacción con la empresa privada, y, en especial, el *art.42* de la *L 42/2007* conforme al *Esquema Nacional de Seguridad* en su *art.4* tiene en cuenta el siguiente principio:

- seguridad integral
- gestión de riesgos
- prevención, reacción y recuperación
- líneas de defensa
- reevaluación periódica
- función diferenciada

El *art. 5.7.1.* en relación a la Firma Electrónica es un mecanismo de prevención de repudio que previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada.

Resulta realmente importante distinguir el tipo de envoltorio y protección que se le va a proporcionar a la vida de un determinado dato.

Podemos y debemos desarrollar teorías acerca de la manipulación de estos datos, acerca de las *Políticas de Acceso* y de la conservación de los mismos

Debemos distinguir idénticamente que la localización de los servidores de datos deben estar separados físicamente de los servidores de aplicaciones y con diferenciadas normas de protección.

Continuando con la recomendación de la separación de los servidores de Datos respecto del resto de los servicios informáticos, y conforme a la estructura de ubicación definida, debemos continuar reconociendo que los recursos, que, por servir de medio directo indirecto para acceder al fichero, deberán ser controlados por esta normativa.

- los centro de tratamiento y locales donde se encuentran ubicados sus ficheros o se almacenarán los soportes que contengan

- los puestos de trabajo, bien locales remotos desde los que se puede tener acceso al fichero

- los servidores, si los hubiere y el entorno del sistema operativo y de comunicaciones en el que se encuentra el fichero

11.4.- Modelo de Datos: Normas de Etiquetado

El seguimiento correcto de los procedimientos legislativos y aplicación de *Medidas de Seguridad* exige un correcto etiquetado[145] tanto en el Esquema de la Gestión de la Configuración en el Sistema lógico, como en el Manejo de los *Soportes* tanto lógicos como físicos.

145 *ISO/IEC 27799, control 7.2.2*. (pag.34): Identifying and where appropiate protectively assets as confidential can be an important tool in staff training and in policy compliance. This works best when the classification acts as an indicator of required information handling compliance. The classification may also be an important component of data protection agreements among jurisdiction and with third-party organization and their staff. The identification and labelling of information assets is also an essential component of *ISO/IEC 27002*

Otra regla que permite generar 'criterios de etiquetado' con significado para los usuarios autorizados , permitirá no identificar su contenido, dificultando su identificación para el resto de las personas.

En concreto el *art. 4.3.2* del *RD 03/2010* de *Configuración de Seguridad* indica se eliminarán o desactivarán mediante el control de la configuración, aquellas funciones que no sean de su interés, sean o no necesarios e incluso, aquellas que resulten inadecuadas al fin que se persigue.

11.5.- Aseguramiento del Plan de Calidad (hardware, HW y software, SW)

Otra posible forma de afrontar el *Documento de Seguridad* sería haciendo referencia directa a apartados concretos de determinados Procedimientos.

Algunos de estos procedimientos a los que podríamos hacer referencia serían los siguientes:

- para evitar que un usuario pueda acceder a recursos distintos de los autorizados
- para solicitud de altas, modificaciones y bajas de las autorizaciones de datos
- de salida y entrada de soportes
- de medidas conducentes a evitar la sustracción, pérdida o acceso indebido
- de cifrado de datos
- de tratamientos de normas y circulares
- de copias de respaldo y recuperación
- de notificación de incidencias

- de auditorías externas e internas

11.6.- Unidades Lógicas: Ficheros

Por Fichero, podemos encontrar dos definiciones: la del contenedor digital en la que se presentan la información al usuario y aquellos archivos formateados en lenguajes de metadatos por ser parte integrante de una Base de Datos. En ambos casos hay que aplicar Medidas de Seguridad, aun cuando es en el segundo caso donde se deben aplicar masivamente, previa interacción, verificación, validación a exponer al usuario.

Es en este segundo caso cuando conforme al a. 5.4.3 del *RD 03/2010* acerca de la *Protección de la Confidencialidad*, se indica que se considerará ataque activo:

a) la alteración de la información en tránsito

b) la inyección de la información espúrea

c) el secuestro de la sesión por una tercer parte

A continuación y profundizando en la gravedad de sus tratamientos debemos recordar que una incidencia es 'cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad del fichero, extendido bajo sus vertientes de confidencialidad, integridad y disponibilidad de los datos'.

Respecto del primer tipo de fichero el conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerando como una falta contra la seguridad del fichero por parte de ese usuario

En relación a las Funciones y Obligaciones del Personal, se cuenta con dos figuras manteniendo la visión expuesta:

- la del administrador del sistema, que mantiene el entorno operativo del sistema

- los usuarios propios del fichero, que se define como aquella persona que utiliza el sistema informático del fichero

Además del personal citado existirá un responsable de la Seguridad del Fichero cuyas funciones serán las de coordinar y controlar el Documento de Seguridad, sin que suponga esto una delegación de responsabilidad respecto del responsable del fichero, según nos recuerda el *RD 1720/2007*.

Conforme al reglamento que sustituye RD 1720/2007 , aun cuando existieran varios responsables de ficheros, no se exime de responsabilidad al encargado del tratamiento , *art.20, 22, 43, 84, 95 y 127.*
En relación directa con la existencia de un fichero, e independientemente de su naturaleza y en el *Documento de Seguridad*, se debe:

- indicar aquellas Leyes o Regulaciones que afecten al Fichero

- incluir la especificación de tipos de datos del fichero, diferenciado sus Medidas de Seguridad de aplicar

- indicación de relaciones con otros ficheros, en función de un mismo responsable

- especificación directa del tipo de información que debe mostrarse sobre cada tipo de fichero, indicando la ruta completa de acceso al archivo

El *RLOPD* coincide en señalar que los ficheros de tratamiento con datos de 'salud' exigen una aplicación de Nivel Alto, y aquellos relativos a la Comisión de infracciones administrativas o penales a un Nivel Medio, idéntica calificación para los datos de Mutuas, y de Entidades Gestoras y de Servicios comunes y los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización:

- recordar que existe, una aplicabilidad de Nivel Básico en los ficheros de tratamientos que contengan datos de salud, que se refieran exclusivamente al

grado o condición de discapacidad o la simple declaración de invalidez. Y que en ellos se debe facilitar la consulta y localización para garantizar el ejercicio de sus *Derechos ARCO*

•recordar que en un tratamiento de Nivel Alto se debe de realizar una revisión mensual del registro por el responsable de seguridad debiendo conservarse cada dos años, y no siendo necesario el registro de acceso si el responsable del fichero es una persona física y es el único usuario

11.7.- Periodicidades: Informes

El responsable de seguridad revisará al mes la información de control registrada, y elaborará un informe que ayudará con posterioridad a la auditoría de seguridad.

Conforme al *art. 103 RLOPD* en el Informe Mensual se deben de adjuntar los consiguientes procedimientos y la relación de medidas seleccionadas se formalizará en un documento denominado *Declaración de Aplicabilidad*, firmado por el responsable de Seguridad del Sistema.

Al explicitar el período de conservación , que debe ser de al menos de dos años, deberá de indicarse:

•por el *art. 4.3.8.* RD 03/2010 de registro de actividad de los usuarios, aquellas actividades realizadas con éxito y sus intentos fracasados. Por otra parte, la determinación de qué actividades debe registrarse y con qué niveles de detalle se determinará a la vista del análisis de riesgos realizadas sobre el sistema

•por el *art.4.3.9 RD 03/2010* se registrará aquella evidencia que pueda posteriormente sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a acciones disciplinarias sobre el personal interno, sobre proveedores externos a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento ilegal especializado

11.8.- Estándares: semántica aplicada

Si se aplica este esquema no se deberá obviar bajo ningún concepto la aplicabilidad de la semántica y conceptos manejados desde los Órganos de Supervisión de cada país, que en este caso resulta la *RD 03/2010*, aun cuando esta regulación pudiera haber estado influida en su publicación desde los Ministerios como premisa inicial y especialmente en las que se citan a continuación:

- Por el *art.37* la prestación de servicios de respuesta en incidentes de seguridad a las administraciones públicas

- El CCN-CERT a través de su servicio de apoyo técnico y de coordinación actuará con la misma celeridad ante cualquier agresión recibida de los sistemas de información de las administraciones públicas

- La valoración del impacto de un incidente con perjuicio a las *Dimensiones de Seguridad* deberá observarse como consecuencia de la determinación de la Categoría

- A su vez la determinación de una categoría resulta de la valoración de la importancia de la información que maneja un sistema, los servicios que este presta y el esfuerzo de seguridad requerido (objetivos, activos, obligaciones, req. legales)

- de la lectura de los niveles (y por comparación) se aprecian los siguientes apartados:

    - capacidad de la organización

    - sufrimiento de un activo (subsanable, no subsanable, irrecuperable)

    - incumplimiento de alguna ley o regulación

    - perjuicio algún individuo (fácil, difícil, imposible recuperación)

    - prescribe con que exista al menos una dimensión perteneciente a una categoría

11.9.- Tratamiento de Datos: responsabilidades de supervisión

Su definición nos indica la,

- Especificación concreta de las personas que pueden o no proponerlos y aprobarlos, así como de las comunicaciones al personal que pueden verse afectados

- En el contrato celebrado al amparo del *art.12 LOPD* con especificación de los ficheros trasladados, el *art.88* se refiere a la delegación del la llevanza del documento de seguridad. Sin embargo, no podrá delegarse en el encargado dicha llevanza en lo relativo a aquellos datos contenidos en recursos propios del responsable

- El objetivo fundamental de implementar las Medidas de Seguridad a las que se refiere el *art.9* LOPD y su reglamento de desarrollo es garantizar que los datos personales se tratan con las adecuadas garantías que permitan asegurar la confidencialidad, la integridad y la disponibilidad de los datos

Debería poder permitir responder al tipo de información a incluir en el tipo de registro de incidencias: *art.90* al *art.100* del Reglamento.

11.10.- Auditorías

Conforme al *art.34.3* y en el marco de los dispuesto por el *art.39* de la *L 11/2007*, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante dentro del alcance por la auditoría.

Conforme al *RD 03/2010* y como consecuencia del análisis de las incidencias se revisará la determinación de los eventos auditables. Por su parte, el *RLOPD* le dedica el Título VIII, *art.96* y

art.110.

El procedimiento ya citado debe considerar la auditoría , al menos, cada dos años no cuando se considere modificación aceptable. Su resultado debe ser siempre un informe en relación a la adecuación de la ley y desarrollo complementario, imponiendo deficiencias y proponiendo medidas correctivas necesarias.

El Informe debe ser emitido por el responsable de seguridad que a su vez deberá ser entregado al responsable del fichero y mediante esta figura quedará a disposición de la *Agencia de Control* de la Comunidad Autonómica.

La auditoría se realizará siempre en relación al plano previsto desde la anterior y , a su vez, revisará la determinación de los eventos auditables.

CAPITULO IV: SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Abstract :

Upon various phases and samples of SE, Software Engineering implementations, we shall develop a scheme for a possible solution for an e-Administration in Law at Informatics with consideration through a legal auditory. The chapter includes also a way, a discussion in the meantime , of a worldwide 'Patient Summary'.

Claves :

Documento de Seguridad, llevanza del documento de seguridad, declaración de prácticas de certificación, configuración de seguridad, requisito informado, ENS, SNS, código tipo, reglamento de incidencias, requisito legal, agente legislativo, safety at work or seguridad en el trabajo, legal compliance, salvaguarda legal, indice del documento de seguridad, BCR, taxonomía, perfil de protección, tarjeta profesional, trazabilidad, CC or Common Criteria

Se trata de integrar el instrumento legal que se corresponde con el *Documento de Seguridad*[146] en el

146 Se encuentran consideraciones especiales a dicha denominación en los sgtes. ptos. significativos:

- tb. *Llevanza del Documento de Seguridad*: *LOPD, (a.12)*
- *RD 1720/2007, (art. 81, 82, 84, 86 y Título VIII Cap. II y Cap. III por Niveles de Seguridad)*
- La existencia de datos de carácter personal requiere de un *documento de seguridad* y la designación de una serie de responsables. Parece natural que estos requisitos se contemplen en la *Política de Seguridad* requerida por el *Esquema Nacional de Seguridad, ENS*: L 42/2007 , (*art.42*)
- En el *legal outsourcing* el tradicional *customer agreement* es sustituido por el *Documento de Seguridad*
- *Ley 59/2003, de 19 de diciembre , de firma electrónica* : El documento electrónico es soporte tanto de documentos públicos como privados. En concreto, el *art. 3.8* nos recuerda que dicho soporte será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del art. 326 de la *Ley de Enjuiciamiento Civil*. En relación con el *Documento de Seguridad* y las consiguientes *Medidas de Seguridad* propuestas:
  - *art. 18*, el 'mantenimiento de un Directorio' actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida
  - *art. 19*, la 'Declaración de Prácticas de Certificación', donde cada prestador de servicios formulará una declaración de prácticas de certificación en la que se detallarán las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia

Sistema de Gestión de Seguridad de la Información, o *SGSI*, siendo este último, recordemos objeto único de análisis diseño, desarrollo y mantenimiento en las normas ISO/IEC 27001-02.

El RD 03/2010 define el *Sistema de Gestión de la Seguridad de la Información* como aquel Sistema de Gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El Sistema de Gestión incluye la infraestructura organizativa, las Políticas, las responsabilidades, las prácticas, los Procedimientos, los Procesos y los recursos. El objetivo fundamental del *Esquema Nacional de Seguridad, ENS*, es el el establecimiento de los principios y requisitos de una *Política de Seguridad* en la utilización de medios electrónicos que permita la adecuada protección de la información que determina el Alcance y Procedimiento para establecer dicha seguridad , se complementa con una regulación que no agota todas las vías de normación, y debiendo entre las decisiones básicas que adoptar la de Seguridad Integral y de Gestión de Riesgos. Aseverando en su Anexo II el Real Decreto que se empleará alguna metodología reconocida internacionalmente.

Este mismo Anexo en su apartado 3 denominado 'Marco Organizativo' por lo que se refiere a la *Política de Seguridad* esta debe de referenciar y ser coherente en lo establecido con el *Documento de Seguridad* en lo que corresponde al marco legal y regulatorio en el que se desarrollarán sus actividades.

El Anexo III correspondiente al RD 03/2010 especifica que la Seguridad de los Sistemas de Información será auditada en los términos apuntados en su apartado f) , cunado existe un *Sistema de Gestión de la Seguridad de la Información* documentado y con un proceso regular de aprobación por la Dirección.

---

de los certificados , las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados.

- *art.27*, en los procedimientos de certificación se utilizarán las normas técnicas cuyos 'Números de Referencia' hayan sido publicado en el <<Diario Oficial de la Unión Europea>> y excepcionalmente por las aprobadas por el Ministerio de Ciencia y Tecnología que se publicaran en la dirección de Internet de este Ministerio.

- *RD 03/2010* : *art. 4.3.2* de 'Configuración de Seguridad' indica se eliminarán o desactivarán mediante el control de la no configuración, aquellas funciones que no sean de su interés, no sean necesarios e incluso, aquellas que en inadecuadas al fin que se persigue. Especial consideración a los soportes utilizados separando explícitamente el uso de los siguientes medios: el envío de ficheros por e-mail o fax, regulado por el art. 92 , debe de ser cuidadosamente estudiado por el responsable del sistema en función a repercutir en el *Reglamento de Incidencias*, indicándose, en cualquier caso, en el *Documento de Seguridad*, art.97, exigiendo en un Nivel Medio el conocimiento de la información de envío , y en un Nivel Alto, art.101, el cifrado de datos.

Si en los Capítulos precedentes de la Tesis versada en Protección de Datos en la Historia Clínica centrábamos la Regulación de la Informática respetando el ámbito Usuario-Técnico Manipulador de sus Datos, y resaltando mayormente la Operativa del Técnico Informático en cuanto a la Salvaguarda Técnica de la existencia del Dato Médico, en el presente Capítulo vamos a apuntar a aquellas integraciones que se hayan podido derivar del aspecto de cada Capítulo precedente en consonancia con lo que se apuntará al final de la Introducción, esto es , la Mejora del *SGSI, Sistema de Gestión de Seguridad de la Información o ISMS, Information Security Management System,* correspondientes a las clausula nº 4 de la norma ISO/IEC 27*001,* esquema que desarrolla la norma ISO/IEC 27002.

De esta forma habremos logrado el siguiente equilibrio en nuestra observación:

1. dato médico – salvaguarda técnica en materia de protección de datos
2. nivel de observación del derecho informático – aplicación software

De esta forma, y sin limitación desde el punto de vista de la *Ingeniería del Software*[147] nos podemos mover y presentar cualesquiera de sus modelados para poder afrontar cuestiones derivadas del tema que nos ocupa y conseguir hacer resaltar que la enseñanza de la Informática precisa no sólo del respaldo como Asignatura de la *Ingeniería del Software*, sino además de la del Derecho asociado a la Informática, se llame como se le llame. De forma que la consiguiente extensión a otras Formaciones Regladas que incluyan en su labor la manipulación de datos de carácter personal, en este caso datos clínicos, no resulta en ningún caso redundante aun cuando imitándolas a su específico ámbito y a Regulaciones más concretas.

Eso sí, conforme al art. 39 RD 03/2010, las especificaciones de seguridad se incluirán en el Ciclo de Vida de los Servicios y Sistemas, acompañados de los correspondientes procedimientos de control, estableciéndose estos por cada Órgano de la Administración Pública, y pudiendo distinguir su aplicabilidad incluso desde los Ayuntamientos , eso sí, supervisados por una Diputación, Cabildo , Consejo Insular, art. 6.

147 John Tukey coined the term in 1958
NATO conference held in Germany in 1968, Software Engineering:
IEEE Computer Society Professional Practices Committee SWEBOK, Guide to the Software Engineering , Body of Kowledge. 2004(pag. 8): <<every profession is based on an body of kowledge and recommended practices, although they are not always defined in a precise manner. In many cases, these are formaly documented, usually in a form that permits them to be used for such purposes as accreditation of academic programs, development of education and training programs, certification of specialists, or professional licensing>>

La base legal de no incurrir en dobles propósitos definitorios es el fundamento principal que presenta la especificación del *Requisito Informado* dentro de la Comisión del Mercado de las Telecomunicaciones cuando ésta se enfrenta a la recopilación de operativas administrativas, siendo su actualización obligada en el período de dos años y exigiéndose un alto conocimiento técnico, económico y jurídico en el momento de su exposición. En el ámbito sanitario es el *Sistema Nacional de Salud* o *SNS* el que va a delimitar el procedimiento, concretando su interfaz.

Por otra parte, nunca está de más apuntar y recordar que los Requerimientos de la Unidad del Sistema Informático Médico pueden ser recopilados en mayor o menor medida en las Operativas del personal de Recursos Humanos, RRHH, y concretamente matizados en los *Códigos Tipos* que están obligados por ley a registrar en el Registro de la Autoridad Competente en materia de Protección de Datos, CA, o *Agencia de Protección de Datos.*

El usuario[148] debe prestar especial cuidado y estar formado en su *Seguridad como Paciente* en dos vertientes:

a) en cuanto al uso y recepción de la semántica[149] en la interacción con los asistentes sanitarios por cuanto: se la va a considerar la determinante del nivel de protección de sus propios datos sensibles generados en relación a su consentimiento consciente e informado

b) en la práctica de su derecho de autodeterminación o de amparo, rectificación y cancelación de datos sensibles clínicos, también reconocidos como *Derechos ARCO*

Si recuperamos la visión que sí poseen las autoridades competentes en materia de protección de datos en cuanto al poso que va ejerciendo la 'influencia invisible' de la ejecución continuada de una determinada aplicación informática en el Seno de una Sociedad, podemos apuntar en tal medida el ejemplo de los *Sistemas de Información Inter-países Europeos* , donde cobra especial importancia la vigilancia y monitorización del control de entrada en las instalaciones, soporte de datos, introducción, utilización, acceso, transmisión y su transporte[150] que de por sí son la base de la elaboración del *Documento de Seguridad* propuesto bien desde la perspectiva del Consumidor-

148 TAMAYO VIVANCO Miren. "Responsabilidad Taxonómica en la Historia Clínica". Revista de Derecho , RDUNED, Num. 11, 2012

149 TAMAYO VIVANCO Miren. "La Semántica en el derecho de la Informática en la Historia Clínica". Diario LA LEY. Año XXXIV. Num. 8011. Martes, 29 de enero de 2013. Disponible en: http:\\www.diariolaley.es

150 *RD 1332/1994,* (art. 118) SIS II. tb. Salvaguardadas

Paciente[151] como desde la perspectiva del Procesador-Técnico[152] promovida desde la propia Comisión.

La tradicional comprobación de daños ante una reclamación de perjuicios si el daño resultaba efectivo y comprobable y amparado desde el *Código Civil*[153], característica de las aplicaciones del ámbito privado amplia su horizonte en cuanto a definición de posibilidades desde el inicio de la aplicación del Procedimiento Administrativo en la Administración Electrónica.

En el ámbito Europeo la ratificación del instrumento, aceptación , aprobación y aprobación del *Convenio 108, art.3.2b*:

> *<<también el presente convenio a informaciones relativas a agrupaciones , asociaciones, fundamentos, corporaciones y cualquier otro organismo formado directa o indirectamente por personas físicas, tuvieren o no personalidad jurídica"*[154]*>>*

, deberá permitir la suficiente cohesión y homogenización de comportamientos, no solo de los responsables en materia de protección de datos , sino de las presiones a las que estos pudieran verse sometidos desde el Gobierno de sus respectivos países.

Solo con estas premisas se deduce que nuevas formulas se derivarán de la convergencia de los diferentes frameworks de aplicación del *Ppo. de Transparencia*[155] .

Será entonces cuando se reconsiderarán los actuales *Niveles de Seguridad*[156] y elevará el tratamiento de *Incidencia*[157].

Si además de intentar no menospreciar las buenas practicas que se han venido produciendo en la Informática previa a su reconducción vía el denominado *Documento de Seguridad* y de constatar que existen claros ejemplos de fácil seguimiento, podemos además añadir sobre la tradicional

151 ARTICLE 29 DATA PROTECTION WORKING PARTY *WP 153, WP 154*
152 ARTICLE 29 DATA PROTECTION WORKING PARTY *WP 195*
153 Ley de Enjuiciamiento Civil, (art. 1902)
154 Superación de la aceptación de persona jurídica en *D 95/46/CE* en la *D 2006/24/CE*
155 Resolucion de Madrid. Principio de Transparencia
vid. PIÑAR MAÑAS, Jose Luis (director) y autores varios. "Transparencia, acceso a la Informaciín y Protección de Datos". REUS. 2015
156 Métrica Magerit de la Administración Pública Española; *ISO/IEC ISO 27002*; *RD 03/2010*
157 *RD 1720/2007*,(art. 90, 100 y 105); *RD 03/2010*, Anexo 2.4

incorporación de modificaciones en una aplicación software la distinción de lo que puede suponer este nuevo requisito software o *requerimiento informado* , más propiamente, cuando se trata de uno legal[158] como es el que se expone a continuación:

Enumeración de Requisito, nº 1	Agresiones del Asistente e-Sanidad. Grupo 3	
Agentes Legislativos	L 14/1986	*General de Sanidad*, como deber individual de cada ciudadano, el mantener el debido respeto a las normas establecidas en cada centro, así como el personal que preste servicios en los mismos.
	L 31/1995	*De Prevención de Riesgos Laborales*, art. 14, los trabajadores tienen derecho a una protección eficaz en materia de seguridad y salud en el trabajo. El citado derecho supone la existencia de un correlativo deber del empresario de protección de los trabajadores frente a los riesgos laborales. Este deber de protección constituye igualmente su deber de las administraciones públicas respecto del personal a su servicio
	LOPS	*Ley de Ordenación de las Profesiones Sanitarias*, art. 5, una vez que se ha producido la situación de violencia, el médico, desde el punto de vista legal y deontológico, está legitimado para romper la relación médico-paciente, salvo caso de urgencia vital del agresor al haberse quebrado la necesaria confianza del paciente en su asistencia
	L 55/2003	art. 17.h del *Estatuto Marco del Personal Estatutario de los Servicios de Salud*, en el que se dispone que el citado personal ostenta el derecho a recibir asistencia y protección de las Administraciones Públicas y Servicios de Salud en el ejercicio de su profesión o en el desempeño de sus funciones
Operativa	Registro de incidentes y agresiones: La unidad básica de prevención de riesgos laborales cumplimentará la hoja de registros de agresiones en su propia base de datos y remitirá una copia vía fax o por correo electrónico a la Secretaría General Técnica. De forma anual cada unidad básica de prevención analizará los índices estadísticos correspondientes a los datos de incidentes y/o agresiones de su ámbito de referencia. Así mismo, la Unidad Central de Prevención realizará una *Memoria Anula* de violencia en el trabajo de los casos ocurridos, y de las medidas adoptadas . Todos los casos se registrarán en la base de datos de agresiones a tal fin.	
Requisito Gráfico-GUI	Cesión de Actividad Médica sobre Paciente (es un checkbox)	

Tabla 5. Entrada-Especificación Requisito Legal

158 Se encuentra un ejemplo clarificador en la incorporación de este tipo de requisito legal en la *Ley de Consumo L 03/2014*, art. 98. denominado *Requisitos Formales de los Contratos a Distancia*: (apartado 2) << El empresario deberá velar por que el consumidor y usuario, al efectuar el pedido, confirme expresamente que es consciente de que éste implica una obligación de pago. Si la realización de un pedido se hace activando un botón o una función similar, el botón o la función similar deberán etiquetarse, de manera que sea fácilmente legible, únicamente con la expresión «pedido con obligación de pago» o una formulación análoga no ambigua que indique que la realización del pedido implica la obligación de pagar al empresario. En caso contrario, el consumidor y usuario no quedará obligado por el contrato o pedido. >>

Aun no resultando impositiva la certificación de la norma ISO/IEC 27799 que extiende el tratamiento de la *ISO/IEC 27001* e *ISO/IEC 27002* en el ámbito sanitario, de facto se permite la certificación de la *ISO/IEC 27001* sin la certificación de la *ISO/IEC 27799*.

Como veremos en un apartado más adelante podemos plantear desde algunos de los Controles de la *ISO/IEC 27799*, y al igual que hiciéramos con los Controles de la *ISO/IEC 27001* las mismas reivindicaciones, no sin recordarnos en su apartado 1.2 que los siguientes puntos se encuentran fuera del ámbito del estándar *ISO/IEC 27799*:

c) la calidad del servicio de la red y aquellos métodos que permiten valorar su viabilidad
d) la calidad de los datos, y distinguiéndolo de la integridad de los datos

Por otra parte, sí que establece claramente la protección del siguiente tipo de información preservando , al menos, los parámetros parametrizables en las *Dimensiones de la Seguridad* en cuanto se refiere a la confidencialidad, integridad y disponibilidad: datos de auditoría o en relación a acciones del usuario.

Concluir añadiendo que las Modificaciones en relación a la *legal compliance* se matiza en el *control 7.2.3* que debe incluir:

d) los últimos controles incorporados por las regulaciones estatales y jurisprudenciales

e) las últimas recomendaciones venidas de asociaciones profesionales y comisionados en materia de privacidad y datos de carácter personal

f) el resultado de casos legales y que establecen precedentes y mejores prácticas

g) aquellas percepciones derivadas de la Operativa de la propia plantilla laboral, investigadores, etc,..

Por último, añadir que tan sólo se han detectado de una manera expuesta la duración del

mantenimiento de una determinada salvaguarda o medida técnica de seguridad en la aplicación de la Seguridad en la Protección de Menores en las Bibliotecas Públicas estadounidenses, tal y como expone la *SEC. 1703* de la *CIPA* americana, reforzando su carácter económico en su *SEC 3601*, *limitation on availability of certain funds for schools, A.ii)* citando textualmente:

<<is enforcing the operation of such technology protection measure during any use of such computers by minors>>

1.- La clausula 4 de la norma ISO/IEC 27001

Retomando el Argumento anterior de que la trayectoria de nuestro Sistema Informático cuenta con suficiente Documentación aunque fuera migrable la terminología semántica y las unidades de Inventario, y de qué modo se introduce y aplica un *Documento de Seguridad*, e independientemente de la Faceta Médica de los Fichero que protege, se procede a recopilar Capítulo a Capítulo aquellas partes directamente implicadas con el Diseño de un *SGSI*, debiendo indicar cómo se aplica , en cualquier caso, el Ciclo P(Plan).D(Do).C(Check).Act(A) para cada parte integrable.

Recordemos el esquema de la Clausula:

4 SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION
4.1 Requisitos Generales
4.2 Creación y Gestión del SGSI
    4.2.1 Creación del SGSI
    4.2.2 Implementación y Operación del SGSI
    4.2.3 Supervisión y revisión del SGSI
    4.2.4 Mantenimiento y mejora del SGSI
4.3 Requisitos de la Documentación
    4.3.1 Generalidades
    4.3.2 Control de Documentos
    4.3.3 Control de Registros

Como nos recuerda la clausula nº 4.2.2, a su vez, podemos implementar los controles seleccionados para cumplir un determinado objetivo de control. Esto es lo que se hace al proponer lo que, más

adelante, se define como 'Perfil de Protección del Ingeniero de Software' .

A continuación, se recopilan las aportaciones individuales que se producen en cada Capítulo de la Tesis y que pueden contribuir a la Mejora y/o Diseño de nuestro SGSI:

- Capítulo I:

  -Especificación de Taxonomías que definen los derechos y deberes de cada Grupo: Ciudadano y Técnico de la e-Administración en el Área Sanitaria

- Capítulo II:

  -Especificación de Actores y Desglose de las Delegaciones de Responsabilidades en el Tratamiento de Datos Clínicos

  -Delineación de Solución Orientada a la Protección de Datos formulada desde la Agencia de Protección de Datos, o EIDP, Cap.II. Apartado 5

  -Concreción de las Líneas de Implementación de mayor *Riesgo* detectadas:

    a) Intercambios de Información, clausula nº 10.8.2

    b) Seguridad en el Soporte y Procesos de Desarrollo, clausulas nº 12.5.1, 12.5.5

- Capítulo III:

  -Recopilación de *Activos Legales*

  -Recopilación de *Motivadores de la Gestión del Cambio* practicado sobre un *Documento de Seguridad* y grabables como Asiento[159] en un *Registro*

159 RD 04/2010. Disposición Adicional Primera. Desarrollo del Esquema Nacional de Interoperabilidad.

-Extracción de unos I*ndices del Documento de Seguridad* que nos permitan afrontar un determinado Nivel de Solución Informática para nuestro SGSI

- Capítulo IV:

-Integración de la perspectiva del SGSI

-Trabajo Documental sobre las Líneas de Implementación de mayor *Riesgo* detectadas, considerando el Albergue de Datos desde las siguientes perspectivas:

a) Plan de Aseguramiento de la Calidad: punto de vista local(según Indices de Documentos de Seguridad)

b) Marco Organizacional: punto de vista supranacional(Documento de Trabajo WP 195 Gt29 D 05/46/CE)

- Especificación en Lenguaje de Auditoría de un Mini-Control que equipara las Seguridades observadas en cada Taxonomía

ISO 27 002 nos comunica que la Organismos localizan, al menos, tres orígenes a la hora de determinar requisitos de seguridad:

a) los derivados de términos contractuales y legales que impone cada área en la que opera

b) los propios riesgos que la organización hace frente

c) el conjunto de principios, objetivos y reglas de negocio que se precisan en el apoyo de operaciones y procesos

Por su parte, los *Planes de Gestión de Riesgos* aglutinan cuatro objetivos vinculados en relación a los riesgos que toda Empresa afronta, y que son:

a) su completa eliminación y superación

b) su reducción a niveles aceptables, puesto que no pueden ser eliminados completamente

c) la convivencia con ellos, estableciendo controles

d) su trasferencia o el establecimiento de un seguro con otra Empresa

Además, deberíamos identificar las amenazas asociadas a los activos, sus vulnerabilidades y los impactos, así como la determinación del grado de riesgo al que se expone ayudándonos para futuros resultados de modo que se puedan realizar y aplicar técnicas estadísticas.

Si dedujéramos que nuestra organización no cuenta con un factor recurso humano dedicado a la Función de *Gestión de Riesgos*, podemos proponer que la solución técnica propuesta va a llevar asociada una nueva Salida en el *Marco de la Excelencia*: se permitirá un feedback entre las Unidades de Auditoría y Calidad mediante el establecimiento de una Medida de Control o Salvaguarda que a su vez hará evidente la *Unidad de Gestión de Riesgos*. Mediante la *clausula 4, ISO 27 002* introduce la *Gestión de Riesgo*s, que debe de tratarse como un proceso formal en relación a unos datos de entrada, su análisis y unos resultados donde todos ellos deberán ser guardados.

Se nos presentan dos temas a considerar:

a) el estándar requiere de periódicas revisiones de los riesgos y controles asociados tomando nota de las amenazas y vulnerabilidades

b) el impacto que los cambios pueden tener en el negocio, sus metas o procesos, tecnología y entorno más inmediato, o bien Regulaciones y Sociedad, exclusivamente para confirmar que los controles activos son tanto apropiados como efectivos

Se recomienda que cada aproximación a la *Gestión de Riesgos* se implemente con la misma herramienta que el Organismo prevea usará en un futuro. Esta aproximación dirige su mirada a dos elementos a tal fin: la probabilidad con que un evento ocurrirá´y la posible pérdida que se producirá. Es posible incluso establecer rangos de eventos que determinen el grado de probabilidad en que suceda un riesgo y generar decisiones en base a ello.

Sin embargo, la aproximación[160] cualitativa es, con mucho, la más extendida de las aproximaciones en el *Análisis de Riesgos* es la que espera la clausula 4.2.1.d o de identificación de riesgos del estándar. No se requiere de la probabilidad numérica, salvo cuando una potencial pérdida sea percibida. La mayoría de este tipo de metodologías utilizan un número de elementos que interrelacionan entre sí se manejan mejor desde diagramas en relación a un activo corporativo y un Log de Riesgos de manera que para cada activo, son identificados su dueño, su amenaza, vulnerabilidades e impacto, teniendo en consideración los siguientes principios:

- 4.2.1.d.1, *activos del objetivo*

  el primer paso es identificar los activos y estos incluyen los Sistemas de Información, referido exactamente a su definición y su relación con la Política de Seguridad

- 4.2.1.d.2, *amenazas*

  normalmente, si no se puede asociar una amenaza a un activo, se puede decir que no se trata realmente de un activo, *asset*

- 4.2.1.d.3 *vulnerabilidades*

  permiten tener mayor o menor impacto a un ataque. De hecho, en el lenguaje del estándar, una vulnerabilidad puede ser explotado por una amenaza

- 4.2.1.d. 4 *impactos*

  la disponibilidad, confidencialidad e integridad de un activo presenta un determinado impacto en la medida que la amenaza con la que se relaciona ha permitido la explotación de la vulnerabilidad. Es en este punto, donde el impacto se le exige no sólo ser identificado siempre que sea posible sino perseguir obtener un valor monetario sobre el coste del atributo que estuviera siendo comprometido (e.g. un puesto de trabajo por otro)

- 4.2.1.e *risk assesment*

  se debe de habilitar la identificación de los Niveles de Riesgos, de manera que podamos concluir para cada riesgo si es aceptable o requiere cierto grado de control

- 4.2.1.f *controles*

160 CALDER Alan, WATKINGS Steve. "IT GOVERNANCE. A Manager's Guide to Data Security and ISO 27 001 / ISO 27 002" . Capítulo 6. 2009.

los controles son las medidas de salvaguardas que se adoptan frente a los riesgos

El control que desarrollamos a continuación se ajusta a lo que el *CBK, "Common Body of Knowledge"* denomina *Recovery Controls (* which are often associated with business continuity and disaster recovery).

En relación a la resolución del riesgo se aconseja lo siguiente: conseguir información acerca del riesgo, si no conoce el auténtico peligro del riesgo, averiguarlo. Por ejemplo, desarrolle un Prototipo para comprobar la viabilidad de su alternativa de diseño. Además, si puede, elimine el origen del riesgo: si el diseño de una parte del sistema es demasiado arriesgado, cambiar la parte del sistema a un proyecto de investigación , y en nuestro caso de Control PDCA se supervisará desde la Gestión de Proyectos y desde el Marco de la Excelencia, como se narra.

1.1.- Plan de Aseguramiento de la Calidad: Indicadores del Documento de Seguridad

Partiendo de la relación de Agentes Legales , podemos concluir que mayoritariamente se está haciendo alusión directa o indirectamente a la *Base de Datos* en cuanto Albergue de Datos[161], y en relación directa a las siguientes claves ordenadas alfabéticamente:

161 Por la parte del Derecho:
- Dos posibles tratamientos: en cuanto a definición: 1) como recopilación de datos recogidos de forma sistemática y accesible de forma electrónica conforme al *D 96/9/CEE, (art. 10)* y *RDL 1/1996 , LPI (art. 136)*: como colecciones de datos que por su selección o disposición constituyen creaciones intelectuales
- la reutilización de su contenido por : contrato de cesión o transferencia de derecho, segun nos recuerda la *L 5/1998* en consonancia con el *D, (art. 7.3)* y de *LPI (art. 133.1.2)*
- la Directiva protege la remuneración del fabricante sin perjuicio de la legislación en materia de protección de datos, conforme al art. 7 *L* conocido como 'dcho sui generis', explicitando que su extracción y reutilización en el prestamo público no constituye un acto de tales ejecucciones. A este respecto existe una invocación directa al *Convenio de Berna*, (art. 6.3) en relación a la extracción pública o reutilización , (art-7.3)
- los contratos suelen practicarse de adhesión , incluyendo una posterior utilización de la mano *LPI (art. 95.104)*
- distribucción y reproduccción, *LPI (art. 1.3.3, art 192)*
- sanciones y procedimientos , cap.I, Libro III *LPI*
- existe una alusión directa en la Ley de la palabra 'compilación' coincidiendo con el tratamiento estadounidense desde su *Copyright Act*
- no se debe confundir con la protección específica de programas de ordenador, *D 91/250/CE*E
- los Estados pueden establecer límites a ciertos derechos: a) reproducción de BBDD con fines privados, no mercantiles b) con fines de docencia o investigación científica c) con fines de seguridad pública
- relación con terceros países: *LPI(art. 11.3), D (art. 10)*
- BBDD en línea considerado en el marco de prestación de servicios
- recordar su consideración en cuanto a *Soporte*
- conforme a la *ISO 27 001*, en el legal outsourcing el tradicional 'customer agreement' es sustituido por el *Documento de Seguridad*

[***accesos***], *[alquiler y préstamo de bases de datos], [asiento electrónico], [atención al cliente], [auditoría de los sistemas informáticos], [autenticación], [Base de Datos en Línea], [calidad de los datos],[cifrado],[códigos de conducta], [consentimientos], [consumidores y usuarios], [derechos ARCO], [datos de carácter personal], [derecho 'sui generis'], [dimensiones de seguridad], [documento de seguridad], [esquema nacional de seguridad], [sistema nacional de salud], [ficheros], [ficheros de acuse de recibo], [información de contrato electrónico], [infracciones agencia protección de datos], [logs], [necesidades estadísticas],[niveles de protección], [medidas de protección de programas de ordenador], [normas técnicas,patentes de programas de ordenador], procedimientos de recuperación] ,[protección de la intimidad], [protección de salud], [prueba documental], [recuperación de documentación], [requerimiento informado],[reutilización de Bases de Datos], [sanciones parámetros de calidad], [secreto], [seguridad de pacientes], [**tarjeta sanitaria**]*

por lo que se puede concluir que la observación del *Documento de Seguridad* deberá estudiar cada uno de estos apartados, al menos, en relación a requisitos legales, generando el correspondiente balanceo con su respectiva salvaguarda que se le genera, y su consiguiente monitorización.

Por otra parte, desde el punto de vista de la generación del *Documento de Seguridad*[162] y respetando aquellos *Indices* expresados en el *Capítulo 3* de la Tesis denominado *Análisis de Riesgos*, podemos añadir a la exportación del capítulo precedente y en relación a las Dinámicas del Proyecto Software las siguientes aplicativas:

1) l*a forma que adopta el documento*

Se deberá dedicar especial consideración al *Modelo Entidad-Relación* de Usuarios que tienen acceso a la Base de Datos, independientemente de si realiza labores de supervisión o no, en consideración de los *Niveles de Seguridad* que se establezcan, y los tipos de auditorías que se practiquen, pudiendo inicialmente recurrir a los Informes de auditorías generadas en años

162 Agencia Española de Protección de Datos. "Guía de Seguridad de Datos".
Disponible en: https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-ides-idphp.php

precedentes, a fin de actuar pro-activamente y generar la consiguiente salvaguarda o medida de Seguridad Auditable.
[*Item Ingeniería del Software, IS*: Modelado BBDD vs. Análisis de Riesgos]

2) *características técnicas del registro de acceso*

La política de accesos practicada puede distinguir entre el acceso público y privado, por ejemplo, entre el funcionario y una empresa contratada a terceros por otra también en el mismo requerimiento. Se puede llegar a optar por controles que precisen de la incorporación de nuevo hardware y, por consiguiente, mayor interoperabilidad, entre el sistema informático y dicha política de acceso practicada, pudiendo integrar posibilidades como biometría, VPN, Wifi, etc,..
[Item IS: Capa Software de Interoperabilidad (Diseño Protocolos Seguridad de habilitación de R/w sobre Datos, Especificación Datos-XMLs vs. Niveles Auditables)]

3) soportes

De nuevo, se impone una redefinición del término deducible de la generación de firmas de certificado que certifique el correcto funcionamiento del 'No Repudio' de la aplicación de un determinado Nivel de Seguridad, no tan sólo de la salvaguarda de los e-mailes como prueba judicial
[Item IS: nueva generación de Bases de Datos]

4) normas de etiquetado

Respetando este feedback que estamos proponiendo entre el albergue de Datos y los indices aplicables en la generación del *Documento de Seguridad*, debemos poder exigir una perfecta correspondencia entre el *Sistema de la configuración* aplicado a nivel lógico del sistema informático y el inventariado de soportes generados, evitando las redundancias
[Item IS: Gestión de la Configuración, Inventariado HW(servidores, terminales, PDAS, lectoras, ..]

5) procedimientos

Por aplicación directa de alguna norma de calidad generada por la propia organización, tal vez es el técnico informático el que deba afrontar el orden que estamos proponiendo de otra forma

[Item IS: Gestión de Proyectos: (valoración y seguimiento de hitos)]

6) ficheros

Además de las bases de datos que hemos generado y mejorado, nos encontramos en el tercer paso en nuestro esquema, en cuanto se presume la obligación de registro en la Agencia de Protección de Datos de un determinado fichero que nos exigirá, tal vez, y dependiendo del Análisis Técnico que se haga no se precise de una nueva generación de Bases de Datos, aunque sí del Estudio y Reorientación de sus Salvaguardas auditables

[Item IS: Gestión de Proyectos: compras (de Servidores)]

7) informes periódicos

La aplicación de la 'Declaración de Aplicabilidad' indicará con qué grado de exigencia se esbozará toda esta actividad auditable y practicada dentro del Plan de Calidad establecido

[Item IS: Procedimiento de Calidad]

Resulta de lógica garantizar con mayor amplitud los legales establecidos, dependiendo de la parte de la estructura organizativa tecnológica y de calidad aplicada, dependiendo de los tratamientos asociados que se practiquen , y que en el campo sanitario resultan obvios

[Item IS: decisiones legales del proyecto(ubicación y modelo de contrato de depósitos de datos]

8) iso/iec 27 002

Se puede iniciar el plan de actuación sobre las bases de datos en base a la presumible línea practicable desde la auditoría propuesta por el estándar internacional exigido

[Item IS: generación de la Mística/Filosofía de Aplicación y provocación expresa a ejemplos de surgimiento de clausulas no mencionables como *The Privacy Statement*]

9) llevanza del documento de seguridad

Resultaría aconsejable la generación de un inventario de actividad distribuidas por Niveles y de paso de Hitos Sw, de manera que el *Ingeniero Software* pueda demostrar, en todo caso, y responder a la demanda de su actividad profesional:

- relación-descripción de paso de entornos con su consiguiente garantía certificada: con especificación expresa de la identidad más la actividad del interlocutor, más indicación del procedimiento aplicable, más explicitación del registro de dicha acción justificable para no incurrir en desamparo

- monitorización del consiguiente estado del proyecto software en el que participa el Ingeniero Sw

[Item IS: Gestión de la Configuración (logs)]

10) auditorías

A la especificación inicial, suma de la especificación de estas accciones y circunstancias en las que debe funcionar

[Item IS: Modificación de la Especificación de Requisitos]

1.2.- Marco Organizacional: WP 195 art. 29 Comisión Europea

De la siguiente exposición nos vamos a atrever a invocar a la *Seguridad del Trabajador* en superación de la Taxonomía planteada al inicio de esta Tesis, con lo que consideramos que podemos presentar una solución de su elevación de caso frente a la *Seguridad del Paciente*, más ampliamente reconocida internacionalmente.

Idénticamente y al tratar de resolver la Supervisión y Monitorización de los Bancos de Datos fuera de nuestras fronteras, incluidos los marcos de trabajo de las internacionales, bien se muevan dentro del territorio reconocido por la Comisión Europea , bien en lo que se ha venido en denominar *third countries*, se deduce que no puede andar tan lejos el planteamiento de una Historia Clínica Mundial, con lo cual sí que podemos hablar con total tranquilidad y , es más, con suficiente necesidad, de la *Seguridad del Trabajo* para el Técnico Informático.

Siguiendo el mismo esquema que en el apartado anterior , vamos a proponer una determinada sección, entre corchetes, del *Documento WP 195* y a continuación realizar alguna observación precisa para nuestro entorno sanitario, donde cobra mayor gravedad e importancia el control de la Medida de Seguridad:

- *RESPONSABILIDAD, [1.1]*:

  nos va a permitir la definición de la virtualización del contrato-proyecto, al menos en relación a las cláusulas aplicables al *Ingeniero Software*, esto es, al conocimiento y formación de interacción en su respeto de la naturaleza del dato en cuyo entorno participa, debe de poder actuar conscientemente sobre el rango que le compete del '*Service Agreement*'.

- *GRADO DE IMPLICACION*, *[1.2]*:

  no olvidar indicar la dirección que parece que devendrá de la aplicación del *Documento de Seguridad*, o un nuevo estándar, o un cambio de política en materia de *Seguridad del Trabajo*, o una revisión de la ampliación de la *Ingeniería del Software.*

- EJERCICIO DEL DERECHO DE PROTECCION EN MATERIA DE PROTECCION DE DATOS, [1.3]:

  los derechos en materia de protección de datos, “data subjects rights”, se verán protegidos judicialmente ante cualquier perjuicio y la contemplación de recibir compensación, y no sólo haciendo referencia explícita de daño físico, any distress; e.g.: desaparición o cese de actividad del controlador. No se puede partir del presupuesto de que cualquier acción dañina contra los Derechos de Acceso, Rectificación, Cancelación y Omisión, y defensa de la Intimidad quede inpune. Es nuevamente la elevación de la Taxonomía correspondiente al Técnico Informático, pero en relación directa con su Seguridad la que nos permite plantear la Seguridad del Trabajador como se hiciera con el tratamiento recibido desde la perspectiva de la Seguridad del Paciente.

- *RESPONSABILIDAD DE DAÑOS, [1.5]*:

  se consideran , además de los presupuestos miembros de los Estados Europeos, los BCRs y brechas gestionadas por sub-procesadores establecidos fuera del espacio europeo. Las

clausulas de los contratos que consideren estos supuestos deberán reflejar, en cualquier caso, de anotar el tratamiento y defensa concreta ante las autoridades competentes

- *RESPONSABILIDAD ECONOMICA, [1.6]*:
  las compañías involucradas en el tratamiento de los BCRs puede responder económicamente por los posibles daños producidos or *to pay compensation*.

- *RESPONSABILIDAD DEL PESO DE LA CARGA DE PRUEBA, [1.7]*:
  propuesta organizacional en base a los presupuestos anteriores de en quién se delega la responsabilidad completa o parcial de una posible brecha. Si de resultas el miembro del grupo que firmó la clausula de '*liability*' , consigue demostrar que la tercera parte involucrada no tiene responsabilidad, es entonces cuando debe desentenderse de su responsabilidad.

- *GARANTIA DE UN PROGRAMA DE FORMACION DE CARA AL USUARIO, [2.1]*:
  debiendo resultar públicos desde la Web del Grupo con una expresión fácil de entender al *data subject*.

- *GARANTIA DEL PROCESO DE DENUNCIA, [2.2]*:
  la doctoranda expresa su aprecio del documento encontrándose, en su análisis, el reflejo por la preocupación del flujo de datos fuera de las fronteras naturales de un estado. El documento expresa la suficiente confianza en el ámbito internacional, y que, por otra parte, nos puede permitir concluir visiones más holísticas y menos genéricas que algunas partes de la doctrina legislativa hasta llegar a poder demostrar la exigencia que se debe de respetar entre:

    - la Seguridad del Paciente
    - la Seguridad del Trabajador

- *ASEGURAMIENTO DEL PLAN DE AUDITORIA, [2.3]*:

además de determinar la entidad o sección del grupo que establece el *Plan de Auditoría* , se ha de decidir la entidad que la llevará a cabo, el tiempo de la auditoría en concordancia con la 'on specific request from the appropiate *Privacy function*' y la cobertura de la misma, esto es,

si se va a realizar sobre las aplicaciones, sobre las Bases de Datos que procesan Informaciones Personales y/o bien sobre trasferencia, sobre decisiones tomadas como nuevos requerimientos legales y que involucran al BCR, las revisiones de los términos contractuales sobre las trasferencias del Grupo, las acciones correctivas y la entidad que recibirá los resultados de la auditoría

- *ACTUALIZACIONES DEL BCR, [5.1]*:

como consecuencia del proceso de modificación, esto es, por introducción de nueva regulación o estructura de la compañía comunicación de dichos cambios a los miembros del grupo , a las autoridades en materia de protección de datos y al controlador. Se establecerán Medidas del tipo siguiente: ninguna transferencia debe ser realizada a ningún miembro del grupo, hasta que éste pueda demostrar de que puede adherirse a seguir el conjunto de clausulas y medidas preestablecidas para el BCR, debiendo expresarse claramente las razones de actualización

- *REGISTROS CONTRACTUALES Y DE CALIFICACION DEL TIPO DE MOVIMIENTO DE DATOS, [6.1]*:

  según los términos de finalización de la provisión de un servicio, los procesadores o sub-procesadores y de acuerdo a las condiciones que establecieran los controllers, retornarán el conjunto de datos personales transferidos, certificando en su caso el momento en que se produjera la correspondiente destrucción, a no ser que existiera regulación que trabara o impusiera condición a alguno de estos puntos. En tales casos, el procesador o sub-procesadores , confirmación y comunicación al controlador su compromiso de garantizar la confidencialidad de los datos trasferidos y de que no se realizara transferencia alguna nunca más. Se permite el caso de la contratación de procesadores externos siempre y cuando se permita la adecuada protección conforme a los artículos 16, 17, 25 y 26 de *D 95/46/ce* y las secciones correspondientes del presente documento *WP 195* .

- *APLICACION DE UN PRINCIPIO DE TRANSPARENCIA, [6.2]*:

  si existiera proceso de investigación iniciada, por ejemplo, en materia criminal y de servicio a la Fuerzas de Seguridad del Estado, los requerimientos asociados serán oportunamente comunicado primero a la autoridad competente en materia de protección

de datos, y a su vez éste al conjunto de la estructura competente de BCR que se hubiere establecido

2.- Control PDCA

Pretende reforzar la aplicación de las secciones siguientes en el RD 03/2010 en su Anexo III:

- 4.2 *Control de Acceso*:
  <<cuando se interconectan sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales y acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabililades de cada sistema>>

- 4.3.8 *Registro de la Actividad de los Usuarios:*
  <<se registrará toda aquella evidencia que pueda sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecucción de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado>>

Cuando se recoge la expresión '*Workplace Safety*' en el ámbito de la *Ingeniería del Software* debemos prestar cuidado cuando pueda que se cite la muerte de trabajador, por poder querer implicar no la muerte física sino la finalización de su relación contractual como consecuencia de una malevolente *Política de Seguridad* en el contexto de los Regímenes de Outsourcing que puede
contemplar la Administración Electrónica cuya naturaleza es Pública, aun cuando la Empresa que proporciona el servicio se mueve en la línea de la Empresa Privada.

Si desde el punto de vista técnico y en el contexto del Sistema Operativo Unix/Linux, por expresar el más claro ejemplo, nos resulta extremadamente sencillo seguirle la pista al Perfil de un Usuario cuando este realiza Pruebas de su Trabajo y los Entornos que tiene Operativos y que se encuentran

perfectamente auditables desde unos sencillos logs que se generan por voluntad del Administrador del Sistema, nos podemos preguntar si tan caro le puede resultar a la Administración Pública el permitirle demostrar al Trabajador hacia su Empresa y/o la misma Sección de la Administración en la que se desempeña su labor que <<efectivamente ha hecho lo que tenía que hacer>>, esto es, ha generado un determinado Hito, este ha sido probado en tal y cual entorno y se han encontrado o no con unos determinables problemas o se han producido incidencias cuantificables de forma que podamos esbozar un Itinerario cuantificable de su Quehacer, pues si de la misma forma hemos conseguido superar males precedentes como la defensa del *daño moral* o el de la *Propiedad Intelectual* , la Salud del *Ingeniero del Software* debiera poder contar con la Justificación de su labor.

El Esquema que hemos presentado para poder llegar a esta Conclusión se inicia en el Comienzo de la Tesis cuando hemos planteado las Taxonomías de dos de los tres Grupos y en relación a la Protección de Datos en el ámbito de la *e-Sanidad*, dígase la del Paciente-Ciudadano y la del e-Técnico, depositando la fe de la del Profesional Sanitario en sus *Códigos Tipos* y elaborados por sus Profesionales. Dichos Profesionales sí que cuentan con la prueba judicial manejable de la *Tarjeta Profesional Sanitaria* que permite la auditoría y acceso por *Niveles de Seguridad* Regulables en el acceso al Historial Clínico de determinados Pacientes o por cada Paciente a determinada Operativa Médica.

Del mismo modo que la Taxonomía del Paciente obtiene su máxima expresión en la *Seguridad del Paciente* y la defensa de sus *Derechos ARCO*, el e-Técnico informático debiera poder elevarse en el campo de la Seguridad del Trabajador manejando una Herramienta como lo es una *Tarjeta Profesional* que reflejara el Proceso Informático que hemos iniciado en relación a la Expresión Formal del Log de su Cuenta de Usuario.

Como consecuencia de que el *Ingeniero de Software* debe ser informado de esta nueva actividad practicable sobre su Oficio, no pretendemos suplantar los Procedimientos de Calidad Software a los que debe responder , sino preceder la actividad de cada Nuevo Proyecto definible con una Virtualización de aquella sucesión de Hitos Registrables desde su Tarjeta Profesional auditable idénticamente desde su Empresa Contratadora y en respuesta de su labor en el Sector Público. Siendo con toda facilidad observable desde un *Ministerio de Trabajo*, por ejemplo, en sus labores de Inspección.

Con esta orientación pretendemos responder a la responsabilidad que se espera de los Trabajadores,

responsabilities of employers, desde la *Agencia Europea para la Seguridad y Salud en el Trabajo*[163]. A continuación presentamos la relación de Controles correspondientes a la *ISO/27001* y la relación que se encuentra dentro de la perspectiva propuesta sugerida

- una aplicación de Supervisión de Indicadores por los que se riga el *Documento de Seguridad*, [*Pp_O*, Perfil de Protección O]

- un Procedimiento de Virtualización del Procedimiento del Contrato del Proyecto del *Ingeniero de Software* identificable como el *Perfil de Protección*[164] del *IS*, [Pp_1, Perfil de Protección 1]

- la instrumentalización de una Tarjeta Profesional para el *Ingeniero Software* que colabora en la Sección de la e-Administración, [Pp_2, Perfil de Protección 2]

163 *Worker Participation in Occupational Safety an Health. EU-OSHAS. "A practical Guide European Agency and Health at Work"*.2012. (pag. 11) <<The legal and policy framework places responsibility for ensuring OSH clearly on the *Employer Council Directive 89/291/EEC* on the introduction of measures to encourage improvements in the Safety and Health of workers at Work Council Directive, 1989, define the responsibility in Article 5: "The employer shall have a duty to ensure the safety and health of workers in every aspect related to the work. The employer may enlist competent external services or persons, but this shall not discharge him from his responsabilities in this area. Article 6 states that 'within the context of his responsabilities, the employer shall take the measures necessary for the safety and health protection for workers including prevention of ocupational risks and provision of information and training as well as provision of the necessary organization and means'. Employers must also have regard to the right of workers to be involved in the management of Safety and Health at work, established by article 11 of the Directive. The *European Community Strategy for Improving Quality and Productivity at Work*(COM, 2007), emphasized the need to promote within businesses the management of Safety and Health at Work. The Strategy set out 'to encourage changes in the behaviour of workers and to encourage their employers to adopt health-focused approaches'>>

164 Puesto que la propuesta a falta de ser integrada en lo Público (y para entonces, de suceder, probablemente encontraría otra expresión), parte de lo Privado, me remito a la Semántica utilizada desde los *Criterios de Certificación de Producto*, más adelante explicados y mundialmente referenciados como *CC*. Sirva de ejemplo esta aplicación acerca del modo de incorporación real en lo Público de Soluciones Técnicas, que una vez superado su Fase de Auditoría y consiguientes Validaciones pasa a lo Público y de nuevo referenciado hacia la parte participante Privada , probablemente, como un Procedimiento a seguir. En referencia a dicho proceso tan sólo encontramos en la Disposición adicional única correspondiente al *RD 170/2007* y en relación a los Productos de Software la mención siguiente: << los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en si una descripción técnica del nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el Título VIII de este reglamento>>

ISO/IEC 27 001 clausule	SPECIFICATION	MANAGING THE BOUNDARIES UNDER PROTECTION PROFILE SOLUTION	ISO/IEC 27 002 control
A.6.1.4	Proceso de autorización de recursos para el procesado de información	inicio de la virtualización del contrato [*Pp_1*]	• Proceso definido e implementado • las políticas y requerimientos de seguridad han de ser cumplidos • el software debe resultar compatible con otros componentes del sistema • uso de facilidades (laptops, etc.) para el procesamiento de información
A.6.2.1	Identificación de los riesgos derivados del acceso a terceros	delimitar tanto los Hitos producidos en cada Entorno y Segmento de la Red (riesgo económico mesurable) y todos los Tipos de Autenticaciones (que pueden ser controlados por otros terceros) [*Pp_1*]	• La identificación de riesgos toma en cuenta: : el acceso físico, el lógico y la conectividad de red • determinación de controles cuando almacena, procesa, comunica, comparte e intercambia información (tb. controles no accesibles por los terceros)
A.6.2.2	Tratamiento de Seguridad en relación con los clientes	Consideración precisamente del Proceso de Virtualización del Contrato Propuesto [*Pp_1*]	La *descripción del servicio o producto* a ser provisto requiere a considerar previo a accesos: • dimensiones de la seguridad(integridad, ...) • restricciones de copiado y divulgaciones • procedimientos que determinen si el activo está comprometido • procedimientos para proteger los activos
A.6.2.3	Tratamiento de la seguridad en contratos con terceros	podría resultar una medida/indicador de la Calidad Producible en base a los Requisitos de Seguridad [*Pp_O*]	Se tiene en mente la indemnización de las partes: • acuerdos para el reporte de notificaciones e investigación de las inexactitudes de información, incidentes y fallas de seguridad • controles para asegurar el retorno o destrucción de la información y los activos al final o en un

			punto acordado
A.8.1.1	Funciones y Responsabilidades	Especificación y Definición incluida en base a las medidas registrables en la Tarjeta Profesional, si se considerara el paso a Soporte Físico, además del Escrito de Hitos y Logs de Accesos visibles y demostrables por parte del e-Trabajador Informático [*Pp_1*] y [*Pp_2*]	Los roles y responsabilidades de la seguridad debieran ser definidos y claramente comunicados a los candidatos para el resto durante el proceso de pre empleo
A.8.1.3	Términos y condiciones de contratación	Firmado del control A.8.1.1 [*Pp_1*]	Se podría utilizar un *Código de Conducta* en relación al Usuario, Empleado, Contratista y Tercera Persona a las Dimensiones de Seguridad, Protección de Datos y Uso apropiado del Equipo
A.8.3.3	Retirada de los derechos de acceso	existencia correcta en la Dinámica de los Movimientos Registrados en la Tarjeta Profesional [*Pp_2*]	Consideración de la terminación del empleo o acuerdos de cambio: • determinación-responsabilidad de la parte que lo determina • el valor de los activos en ese momento
A.10.1.3	Segregación de Tareas	Concreción de la Categoría Profesional del Interlocutor que permite una Determinada Autenticación y Conocimiento del Nombre de su Empresa en régimen de outsourcing (a fin de reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización)	Se valorará la independencia de la auditoría de seguridad
A.10.1.4	Separación de los recursos de desarrollo , prueba y operación	no se debe permitir accesos a Entornos fuera de lo estipulado [*Pp_1*]	Se debe de evitar la capacidad de cometer fraude o introducir código no-probado o malicioso
A.10.2.2	Supervisión y revisión de los servicios prestados por terceros	[tb. Auditables periódicamente [*Pp_O*]	Revisión de rastros de auditoría de terceros y registros de seguridad, problemas operacionales, monitoreo de fallas e interrrupciones relacionadas con el servicio entregado
A.10.6.1	Controles de Red	Especificación de aquellas Medidas de Seguridad que permiten la aplicación de un [*Pp_1*]	Protección de la infraestructura de soporte
A.10.7.1	Gestión de Soportes Extraíbles	[*Pp_2*]	Si no fueran requeridos por más tiempo, los contenidos de los medios re-usables que no son removidos de la organización no

			debiera ser recuperables
A.10.10.2	Supervisión del uso del Sistema	Sistema Informático [*Pp_0*]	Prácticamente una especificación del interfaz del componente software
A.10.10.5	Registro de fallos	[*Pp_2*]	Entrada de medidas correctivas
A.11.6.1	Restricción del acceso a la información	La Política de Seguridad debe perseguir el buen desarrollo de [*Pp_1*]	Control de derechos de acceso de otras aplicaciones
A.12.5.5	Externalización del desarrollo de software	Orientación Inversa de la Propuesta [*Pp_1*], pero no contradictoria	Derechos de acceso para la *auditoría de calidad* y *seguridad del trabajo* realizados
A.13.1.1	Notificación de los eventos de seguridad de la información	Supervisión de los Eventos que produjeran los Controles que aseguran [*Pp_1*] y [*Pp_2*]	• Toma de conducta correcta ante un evento en la seguridad: anotaciones de no cumplimiento, mensajes, conducta extraña • referencia a proceso disciplinario
A.13.2.3	Recopilación de evidencias	[*Pp_2*] como Soporte	Cuando una acción de seguimiento involucra una acción legal , consideración de las reglas de evidencia(admisibilidad, peso)
A.15.1.4	Protección de Datos y Privacidad de la Información Personal	aludiendo al doble sentido de Supervisión del Sistema Informático y la Seguridad del Trabajo del e-Trabajador (ANR)	Equilibrio entre las legislaciones estatales, el marco de Privacidad y la determinación de Actores (Cap. II)

Tabla 6. Supervisión ISO/IEC 27 001, Complemento ISO/IEC 27 002

Imaginemos que una Entidad Reguladora Autorizada en Materia de Protección de Datos proyecta el Diseño de una App, aplicación informática, que facilite la labor del legislador en materia de Protección de Datos y considera que la Gestión de los *Documentos de Seguridad* que se auditan desde la Entidad puede producir material suficiente para permitir el favorecimiento de la Ayuda al Legislador en cuanto a sus Conclusiones de Resultados y generación de legislación positiva para el Desarrollo del ejercicio del Derecho en la Informática.

Podemos plantear la opción de recurrir a la Empresa Pública o Privada para la consecución de su Diseño y/o Implementación.

Se observa que se precisa del Observatorio del trabajo existente de Fundamento Estadístico para la Especificación del Prototipado en cuanto a:

a) el Interfaz

b) el juego del modelo de Indicadores a aplicar, locales o globales. Consideración de la Naturaleza del Dato

c) evaluación en las direcciones de las políticas: resultando la Política auditable, especificación del Framework de integración de modificaciones legales

A continuación, podemos hacer alusión en base de la Aplicación o Minimización por Aplicación de Auditoría Interna, que permite la Observación de la perspectiva del Auditado. Por ejemplo, que se le concede Prioridad a la perspectiva de la Base de Datos: estamos detallando el Detalle del Indicador practicado sobre el Auditado que se puede traducir en archivados de experiencias.

A continuación y a modo de relación preguntas-respuestas podemos llegar a expresar el nacimiento de la *e-Administración del Derecho Informático*[165]

- ¿resulta correcto que la iniciativa partiera de la Empresa Privada?

la Supervisión siempre debe producirse desde lo Público

- ¿existe suficiente casuística de modelado en la función estadística?

consideración de la fase del Plan Informático Estadístico de la EU

- ¿resulta factible la automatización de las auditorías?

afirmativa

En relación a la valoración de la dificultad, y partiendo de la intención de poder expresar visualmente y por medio de Gráficos[166], la variabilidad dentro de una determinada Operativa de los comportamientos de las diferentes secciones auditables a fin de, y aplicando diferentes algoritmos, tablas de indicadores y volúmenes de datos, aquellas políticas que convenga reforzar internamente o impulsar legislativamente, conseguiremos reforzar la Funcionalidad del Soporte a la actividad parlamentaria en relación al Desarrollo y Optimización de los Sistemas de Información, inclusive la

165 L 19/2013, Unidades de Información, (art. 21)

166 MAGERIT-version 3.0.. "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III-Guía de Técnicas". Cap. 3 Técnicas generales. 3.4 Técnicas gráficas (pag.26), Madrid octubre de 2012.

elaboración de Guías , siempre orientadas a la potenciación auditable de determinadas líneas base del *Documento de Seguridad*.

La Técnica aplicable, probablemente, será una *Valoración Delphi* sobre la preparación de un cuestionario cuya valoración se desea conocer, permitiendo realizar un Histograma sobre la Valoración de los Indicadores que se hubieren hecho implícitos en los cuestionarios a valorar y aplicando *Teoría de Modelos de Estadística Básica*[167]. Ante un histograma disperso siempre hay que preguntarse si se ha hecho la pregunta correcta a las personas correctas, y/o si ha estado la pregunta correctamente expresada .

Precisamente , y debido a que el ámbito sanitario cuenta con los mayores controles en relación a la Protección de Datos, y tal vez por haberse considerado la naturaleza del dato como de sensible y viéndose repercutida toda la cadena de la acción laboral afectada, podremos obtener un mejor gradiente de calidad en los resultados, y poder aplicarlos a los Sistemas Informáticos con otras competencias.

Podemos, distinguir, de entrada con

- la relación de Escenarios definidos precisamente por el conjunto de actores que se presuponen participan en cada operativa, pudiéndose recortar , incluyendo o aumentando el número de roles y dependiendo de las especificaciones de los *Códigos Tipos* participados: la relación completa quedaría resumida por los reconocidos en el apartado 3.3. sumándose a ellos los encontrados en las especificaciones de los Sistemas Informáticos Europeos y que actualmente se encuentran en implementación como sería el caso de los LISOS , apartado 3.4.3, (el controlador, el procesador, la agencia de protección de datos-interlocutores por *Niveles de Seguridad*-, el promotor, el monitor, la CRO, el investigador, el auditor, la agencia de medicamentos y productos sanitarios, el asistente de e-sanidad-interlocutores por Niveles sujeto al desarrollo de la LOPS y evolución de las Certificaciones Profesionales por relación Grupo Profesional y Categoría-, el perito, los supervisores supranacionales como los LISOS y

167 Se pueden considerar recubrimientos de Capas Software sobre Lenguages de Programación Estadísticos como Octave o R
IEEE Computer Society Professional Practices Committee . SWEBOK, 1.5 *Quantificable Requierement* (pag. 35): Software requirements should be stated as clearly and as an ambiguosly as possible, and, where appropiate, quantitatively. This is particularly important for non functional requirements
MAGERIT v3.0 "Metodología de Análisis y Gestión de Riesgos de los Sistemas Informáticos. Guía de Técnicas." : 3.4 Técnicas Gráficas; 3.7 Valoraciones Delphi; 3.7.3.1 Análisis Estadístico (media, mediana, desviación media, cuartiles, recorrido intercuartílico

los supervisores supraeuropeos -precisando el proyecto-)

- la tipología del Soporte de la Unidad Administrativa Tecnológica: Capa de Software concreta, Base de Datos, Verificación de Protocolo, Inventariado de HW, etc, ..

- grupo de indicadores que se intenta analizar, como resultado de cada auditoría, pudiendo basarnos en la propia especificación *ISO 27 002* conjuntamente con los *RD 03/2010* y *RD 04/2010*

- generación de archivos con formato *.pdf, conducentes al envío de certificados digitales-firma electrónica

- framework de entrada de cómo se recepciona la información y que, obviamente, se encuentra sujeto a a los requerimientos de interoperabilidad de cada momento y situación, pudiendo ser incluida la consideración de catástrofe natural. En tal medida la especificación del diseño de la *Base de Datos* con variables cruzadas, esto es, la especificación del diseño de fichero con los datos a analizar y que se considera entrada

Del conjunto de una muestra semestral, y por otorgar un período razonable de prueba, podemos intentar extrapolar alguna dependencia y en qué orden entre dos Indicadores, cuando, además, por ejemplo, se acaba de introducir determinada salvaguarda en la Sección de la *Administración Electrónica*, lo que propondría otro modelo de trabajo que sería la relación de interdependencia entre Medias de Seguridad. De manera, que se propondría estudiar la Arquitectura tecnológica de ambos Indicadores en circuito, a fin de tratar de minimizar no sólo la dependencia del error, sino la resolución de incidencias en la auditoría del *Documento de Seguridad.*

De esta forma, la introducción de una auditoría más extensa, podría estar iniciada con premisas basadas en la experiencia de este tipo, y de resultas, consultables en un catálogo de Optimización permitiéndonos evitar los puntos más débiles de las Auditorías, y consiguiendo desarrollar una nueva Ciencia sobre la Estadística de estos Indicadores y Niveles de Corrección de Dependencias.

Con esta orientación se puede proponer una línea en la auditoría legal practicada: el estudio de la *Trazabilidad*[168], y que, por otra parte, resultaría sumamente útil a la hora de evaluar un daño

168 *Guía CCN-STIC nº 803,* (pag. 25) : propiedad o características consistente en que las actuaciones de una entidad

compensatorio en el ejercicio del *Habeas Data.*

Para concluir y puesto que el análisis del comportamiento de cada *Documento de Seguridad* se puede realizar por separado, o bien obtener mayor información cuando se individualiza esta información, por selección singular por parte del usuario, se guardará información del *Caso de Uso* relativo a tal Operativa.

Se podrían generalizar la supervisión de las auditorias por extensibilidad de los casos de uso[169]: y obtener valoraciones agrupadas, por ejemplo: la relación <<*extiende*>> se utiliza cuando un caso de uso es similar a otro caso de uso pero se le añade alguna característica nueva.

Por tratarse de operativas similares, existirán comportamientos de datos concretos cuya observabilidad merezca apuntar en base a los indicadores que se definen para ellos, en base, al *Plan de Trazabilidad*, que corresponden , más propiamente a una auditoría interna o bien a la ejecución de los Derechos ARCO. Se pueden presentar ejemplos de los dos casos. Esta claro que se debe presentar el modelo propio de las Base de Datos, para indicar en el proceso de Ingeniería Inversa como le afectarían la generación de estos Informes.

Incluso se puede presentar la cuestión de si en el Ejercicio de los *Derechos ARCO*, el Paciente podría obtener una Representación de este Modelo como prueba del Circuito que han recorrido sus datos y haciendo invocación del citado *Derecho de Impugnación de Valoraciones*.

Por su parte, los Indicadores que maneja el Sistema Nacional de Salud lejos de aligerarse, se incrementará y ganará en complejidad con el tiempo. Razón por la cual, aunque nuestro razonamiento basado sobre el ENS, no resulta innecesario contar con una breve descripción de lo que

---

pueden ser imputadas exclusivamente a dicha entidad

IEEE Computer Society Professional Practices Committee SWEBOK, Guide to the Software Engineering , Body of Kowledge.. 2004, (pag. 42): 7.4: *Requirements Tracing*.: <<Requirements tracing is concerned with recovering the source of requirements and predicting the effect of requirements tracing is fundamental to performing impact analysis when requeriments change. A requirement should be traceable backwards to the requirements and stakeholders which motivated it. Converserly, a requeriment should be traceable forwards into the requirements and design entities that satisfy it>>

169 PRESSMAN Roger. "Ingeniería del Software: Un Enfoque Práctico". 7º Ed. 2010. University of Connecticut. Cap. 5. (pag. 113): los casos de usos se definen desde el punto de vista de un actor. Un Actor es un papel que desempeñan las personas (usuario) o los dispositivos cuando interactúan con el software.... En esencia, un caso de uso narra una historia estilizada sobre cómo interactúa un usuario final (que tiene un cierto número de roles posibles) con el sistema en circunstancias específicas. La historia puede ser un texto narrativo, un alineamiento de tareas o interacciones, una descripción basada en un formato o una representación diagramática, Sin importar su formato un caso de uso ilustra el software o sistema desde le punto de vista del usuario final.

supone el actual Esquema de Trabajo , basado en el proyecto *ECHI* y promovido por la propia Comisión. La variabilidad en la recogida y procesamiento de los datos en los 27 Estados miembros cuenta con un primer grupo de cuarenta Indicadores de Salud de la Unión Europea. Otros juegos de Indicadores en los que trabajan otros Organismos se distribuyen entre la OCDE, EUROSTAT y OMS, entre otros. En el futuro, y tal y como se perfila en el seguimiento de los Sistemas Informáticos descritos en el Capítulo segundo, se completará el enfoque[170] mediante la incorporación de otra información en el campo de la prestación farmacéutica, la salud alimentaria, la salud medioambiental y otras vertientes de la Salud Pública, así como del ámbito del Consumo.

De la solución de Control PDCA formulado podemos extraer nuevas conclusiones, por otra parte obvias cuando se considera cada clausula o control de forma individual, y en este caso:

170 Plan de Calidad para el Sistema Nacional de Salud. "Indicadores Clave del Sistema Nacional de Salud".Marzo 2007

Expresión de la Conclusión de Tesis	Argumentario
[Conclusión.1] Aplicación Informática como *Salvaguarda Legal*	Elevación de la Prueba Judicial garantizada como Aplicación Informática en la Aplicación y Desarrollo de los Roles de la Familia Profesional Sanitaria y no dejado a la buena voluntad de la Planta de cada una de sus Categorías Profesionales a)Consecuencias de su Observación: Se puede garantizar el Marco Legal del Trabajador Informático por Trazas de los Hitos de su Categoría Profesional de manera que podamos afirmar que <<hace lo que tiene que hacer>> , al menos desde el punto de vista informático
[Conclusión.2] Elevación de Apreciación de *Requisito Informado Legal* funcionando como *Agente*	Iniciación de Políticas en torno a la Tarjeta Sanitaria: coberturas desde el Trasfondo de su Vida Laboral: a)Cambio de Gestión y Monitorización de Tarjeta Profesional. Ejemplo: Ministerios de Trabajo y no de Consumo y/o Sanidad b)Aporte al Valor Añadido de la HC Mundial, aun por especificar

Tabla 7. Tabla de Conclusiones Control PDCA

2.1.- ENS

Frente al razonamiento de la Taxonomía del Paciente y regulado por derecho fundamentándose el el *art. 13* de la *LOPD*, el ejercicio del *derecho de impugnación de valoraciones ,* el afectado tiene derecho a obtener información del responsable del fichero sobre los criterios de valoración y el 'programa' utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

En la afectación por analogía de la Taxonomía del e-Sanitario encontramos en algunas Comunidades Autonómicas la utilidad de la herramienta de las *Tarjetas Sanitarias Profesionales* que nos han permitido llegar a la Propuesta denominada "Perfil de Protección del Ingeniero Software" y que hemos sugerido al querer potenciar la *Seguridad en el Trabajo* o *Safety at Work*.

Por otra parte, interesa resaltar la importancia que cobra en este punto el apartado nº 4 de aplicación del *Documento de Seguridad* expuesto en el capítulo anterior, denominado *Normas de Etiquetado* por considerar de fundamental y central importancia en este apartado la consideración que realiza la norma *ISO/IEC 27799* en su *control 7.4.2.1*[171] y que nos conduce a postular el carácter *Central* que debieran tener el tratamiento de estos datos de carácter especialísimo, permitiéndonos sugerir la idea

171 *ISO/IEC 27799* (pag. 34) <<Because one cannot predict the *sensititviy* of a given element of personal health information through all its uses and all the phases of its life cycle, all personal information should be subject to suitability careful protection at all times>>

de que al igual que ocurre con otras soluciones que se están encontrando en el horizonte de la implementación[172] del camino que debe de seguir Internet se debería reconducir precisamente el tratamiento de ese carácter especialísimo como el nodo principal o Entidad Informática Mínima a partir de la cual se debiera desenvolver el resto del Sistema Informático, de manera que no tuvieran que complicarse Ingenierías Inversa futuras.

Persiguiendo reforzar la simplicidad técnica y evitando caer en dificultades de carácter técnico que hicieran rechazar su aplicabilidad queremos recordar el ejemplo expuesto de una Auditoría de los Logs en el Sistema Operativo Unix/Linux desde el control *7.7.10.2* denominado '*Audit Logging*' y que postula que aquellos Sistemas Informáticos en el ámbito de la Sanidad y que ejecutan el procesado de información médica deberían crear un registro auditable seguro en cada ocasión que un usuario accede, crea, actualiza o almacena el *medical record* a través del *SI*, Sistema Informático. El Log resultado debería identificar de forma unívoca al usuario, y al dato objeto y el instante de la tramitación por la Red.

Precisamente, cuando interactúan tantos actores pertenecientes tanto a los grupos de la Familia Profesional Sanitaria[173] que hemos venido en denominar *e-Asistente* para diferenciarlo del *Ingeniero de Software*, perteneciente , por su parte, a la Familia no tan delimitada profesionalmente en cuanto a su academicidad de los Técnicos informáticos, es cuando resulta más clara la necesidad de crear el Sistema que aborde el apartado que nos compete desde su Centro elevando precisamente el *Sistema de Etiquetado* en cuanto que deberá ser reflejo y vínculo detectable en los innumerables accesos , todos ellos auditables y protegidos, desde la parte de una Inspección de Trabajo en un primer nivel, y en segundo desde la Supervisión de Datos, y aún cuando hoy en día se está viendo en orden inverso.

Sí que bien es cierto que existe una alusión directa en el *control 5.4* en la norma *ISO/IEC 27799* a la información médica , cuando nos recuerda que existen varios tipos de información cuya confidencialidad, integridad y disponibilidad que debe ser protegida, concretando en su apartado g) y en relación a los datos de auditoría interna que produce el Sistema Informático y donde quedan registradas las acciones de los usuarios. Encontramos, por otra parte, en el *control 7.5.1.2* de

172 The development of the TAS3 PDS is based on work done by the Internet of Subjects Foundation outside TAS3. The IoS defines *user centricity* as a person-centric architecture where every piece of data produced by, or related to, an individual is published and stored in his/her own personal space. Thus the use of this data in distributed computing applications will stem from discovery of data. (IoS www.iosf.org)

173 *Real Decreto 1093/2010*, Relación de Anexos: Valores que pueden tomar las Variables de 'Categorías Profesionales'

Monitoreo o *Screening* la sugerencia de que todo el personal que participe en el procesado de información clínica debería, como mínimo referir su dirección y puesto de trabajo anterior a la ocupación que le ocupa así como la sugerencia de revisar desde las Familias Profesionales a la que pertenece su real asociación y pertenencia. Ante tal postura, nos podemos preguntar si el Ingeniero de Software no puede exigir el mismo grado de exigencia al respecto de la garantía respecto de su labor a fin de justificar su actual contrato.

De la mano de la Guía de Seguridad *CCN -STIC -813* en relación a los "Componentes Certificables en el Esquema Nacional de Seguridad, ENS" nos permitimos introducir , producido por el Centro Criptológico Nacional, CCN, el procedimiento de Certificación que no puede ser obviado. Recordamos, además, que el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, se constituye al amparo de lo dispuesto en el *art. 22* del *Real Decreto 421/2004* y regulado por la *Orden PRE/2740/2007.*

El uso de componentes certificados, bien hardware bien software es una Medida de Seguridad que aplica con carácter general al Nivel Alto y, en algunos caso, al Nivel Medio. En *Common Criteria* o *CC* como ya veremos las Salvaguardas se denominan Requisitos de Seguridad.

La certificación se otorga mediante resolución del CCN, a instancias del propio fabricante. Dicha resolución identifica las Normas de Seguridad utilizadas, la *Declaración de Seguridad* utilizada o Requisitos de Seguridad que cumple el producto y el *Nivel de Garantía* y Vigencia de la misma.

El Organismo de Certificación utiliza la siguiente norma para la certificación: "*Common Criteria for Information Security Evaluation, CC*" y que se publica como ISO/IEC 15408. En relación a los requerimientos de funcionalidad para Módulos criptográficos y Prueba de Requerimientos: *ISO/IEC 19790:200* e *ISO/IEC 24759: 2008*. Aun cuando se considera certificación no funcional de seguridad a la Criptológica.

El Documento Técnico que hace referencia a las Propiedades de Seguridad del Producto se conoce como *Declaración de Seguridad* en términos de CC o *Política de Seguridad* en la norma *ISO/IEC 19790:2008* de Seguridad de Módulos Criptográficos. Incluye, por su parte, la descripción del problema, los activos de la información a proteger por el producto, los ataques esperados, la descripción del entorno de uso, las hipótesis que se aplican a este uso y las políticas organizativas que se deban respetar o aplicar. Además del documento referido , aparece la especificación del *Perfil*

de Protección, Protection Profile o PP que se configuran como una acuerdo general sobre un problema de seguridad y una posible solución. De las secciones de las que consta la Declaración de Seguridad, es la *Declaración de Conformidad* o *Conformance Claim* la que muestra si ésta debe ser conforme a algún Perfil de Protección , y si es así, a cuáles.
A efectos del *Esquema Nacional de Seguridad*, los *Certificados CC* emitidos por terceros países se reconocen hasta un nivel EAL4. La relación de países reconocidos va aumentando y se puede consultar en la página web del "Arreglo de Reconocimiento Mutuo de Common Criteria"[174].

En cuanto a la vigencia, los certificados emitidos por el Organismo de Certificación son válidos hasta que se revocan, la revocación se publica, al igual que el certificado en el *Boletín Oficial del Estado*. Cada dos años de su emisión, el Organismo de Certificación realiza una revisión de la vigencia de cada certificado. El objetivo de dicha revisión es la comprobación de inapreciable variabilidad de sus definiciones. La revisión de los certificados puede provocar la anulación del mismo, por resolución expresa del Director de Certificación.

En consideración de la legislación vigente, el *RD 03/2010* que da cumplimiento al Esquema Nacional de Seguridad, y en aplicación de su art. 27 estamos elevando la condición de mínimo exigible que tiene en cuenta:

1. los activos del sistema

2. la categoría del sistema

3. las decisiones que se adopten para gestionar los riesgos identificados

Conforme al mismo Decreto Anexo II 4.2.d que determina que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización, se pude concretar que en tiempo real ese nuevo Componente se conformaría como una herramienta clasificatoria o instrumento para la evaluación de gestión de cambios y vigilancia de personal.

174 *Protection Profiles*: Access Control Devices and Systems; Biometric Systems and Device; Boundary Protection Devices and Systems; Data Protection; ICs, Smart Cards and Smart Card-Related Devices and Systems; Key Management Systems; Multi-Function Devices; Network and Network-Related Devices and Systems; Operating Systems; Other Devices and Systems; Products for Digital Signatures; Trusted Computing
Disponible en: http:\\www.commoncriteriaportal.org.

El proceso de Certificación es valorado desde el RD 03/2010, art. 18, admitiendo que aquellos productos de seguridad de las Tecnologías de la Información y Comunicaciones que vayan a ser utilizados por las Administraciones Públicas serán precisamente valorados cuando tuvieran certificada la funcionalidad de seguridad relacionada con el objeto de adquisición. Debiendo estar dicha Certificación de acuerdo con las normas y estándares de mayor reconocimiento mundial.

2.2.- El Marco de la Excelencia

Las siguientes frases , aunque escuetas, deben recordarnos que en cada apreciación que se expresa acerca del valor añadido de una aplicación software son transportadas informaciones que utiliza el mercado estadístico, por ejemplo:

- aplicación temporal del momento
- tecnologías que han demostrado su rentabilidad
- un plus de marketing
- la sujeción del consumidor a sus respectivas necesidades
- la valoración social del campo en la que se ha decidido invertir la tecnología, por ejemplo, una inmobiliaria
- la linea que el propio mercado informático ha encontrado en su progreso, en este caso, desde aplicaciones destinadas a pequeños electrodomésticos, aplicaciones industriales, aplicaciones de gestión (interacción pública y privada), aplicaciones web, la simbiosis en red de todas ellas, la tecnología móvil de forma concreta
- su estabilidad en el mercado , que en este caso, será un validador certificable de paso de servicio a otra como puede ser la tecnología TDT en un futura HC Mundial

Estas valoraciones pueden ser continuamente incrementadas observando el desarrollo de la *D 31/2000/CE* y *D 34/2002* en relación al Comercio Electrónico y los Servicios de la Información.

Idénticamente se desea una certera y objetiva aplicación sucesiva del art. 9 del *RD 1720/2007* de Tratamiento del dato de carácter personal, en este caso , de salud con fines estadísticos, históricos o científicos, amparándose en la determinación de los fines en la *L 12/1989* , reguladora de la Función Estadística Pública, y la *L 13/1986* de Fomento y coordinación general de investigación científica y técnica, y sus respectivas disposiciones de desarrollo.

El documento que especifica los procesos del sistema de gestión de la calidad, incluyendo los procesos de realización del producto y los recursos a aplicar a un producto, proyecto o contrato específico, puede denominarse *Plan de la Calidad* conforme lo establece la normativa internacional *ISO 9001* en su cuarta Edición del 2008 en relación a *Requisitos de un Sistema de Gestión de la Calidad*. Considerando en su apartado 7.2 que los Procesos relacionados con el Cliente se pueden categorizar por la determinación , primero de los requisitos relacionados con el producto, y segundo, con los requisitos legales y reglamentarios aplicables al producto. En cualesquiera de los casos, manteniendo un PDCA sobre su apartado 7.5.3 en relación a la Identificación y Trazabilidad, el mantenimiento de registros y el control de la identificación única del producto deben garantizar la trazabilidad, de manera que podamos seguir idénticamente aquellas acciones correctivas que se aplicaran a a la eliminación de las causas de las no conformidades del Plan de Calidad.

Recordemos que la adopción de un *Sistema de Gestión de la Calidad* , por ser una decisión estratégica de la Organización no sólo está influenciado por los requisitos del sistema sino , además, por los procesos que emplea. Por ello resulta tan importante la necesidad de considerar los procesos en términos que aporten valor.

Apunta, en caso de complejidades de contrataciones externas, la ISO 9001 que un proceso contratado externamente es un proceso que la organización necesita para su sistema de gestión de la calidad y que la organización decide que sea desempeñado por una parte externa. Sumándose a los controles anteriormente expuestos los siguientes:

> a) el impacto potencial del proceso contratado externamente sobre la capacidad de la organización para proporcionar productos conformes con los requisitos,
>
> b) el grado en el que se comparte el control sobre el proceso,

c) la capacidad para conseguir el control necesario a través de la aplicación del apartado

En relación al término *Procedimiento Documentado* se significa que el procedimiento sea establecido, documentado, implementado y mantenido y que, idénticamente la organización debe establecer uno para definir los controles necesarios para la identificación, el almacenamiento , la protección, la recuperación , la retención y la disposición de los registros (históricos y localizaciones de sus modificaciones). Estas informaciones de entradas a revisión por la dirección debe incluir el estado de las acciones correctivas y preventivas y los resultados de la revisión todas las decisiones y acciones relacionadas con la mejora de la eficacia del sistema de gestión de la calidad y sus procesos. Los registros sólo serán necesarios para proporcionar evidencia de que los procesos de realización y el producto cumplen los requisitos.

Luego ya estamos sobreviendo que la negligencia sobre un proceso puede venir dada por un erróneo Mantenimiento del Procedimiento Documentado, hecho que incide claramente sobre el Seguimiento de un *Documento de Seguridad*, elevando el grado de importancia sobre los Indicadores ya analizados y desarrollados sobre el WP 195 y en relación a las Transferencias.

2.2.1.- Evaluación de la Propuesta

De forma pareja a la supervisión del Control PDCA introducido desde el Marco CAF contemplado por las Administraciones Pública Española, se procede a realizar una evaluación subjetiva conforme al Desarrollo que en torno a dicho control se hubiera ido facilitando a lo largo del Desarrollo de la Tesis, conforme al contenido de sus cuatro capítulos:

- Capítulo I:

  Se considera necesaria la incorporación de un Control (Medida de Salvaguarda) con posibilidad de gestionarse mediante dispositivo físico a fin de concretar el desarrollo obtenido desde la Perspectiva de la *Seguridad del Paciente,* que ve reflejada el manejo y definición de la *Taxonomía* de su Grupo de Ciudadano en el ejercicio de los *Derechos ARCO* y demostrables sus movimientos en el *Sistema Nacional de Sanidad, SNS,* mediante la Tarjeta Sanitaria con la que tiene acceso a su Historia Clínica, HC.

El *e-Técnico* que trabaja en el *SNS* permite precisamente la existencia y mantenimiento de dicha información, por lo que debería poder, de forma gestionada, demostrar sus actividades en el ejercicio de su profesión en el caso de ocurrir una Incidencia, desglosada su actividad tanto lo permita la Gestión del Proyecto del que participa.

- Capítulo II:

Aun cuando reste una mayor Integrabilidad entre los diferentes Sistemas Informáticos Europeos Existentes que manejan un dato clínico, su Operativa deberá resultar diferenciada, y así, por ejemplo, en el caso del IMI podremos incorporar a la colección de Actores que hemos podido extraer de los diferentes Escenarios posibles uno nuevo,el denominado *LISO* que añade al ejercicio del los *Derechos ARCO* la denominada *Privacy Statement,* Clausula de Privacidad, cubriendo la responsabilidad sobre cada Estado miembro.

Respecto a la Elaboración de un *Código Tipo Internacional* sí que existe una unanimidad oficial de la que se fundamenta nuestra legislación en la identificación de los posibles *Actores* y que en el ámbito sanitario cobra especial particularidad por considerar los *Ensayos Clínicos* y la *Farmacolovigilancia* con responsabilidades diferenciadas en el Tratamiento de Datos de Carácter Personal.

El derecho a Monitorear y Supervisar la Trazabilidad del Dato (clausula 6.2.2) se ve incrementada desde la perspectiva de la aplicación de la *ISO 27001* en la consideración de la incorporación de terceras partes o empresas participantes en régimen de 'outsourcing'. Habiéndose clasificado la información en base a su valor, requerimientos legales, sensibilidad y grado crítico para la información. El Monitoreo de los *Niveles de Desempeño* subscritos permitirá visibilizar actividades de Seguridad contemplados por la *Métrica* como es el caso de la *Gestión del Cambio.* Con lo que el Proceso al que dará respuesta el Control deberá mostrar probatoriamente del respeto , por ejemplo, de clausulas consideradas de diferenciación de Niveles de Seguridad en su actuación como son la 12.4.3 (Control al Código Fuente del Programación) y la 12.5.3 (Restricciones sobre los cambios en los Paquetes de Software).

A su vez, el *Esquema Nacional de Seguridad, ENS,* considera que debe existir una clara

diferenciación entre el responsable de la información, el responsable del servicio y el responsable de seguridad. Así mismo, la estrategia de protección realiza la distinción de diferentes *Capas de Seguridad* hábiles sin menoscabo de la protección de sus *Dimensiones de Seguridad* particularizadas: disponibilidad, autenticidad, integridad, confidenciabiliad y trazabilidad.

Se recoge la sugerencia por parte de la *Agencia de Protección de Datos* de implementar una medida proactiva que permita identificar, eliminar, y/o mitigar el impacto de los riesgos asociados en torno a la intimidad de una persona.

La aplicación exacta del estándar *ISO 27002* en el ámbito clínico existe y se denomina ISO 27799, que nos recuerda en su clausula 7.7.10 de Monitoreo que los requisitos que responden a la seguridad del dato clínico son los correspondientes a los de auditoría y de logging, siendo nuestro control si no una respuesta a una auditoría con posible soporte físico a la actividad de 'logging' que deberá ser redefinida en base a este proceso.

El conjunto de *Casos de Uso* debe encontrar su reflejo en la actividad de Logging y consiguientemente de Auditoría y registrable su interacción con el *Ingeniero de Software* al que se le desea elevar la *Seguridad en el Trabajo*.

- Capítulo III:

La deficitaria integración[175] de las operativas a día de hoy de las diferentes partes que puede constar una e-Sanidad más global, da pie a recopilar como *Requisito Informado* y en esta Tesis aquellos aspectos de la Ley que caractericen fuertemente al *SNS* en todas sus áreas y plataformas tecnológicas, apuntando, además, dichas características a posibles *Motivadores en la Gestión del Cambio del SGSI o del SI,* propiamente dicho. Dicha recopilación de requisitos queda soportada por el *Diccionario de Datos* del *SGSI.* Pongamos un ejemplo: Imaginemos que motivado el *Consejo de Consumidores y* que admitidos estos a trámite por la propia *Comisión del Mercado de las Telecomunicaciones, CMT*, consiguieran elevar la necesariedad de distinguir en el conjunto mínimo de información de la *HC* aquellos escaneos de los *Consentimientos Informados* que hubieran tenido lugar en períodos de

175 La difilcultad aparece expresamente invocada en la Ley, i.e. LOPD, art. 32 Códigos Tipo: << En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecerán deberán respetar los principio fijados en aquel >>

hospitalización, más necesarios cuando se procede a tratar el paciente en una cooperación entre C*entros Hospitalarios* que no tienen por qué pertenecer a la misma *Comunidad Autónoma.* Puede suceder que se hubiera considerado alguna Ley más al respecto de las existentes en relación a los *Consumidores*[176] ; o bien que dicha aprobación venga motivada exclusivamente por la Regulación de la propia *CMT*; o por variación de la Ley de dicho *conjunto mínimo*. También pudiera suceder que la propia *Ley de Transparencia* comenzara a distinguir supuestos por áreas de competencia.En cualquiera de estos casos, probablemente constará un *Asiento* del *EVS, Métrica,* correspondiente previo cuya modificación afecte directamente a la orientación de su Diseño, factor que deberá constar conforme a la opción más clara de nuestro discurso, razonando el *Interfaz* y la parte de la *Operativa* por la que se acceda a dichos *Consentimientos Informados* y con qué finalidades. Nuevamente necesitaremos del aporte de nuestro *Diccionario de Datos*, que se irá construyendo conforme se regula la legislación. El *Ingeniero de Software* , por su parte, deberá de poder acceder a la Información actualizada de quién le puede pedir responsabilidad en el Tratamiento del *Dato Clínico*. Es esta una parte del *SGSI* que el *Paciente*, sin embargo, no tiene por qué ver desde su *HC*.

No debemos confundir las *Mediciones* sobre *Indicadores* que se pudieran realizar sobre el Grado de Efectividad que alcanzan las *Medidas de Seguridad* dentro del *SGSI*, y que muy bien aparecen apuntadas por la norma *ISO /IEC 27004*[177], con los 'Indices' que pudiéramos aplicar a un *Documento de Seguridad* para expresar su Especificación y aplicable a algún

176
- Ley de Cesación de Servicios Sociedad de la Información , L 34/2002
- Derechos y Obligaciones del Paciente en la HC, L 11/2002
- Consejo de Consumidores, L 32/2003
- Procedimiento de Actualización del SNS, L 1030/2006
- Procedimientos de Resolución Judicial, L 56/2007
- Derechos Usuario en relación con las redes y los servicios de comunicaciones electrónicas, D 2009/136/CE
- Resolución de Litigios Transfronterizos, ORECE, D 2009/140/CE
- Conjunto Mínimo de Datos de los Informes Clínicos en el SNS, RD 1093/2010
- Aplicación de los Derechos de los Pacientes en la Asistencia Sanitaria Transfronteriza, D 2011/24/CE
- Ley de la Transparencia, L 19/2013
- Defensa de los Consumidores y los Usuarios, L 3/2014

177 Continuando con la invocación que se practica de la aplicación de la *Guía CCN-STIC nº 815* en relación a *Métricas e Indicadores del Esquema Nacional de Seguridad*, apreciamos un ejemplo de Publicación por parte del Subdirector Adjunto de Coordinación de Undades TIC , Dirección de Tecnologías de la Información y las Comunicaciones y en respuesta a emitir un *Informe del Estado de Seguridad de las Administraciones Públicas* , una vez desplegada la herramienta INES en 2014 que facilita precisamente la recogida y consolidación de la información que facilita la emisión de dicho informe, y conforme a los parámetros del ENS, RD 03/2010. AMUTIO, Miguel Angel. "El Esquema Nacional de Seguridad, cinco retos próximos". Boletic 73. Fundación ASTIC. Revista de la Asociación Profesional de los Cuerpos Superiores de Tecnologías de la Información en la Administración. Mayo 2015

Caso o nueva Medida de Seguridad nueva a analizar, como bien apuntamos primero en el apartado Cap. III. 11, y segundo en el apartado Cap.IV.1.1.

- Capítulo IV:

En la Categorización de la *Delegación de Responsabilidades* en torno al trabajo que se realiza respecto al Tratamiento de Datos en la *HC*, contamos por una parte con las sugerencias del Grupo de Trabajo *Gt29* correspondiente a la *D 95/46/CE* recopilado en su *Documento WP 195*, donde separa claramente las funciones del *Controlador* y el *Procesador* , sin dejar de recordarnos que aplicado al marco de las Transferencias Internacionales debe de adaptar, además, el Nivel de País y el del Mantenimiento Técnico, por lo que como Funcionalidad diferenciada da lugar a la observación de 4 Niveles Mínimos de Seguridad de Aplicación al Dato en la *HC*, y debiendo ampliar a los *Requisitos Informados* recopilados en el Capítulo II, esta consideración. Debemos recordar que aun cuando no existiera formalmente más que un único responsable en el Marco de las Transferencias Internacionales, estas funciones deben resultar diferenciadas.

2.2.2.- CAF, Common Assesment Framework

Desde el punto de vista de la Evaluación, Reconocimiento y Acreditación de la Excelencia el *Modelo EFQM*[178] propone animar a las organizaciones a que apliquen los valores recogidos por la Carta Social Europea y el Pacto Mundial de la ONU, permitiendo una actividad socialmente responsable y sostenida en todas sus operaciones.

Esta nueva versión del *Modelo EFQM*, Marco Común de Evaluación, y que en su aplicación a las Administraciones recibe el nombre de *CAF*[179], *Common Assesment Framework*, se constituye como

178 En los Fundamentos del Modelo EFQM se encuentra un esquema lógico que se denomina REDER, en inglés RADAR y está formado por cuatro elementos que sintetizan los que una organización necesita realizar: Resultados, Enfoque, Despliege y Evaluación -Revisión. La autoevaluación permite que los componentes de una organización se comparen con un modelo. Permite distinguir los puntos fuertes y áreas de mejora.El modelo presenta una escala de puntuación por cada uno de los criterios y subcriterios. En su nueva versión Modelo EFQM-2013 no presenta cambios en los enunciados de los 9 Criterios o de los 32 subcriterios, por ello las organizaciones que vayan a realizar sus autoevaluaciones o estén redactando una memoria a fin de solicitar una evaluacion externa no se verán afectadas por la nueva versión

179 Agencia Estatal de Evaluación de las Políticas Públicas y la Calidad de los Servicios, AEVAL. "Mejora de las organizaciones públicas por medio de la autoevaluación", CAF 2013. Ministerio de Hacienda y Administraciones

una herramienta de gestión de la Calidad Total desarrollada por y para el sector público y fundamentada en el *Modelo de Excelencia de la Fundación Europea para la Gestión de la Calidad*, facilitando el benchlearning o aprendizaje entre las organizaciones del sector público.

Una de las importantes novedades que introduce CAF 2013 es la de *Gestionar con Agilidad* sustituyendo al tradicional Gestionar por Procesos en cuanto que la estructura de procesos tiene que ayudar a responder de forma eficaz, eficaz y ágilmente ante los posibles Escenarios futuros, anticipando el entorno en el que tendrá que participar una Organización, introduciendo en el entorno de crisis, incertidumbre y volatilidad, entre ellos, la responsabilidad ante terceros y la transparencia.

El enfoque holístico de la gestión de la calidad total no significa que el conjunto de los aspectos del funcionamiento de una organización son evaluados detenidamente, sino que todos los elementos que la definen presentan un impacto recíproco entre sí.

Las Organizaciones que han usado CAF de una forma eficaz, pueden recibir el certificado de *Usuario Eficaz del CAF* válido durante dos años. El proceso de retro alimentación externa CAF y el 'Certificado de Usuario Eficaz CAF' están bajo la responsabilidad de los Estados Miembros, siendo el *Instituto Europeo de Administración Pública , EIPA* el encargado de la Coordinación de la Red y Gestión de su sitio Web.

A la recopilada noción de transparencia a lo largo de la Tesis, hemos de sumarle una más , precisamente la que recoge el método de Calidad Total que se aplica en las Administraciones, CAF. Propone un método de Autoevaluación voluntario que nos va a permitir generar una visión mucho más holística acerca de la Propuesta presentada en el Capítulo IV y su consiguiente Observación desde diferentes perspectivas. Para ello podemos invocar un pequeño esquema del conjunto de sus Criterios, Subcriterios y Observaciones de Agentes:

Públicas.

CRITERIO	SUBCRITERIO	Invocación de Agente
1. liderazgo	1.1. dirigir a la organización desarrollando su misión, visión y valores	• desarrollar un sistema de gestión que prevenga comportamientos no éticos, a la vez que apoye al personal que trata con dilemas éticos; dilemas que aparecen cuando distintos valores de la organización entran en conflicto • gestionar la prevención de la corrupción identificando potenciales áreas de conflictos de intereses y facilitando directrices a los empleados sobre como enfrentarse a estos casos
2.estrategia y planificación	2.1. reunir información sobre las necesidades presentes y futuras de los grupos de interés así como información relevante para la gestión	El ciclo PDCA(planificar, desarrollar, controlar, actuar) juega un papel importante en el desarrollo y la implementación de la estrategia y planificación de una organización pública. Empieza recopilando información relevante sobre las necesidades actuales y futuras de los grupos de interés relevantes, sobre productos y servicio (outputs) e impacto (outcome) y sobre las evolución del entorno externo. Esta información es indispensable para apoyar los procesos de planificación estratégica y operacional. También es fundamental para dirigir las mejoras planificadas en el desempeño de la organización (para poder ser ejecutada con éxito, la estrategia tiene que plasmarse en planes, programas, objetivos operativos y medibles. La supervisión y la dirección tiene que formar parte de la planificación así como estar atentas a las necesidades de modernización e innovación que soportan a la organización en la mejora de su funcionamiento. Monitorizar de forma crítica la implementación de la estrategia y de la planificación nos permitirá actualizarlas y adaptarlas a cuando sea necesario)
3.personas	3.3. involucrar a los empleados por medio del diálogo abierto y del emponderamiento, apoyando su bienestar	se pretenden romper con los silos organizativos generando sugerencias para mejorar los resultados, usando estos para realizar mejoras y considerándose a su vez estas como buenas prácticas
4. alianzas y recursos	4.1 desarrollar y gestionar alianzas con organizaciones relevantes	Las organizaciones públicas son vistas como parte de una cadena de organizaciones que juntas, trabajan en pro de un resultado específico para la ciudadanía, considerando que la calidad de cada una de estas alianzas tiene u un impacto directo sobre los resultados de la cadena. 5. Identificar las necesidades de alianzas público-privadas , APP, largo plazo y desarrollarlas cunado sea apropiado.
	4.3 gestionar las finanzas	Aunque las organizaciones tienen a menudo muy poco que decir sobre la asignación de recursos, se debería prestar mayor escrupulosidad en la preparación de presupuestos
5. procesos	5.2 desarrollar y prestar servicio	3. involucrar a a estos y a otros grupos de interés

	orientados a los ciudadanos/cliente	en el desarrollo de los estándares de calidad para los servicios y productos, que respondan a sus expectativas y sean gestionables por la organización 5. involucrar a estos en el diseño y desarrollo de nuevos tipos de servicios interactivos, de entrega de información y de canales de comunicación eficaces.
	5.3 coordinar los procesos en toda la organización y con otras organizaciones relevantes	7.crear una cultura para trabajar transversalmente en la gestión de los procesos, saliendo de los compartimentos estanco
6. resultados	6.2 mediciones de resultados	En relación con la transparencia de la prestación de servicios y productos: . número de canales de información . disponibilidad y precisión de la información . disponibilidad de los objetivos de rendimiento y resultados de la organización . número de actuaciones del Defensor del Pueblo . alcance de los esfuerzos para mejorar la disponibilidad, precisión y transparencia de la información .resultados de los indicadores sobre la calidad de los productos y la prestación de servicios : .número y tiempo de procesamiento de las quejas . número de ficheros devueltos con errores o casos que necesiten repetir el proceso . cumplimiento de los estándares de servicio publicados, por ejemplo, requerimientos legales
7. resultados de las personas	7.2 mediciones de desempeño	el criterio distingue dos tipos de resultados: las mediciones de excepción en las que las personas son preguntadas directamente y las mediciones de desempeño, utilizadas por la organización para monitorizar y mejorar la satisfacción de las personas y sus resultados. Los resultados suelen incluir mediciones internas del comportamiento de las personas en la práctica

Tabla 8. CAF 2013- Perfil de Protección ISW

Es el camino de la excelencia organizacional el que conduce a una correcta percepción del desarrollo y comunicación social de la Transparencia y de igual manera que resulta difícil extraer la conclusión de que le manejo del *Documento de Seguridad* deba dejarse mayormente a la Calidad que obtenga cada Responsable de Seguridad, esta Calidad debiera ser parametrizada en base a la percepción y desenvolvimiento que supone la observación y análisis que proporcionan los Informes publicados por las Agencias Reguladoras en cada país, por ello consideramos necesario expresar estos Indicadores y un ejemplo de su aplicación.

Ahora bien, no incurramos en el error retórico de concluir que el objetivo tercero del Modelo EFQM de Gestión de la Calidad en su tercera versión y que dice así: “facilitar la autoevaluación de una

organización pública con el fin de obtener un diagnóstico y definir acciones de mejora" nos haga ver que existe una relación dependiente entre la aplicación de una solución ISO 27 001 en método de autoevaluación, sino que en este caso, y por tratarse de los Servicios Informáticos de la Administración Pública se ha de reconocer la independencia del Esquema de Auditoría, pues de otra forma no resultaría objetiva la Propuesta.

Como enfoque holístico del análisis del rendimiento de la organización, la estructura de nueve criterios identifica los principales aspectos que deben ser considerados en el análisis de cualquier organización; los enumerados del 1 al 5 se refieren a las prácticas de gestión de una organización, denominados agentes facilitadores y determinan lo que hace una organización y cómo enfoca sus tareas para alcanzar los resultados deseados; los enumerados del 6 al 9 como resultados alcanzados en áreas de ciudadanos/clientes, las personas , la sociedad, la responsabilidad y las claves del rendimiento se miden por indicadores de percepción y de desempeño. Siendo los subcriterios expuestos como ejemplos que explican su contenido con más detalle sugiriendo posibles áreas donde se estudia cómo la organización alcanza los requisitos expresados en el subcriterio, y basados en una buena cantidad de buenas prácticas. En la integración de las conclusiones de la autoevaluación de los agentes facilitadores y de los criterios de resultados en las prácticas de gestión se constituye la innovación continua y el ciclo de aprendizaje que acompaña a las organizaciones en su camino hacia la excelencia. En ocasiones, percibiremos que una interacción-relación sustancial se materializa al nivel de subcriterio.

Normalmente, se considera que el CAF es una medición de base cero y el modelo indica las áreas en las que esencial empezar a medir. Literalmente confirma el documento que cuanto más progresa una administración hacia la mejora continua, más sistemática y progresivamente estará recogiendo y gestionando información, tanto interna como externamente.

Nos recuerda la aplicación del *Esquema Nacional de Seguridad*, en su art. 43 RD 03/2010, que la valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

2.3.- Ingeniería de Software basada en Componentes

La práctica de no desdecir en ningún momento el planteamiento del primer capítulo conduce a establecer analogías en el desarrollo de la Tesis sin olvidar ambas *Taxonomías*. De este modo, y encontrando suficientemente desarrollada el Área de *Seguridad del Paciente*, se plantea una propuesta defendida y defendible tanto en el Área de la Excelencia como de las normas ISO/IEC convenidas a tal fin en el Área de *Seguridad del Trabajo* para el *Ingeniero de Software*.

Se trata , sin más, de una solución que nos permite cubrir una laguna dentro del ámbito de una Prueba Judicial y que no viene sino a proteger el Derecho al Trabajo del Ingeniero de Software en el área de protección de datos respetando como guía el de la Sanidad Electrónica o *e-Salud*. Existiendo su correspondencia, y no siempre tan extendida, para la Categoría del Asistente con Categoría Profesional Sanitaria cuando se resuelve el Diseño del Hardware en una Tarjeta de Lectura.

Configuraciones más complejas que tratarán de analizarse y presentarse de una forma más universal, determinarán considerando una colección de criterios y subcriterios, en el *Marco de la Excelencia* si el coste y la Configuración de cada Proyecto Software no se desdicen de ampliar la Propuesta con sus tres Procesos descritos.

Desde la parte de la *Ingeniería del Software* y como representación abstracta de un proceso de software desde una perspectiva particular se introduce un *paradigma de proceso* o modelo de proceso denominado *Ingeniería de Software basada en Componentes* basándose en la existencia, normalmente, e integración de componentes. Intentando superar la situación inicialmente deseable que el *Desarrollo Orientado a Objetos* hubiera deseado encontrar en su reutilización externa.

Un *Componente software* se caracteriza en la cualidad de separar su Implementación de su Interfaz resaltando la cualidad de poder reemplazarse sin cambiar el sistema y destacando su fundamento independiente. Además, cuando los componentes cumplen con los estándares (cómo se comunican entre sí) , se podrá garantizar la independencia de su funcionamiento en relación a un lenguaje de programación.

Un planteamiento que se ha venido en discutir queda manifiesto en la presentación de la Propuesta "Perfil de Protección del Ingeniero de Software", y en relación a su posible certificación[180]: se ha

180 SOMMERVILLE Ian. Ingeniería del Software. Ed. Pearson-Addison-Wesley. 7ª ed. 2005. Cap. 19

propuesto que asesores independientes deberían certificar los componentes para asegurar a los usuarios que los componentes son confiables (reliability), sin quedar del todo claro cómo debería hacerse esto, porque

- ¿quién pagaría la certificación?
- ¿quién sería responsable si el componente no funciona de acuerdo con la certificación?
- ¿cómo podrían los certificadores acotar su responsabilidad?

Siempre que el componente responda a una certificación formal no debería conllevar ninguna otra dificultad.

Reiterando en subrayar sus características de logros incidimos en considerar:

- reutilización de sw (software reuse)
- reducción del coste de mercado(reduced time-to-market)
- interoperabilidad (interoperability)
- facilidad de certificación de la Calidad(ease of quality certification)

Uno de los primeros pasos que se ha de dar en el Diseño de un Componente Software es la reutilización de otras partes del Sistema sin que suponga una carga en las transacciones y cuyo hilo de proceso resulte perfectamente distinguible.

Precisamente cuando nos acercamos a un Sistema tan complejo, y podemos situarnos en nuestro ejemplo sin tener que recurrir a otro pues desdibujaría el estado de arte actual de la Administración Electrónica, consideramos que al menos deberíamos realizar una aproximación a los Modelos de Datos o Repositorios de las Unidades de :

- Recursos Humanos
- Gestión de Proyectos

- Gestión de Perfiles

- Gestión de la Configuración

- Departamento de Incidencias

En esta tesitura ya resulta obvio el recordar que probablemente estamos intentando dar respuesta a un problema de Ingeniería de Software con una ya larga trayectoria iniciada en un modelo secuencial como el de cascada y sobreescrito por otros modelos iterativos y/o evolutivos como los incrementales, prototipados, el de espiral, etc,.

Efectivamente, y puesto que partimos en el inicio del Diseño del Componente del uso del conocimiento que se tiene del dominio, y en relación al mantenimiento y considerando que se cuenta con diferentes componentes con ciclo de vida independientes, pudieran aflorar cuestiones legales en caso de que el sistema fallare.

Una información que el Administrador del Sistema tiene hábil y visible en todo momento y que se puede extender, debe hacerse partícipe de una forma visible y clara al Ingeniero de Software de forma que pueda cotejar su situación en cada momento en relación a su actuación en un determinado proyecto, y pudiendo presentar y defender bien respecto de su Empresa en Outsourcing, bien ante el propio Administrador del Sistema.

A continuación esbozamos el esquema lógico de dificultad que un ISW puede tener en mente:

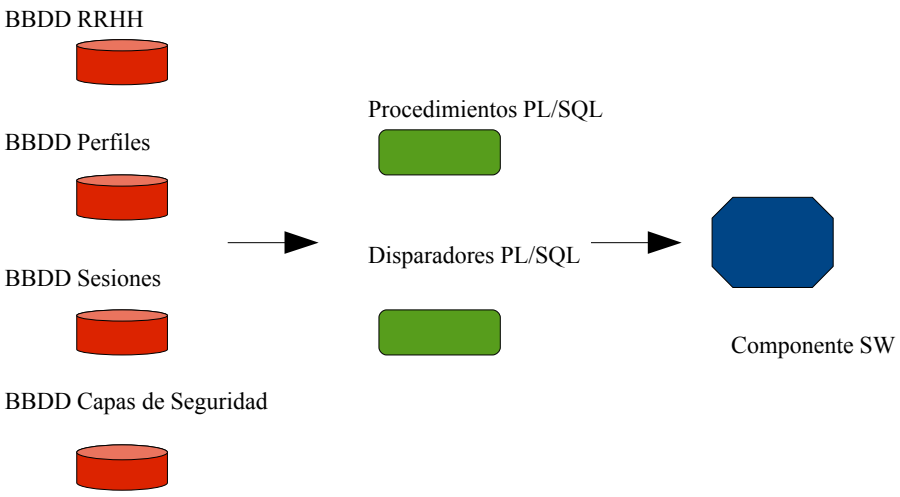


Figura 1. Perspectiva Lógica del ISW

El Punto Crítico en la elaboración del Componente Software reside en la *Especificación de un Hito de Proyecto*, y que como hemos indicado será configurable para el ISW y en relación a los Perfiles de Acceso, las Sesiones de Trabajo y las Capas de Seguridad que se le aplicaran.

Internamente al Componente Software recibe como Entradas todos estos datos y como Salidas una representación gráfica de la situación de los datos cruzados en cada momento. Además de la tradicional supervisión del Administrador del Sistema, contaremos con el seguimiento desde Gestión de Proyectos y desde el Departamento de Incidencias, debiendo completarse conforme discurra el Proyecto con el Cuadro de Incidencias que se vaya considerando documentar a fin de una mejora de la evolución del Proyecto quedando de esta forma claro que el Seguimiento que se debe practicar ha de resultar continuo.

Configurable el Hito y configurable la Incidencia desde una redacción textual hasta un detalle decidido desde la Sección de Soporte y ya existente, se trata tan sólo de hacerla visible y representable, pudiendo manejarse en las Sesiones de Trabajo, previo a emprender nuevas decisiones, abriendo una discusión acerca de la ralentización de procesos y de cómo afectan unos a otros, lo cual no nos conduciría sino a una Optimización de todo el Sistema.

La determinación máxima de abstracción del Componente permitirá tratar de idéntica manera a la

Información de las Sesiones como a las de las Capas de Seguridad, permitiendo dicha abstracción el inicio de su representación visual como recurso gráfico y vinculable a las decisiones del Usuario. Es en este punto donde se debe recordar que ya existen estándares de tecnologías que permiten la comunicación entre componentes, sin tener que recurrir a Diseño completo de una nueva.

Es precisamente el elemento de *disponibilidad* el que permite la caracterización del éxito de la Ingeniería de Software basada en Componentes, *ISBC* y que suele denotarse como *middleware*[181].

Por su parte, la *Especificación OMG del Lenguaje de Modelado Unificada*[182], define un componente como una parte modular, desplegable y sustituible de un sistema que incluye la implantación y expone un conjunto de interfaces.

Es precisamente dentro de la arquitectura del software cunado se necesita un componente desde un punto de vista tradicional (no orientado a objetos y no relacionado con el proceso) también llamado *módulo* que incluye las siguientes funciones:

1. como componente de control, coordinando las invocaciones de los demás componentes del dominio del problema

2.como componente del dominio del problema

3. como componente de infraestructura y que es el que tratamos de ofrecer a continuación para ayudar a clarificar la exposición.

2.4.- Gestión de Proyecto

La Guía utilizada para la presentación de la Sección Gestión del Proyecto se corresponde con la Semántica utilizada en el *PMBok*[183].

Partimos de la premisa de que un riesgo es un evento que, de producirse, produce un efecto negativo

181 OMG CORBA, Microsoft .COM, Microsoft .NET, Sun JavaBeans

182 PRESSMAN Roger. "Ingeniería del Software: Un Enfoque Práctico". 7º ed. 2010. University of Connecticut. Cap. 10., (pag. 234)

183 Project Management Institute, PMI, Norma Americana Nacional ANSI. "PMBOK, Guía de los Fundamentos de la Dirección de Proyectos." 3º Edición., 2004, pag. 70- 199, cap. 7, cap. 11

sobre, al menos, un objetivo del proyecto, como tiempo, coste, alcance o calidad; puede tener una o más causas, y si se produce uno o más impactos.

El riesgo del proyecto tiene su origen en la incertidumbre que está presente en todos los proyectos. Los riesgos desconocidos no pueden gestionarse de forma proactiva, y una respuesta prudente del equipo del proyecto puede ser asignar una contingencia general contra dichos riesgos.

Si consideramos, que la legislación y su ejercicio de derecho sobre la naturaleza del dato médico o de cualquier otro dato que la administración pueda manejar del ciudadano, debe ser igualmente ejercido sobre los tres grupos taxonómicos que se razonan en el Capítulo I, debemos tener presentes que las interrelaciones pueden resultar complejas en la justificación de la veracidad de un dato, donde pueden quedar implicados los tres grupos . Considerando, como hemos venido razonando, la mayor carga de trabajo que le queda al legislador es la profundización sobre el grupo denominado Ingenieros de Software, este debería poder, sin que le supusiera mucho esfuerzo, justificar la labor de su tarea (el estado real) en cada momento de su actividad diaria. El riesgo sería, por ejemplo, no poder demostrar su acción y resultados en entornos de traspasos según se van superando hitos demostrables, y en consecuencia, y mucho más allá de no poder demostrar que ha cumplido su tarea de custodia correcta del dato de carácter personal, incurrir en una trampa que el no ha preparado como consecuencia de negligencia de control de Supervisión del Responsable de la Sección sobre Empresas Privadas que pueden cooperar en una misma Unidad de la e-Administración.

ejemplo.riesgo: prueba deficiente de hito

ejemplo.impacto: inconclusión proyecto-software
contingencia-general: CAF 2013

Sobre el proyecto implementado en la Tesis se ha llevado a cabo un “Análisis de Sensibilidad” que ayuda a determinar qué riesgos tiene el mayor impacto, examinando la medida en que la incertidumbre de cada elemento del proyecto afecta al objetivo que está siendo examinado, cuando todos los demás elementos inciertos se mantienen en sus valores de líneas base.

Al desarrollar el Acta de Constitución del Proyecto, se deben tener en cuenta todos y cada uno de los factores ambientales de la empresa y de los Sistemas de Información que estuvieran relacionados con el éxito del proyecto o pudieran influir sobre él de alguna manera. Esto, incluye, entre otros,

conceptos como los

Sistemas de Autorización de Trabajo de la Compañía

quedando en evidencia temas como la tolerancia al riesgo de los trabajadores. Es precisamente el Sistema que deseamos implementar aunque probablemente ya podamos extraer cada uno de los activos que se usan para ejercer influencia sobre el éxito del proyecto de los propios procesos existentes de la organización, a saber:

- procesos y procedimientos de la organización para realizar el trabajo

- procedimientos para la gestión de polémicas y defectos

La palabra *Identificación de la Configuración* dentro del Proceso de Control presenta su propia definición: suministra la base a partir de la cual se define y verifica la configuración de productos, resultados o salidas, se clasifican estos, se gestionan sus cambios y se mantiene su contabilidad.

De modo, que, dentro del Control del Alcance debemos considerar en dos ocasiones la palabra alcance:

- *el alcance del proyecto*: el trabajo que debe realizarse para entregar un producto, servicio o resultado con las funciones características especificadas

- *el alcance del producto:* las características y funciones que caracterizan a un producto, servicio o resultado

Considerando que el *Plan de Gestión del Alcance del Proyecto* incluye, entre otros:

- un proceso que especifica cómo se obtendrá la verificación y aceptación formal de los productos entregables completados del proyecto

En ocasiones puede que no resulte posible la descomposición de un producto entregable o subproyecto que se logrará a muy largo plazo. Normalmente, el equipo de dirección del proyecto

espera hasta que se aclare el producto entregable o subproyecto, de modo que pueda desarrollarse los detalles del *Desglose del Trabajo* o *EDT*, técnica conocida como Planificación Gradual. Para llegar a un Esfuerzo de Trabajo fácil de manejar, es decir un Paquete de Trabajo sólo debe descomponerse hasta el nivel siguiente.

El documento generado por el proceso que respalda la EDT se denomina *Diccionario de la EDT* cuyo contenido incluye los *Paquetes de Trabajo* y las *Cuentas de Control*. El Diccionario de la EDT es un componente de la definición del alcance del proyecto detallado y se usa para verificar que los productos entregables que se están produciendo y aceptando están comprendidos dentro del alcance del proyecto aprobado.

Una posterior *Análisis de Variación* nos puede indicar entre los aspectos importantes de control del alcance del proyecto la determinación de la causa de la variación relativa a la línea base del alcance y decidir si son necesarias acciones correctivas.

Por su parte, recordar que en una Cuenta de Control se puede ubicar un punto de Control de Gestión de la estructura del desglose de trabajo por encima del Paquete de Trabajo. En definitiva, probablemente antes de tomar la decisión de la aplicación del Seguimiento del Marco de Excelencia,la cuenta de Control deberá ser consensuada y aprobada desde la Contabilidad del Organismo de la e-Administración donde se vaya a llevar a cabo esta Presentación.

Va a ser el Paquete de Planificación como componente de la EDT ubicado por debajo de la Cuenta de Control , pero por encima del Paquete de Trabajo el que se utilizará para planificar el contenido de trabajo conocido que no tiene actividades del Cronograma detalladas, como es el caso presentado de la propuesta CAF 2013.

Si en la Cuenta de Control se incluyen las estimaciones de Costes para los Paquetes de Planificación, entonces se incluye el Método para preparar su presupuesto.

Y como bien se atestigua, lo requisitos de riesgo con implicaciones contractuales y legales pueden incluir la salud, la seguridad personal y material, rendimiento, el medioambiente, los seguros, los derechos de propiedad intelectual, igualdad de oportunidades de trabajo, licencias y permisos.

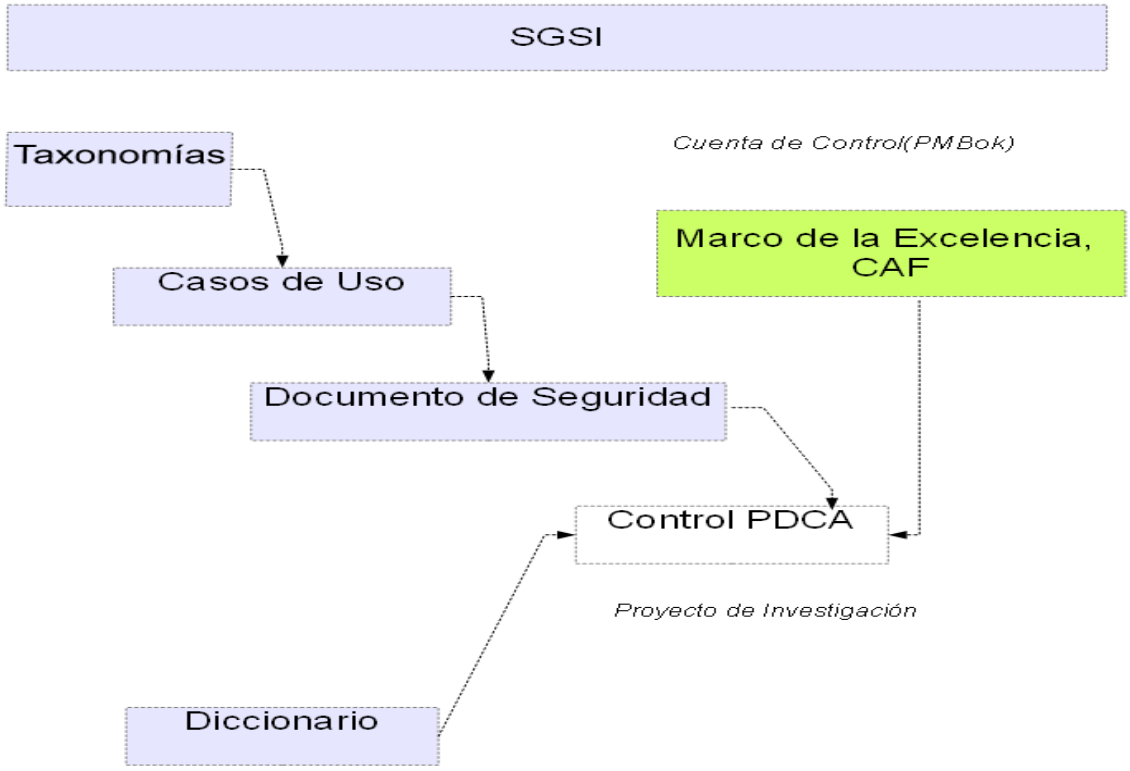


Figura 2. EDT, Desglose de Trabajo

, y donde cada *Paquete de Trabajo* cuenta con el siguiente Desglose de *Tareas*, conforme hemos ido relatando a lo largo del Desarrollo de la Tesis:

Paquete de Trabajo: 1. TAXONOMIAS
Tareas:

1.1. Estudio Histórico de la Privacidad
1.1.1. Identificación Grupos Taxonómicos
1.1.2. Desarrollo de Taxonomías

Paquete de Trabajo: 2. CASOS DE USO
Tareas:

2.1. Análisis de Códigos de Buenas Prácticas y Regulaciones
2.1.1. Identificación de Actores y Escenarios
2.1.2. Gestión del Riesgo:
2.1.2.1. Líneas de Implementación de Mayor Riesgo ISO/IEC 27002
2.1.2.2. Definición de Tecnología en Medida de Seguridad: EIDP

Paquete de Trabajo: 3. DICCIONARIO
Tareas:

3.1. Estudio de Legislación asociada a la HC
3.1.1. Identificación de Activos
3.1.2. Estudio de Viabilidad, Gestión del Cambio (Métrica): motivadores del Cambio

Paquete de Trabajo: 4. DOCUMENTOS DE SEGURIDAD
Tareas:

4.1. Documentos-Guía AEPD
4.1.1.Identificación de Indicadores y muestra de discurso de empleo

Paquete de Trabajo: 5. CONTROL PDCA
Tareas:

5.0.Articulo 2 como Verificador de su Hilo conductor
5.1.Aplicación de Indicadores a las Bases de Datos
5.2. Aproximación del Documento WP 195 al desequilibrio encontrado en el Desarrollo de las Seguridades de los Grupos Taxonómicos Publicados, Articulo 1)
5.3. Especificación de Medida de Seguridad o Control en el lenguaje de los Controles de la ISO 27002
5.4.Aplicación del Marco de Excelencia, CAF
5.5.Gestión del Proyecto SGSI

CONCLUSIONES

Considerando que deberemos reforzar toda aquella consideración en torno a la Protección de Datos en el Area Clínico-Asistencial, se despliegan las posibilidades de invocación del instrumento jurídico reconocido en el RD 1720/2007 y denominado 'Documento de Seguridad' en el Indice expuesto.

Sírvanos la norma no certificable ISO/IEC 27002 de aplicación de controles de la norma sí certificable ISO/IEC 27001 como esquema de Lenguaje de Auditoría en el *Sistema de Gestión de la Seguridad de la Información* que impulsan y que se va desenvolviendo:

- Capítulo I:

Recopilación histórica de todos los trabajos realizados en torno a la Privacidad, aportando una Publicación en torno a dos de los tres Grupos Taxonómicos resultantes del Estudio de los Usuarios de la Administración Electrónica en la Sanidad o e-Sanidad,

a)el Ciudadano-Paciente

b)el Asistente Sanitario

c)el Técnico Informático

Consideramos la *Seguridad del Paciente* razonablemente bien desarrollada y practicada en la e-Sanidad, identificándose con su *Tarjeta Sanitaria;* el Asistente Sanitario con bien definidos *Códigos Tipo* registrables en la *Agencia de Protección de Datos,* y con la Salvaguarda efectiva de *Tarjetas Profesionales* que permiten gestionar de forma auditable los accesos por Perfiles de Categorías; y el denominado *Ingeniero de Software* que aglutinando también una diversidad de Perfiles Profesionales adolece de una cobertura jurídica equiparable a la anterior, por lo que comenzamos el Trabajo de la Tesis desarrollando su Taxonomía en el ámbito de la Protección de Datos de la Historia Clínica.

- Capítulo II:

Recopilación fundamentada en documentos emitidos por Organismo oficiales así como en legislación tanto de Actores como de Escenarios (clasificación en el Estado del Arte), que reconocen legalmente Sistemas Informáticos Europeos con especial tratamiento en relación a la Protección de Datos de Carácter Personal con extensión hasta la e-Sanidad. Se consideran posibilidades abiertas como las del *Sistema Europeo de Alertas* por considerar este tipo de datos de carácter especialísimo con vistas a futuras investigaciones y prácticas de Interoperabilidad cuya trayectoria no deberá ser desdicha. De su texto, se origina una segunda Publicación , habiendo querido reforzar la idea de que la conocida disertación "autodeterminación informática vs. Libertad informativa" no encuentra un nuevo caldo de cultivo considerándose el ámbito Farmacovigilante-Sanitario (público o privado), sino como el que mejor reconoce su faceta en relación al "consentimiento informado", y principio fundamento estrella en la Taxonomía del Paciente.

Retomando el hilo conductor que se indica al final de la Exposición de la Introducción, el desarrollo de implementación de controles de la norma ISO/IEC 27001 en la norma ISO/IEC 27002 no tienen otro objetivo que lo indicado por su clausula 4: esto es, de Análisis, Diseño, Desarrollo y Mantenimiento de un Sistema de Gestión de Seguridad de la Información elevando, en cualquier caso, el tratamiento que se hace del 'Riesgo' como bien formulan los modelos más desarrollados de la Ingeniería del Software.

En este horizonte extraemos y apuntamos aquellos controles que nos permitirán identificar semánticamente hacia donde deberemos orientar nuestra mirada por el grado de dificultad de objetivos, y elevación de la amenaza del Riesgo.

Así mismo, y muy acertadamente , se perfila, si se encontrara, un posible tipo de Solución de Salvaguarda Técnica reconocido como EIDP por la Agencia de Protección de Datos o como PIA, por la literatura internacional., y que reconoce la resolución de una *Incidencia* en el Marco de la Protección de Datos, después de valorado su *Impacto*.

Como se demuestra en el Capítulo IV ambas posturas nos ayudan en la definición de un nuevo Control ante un problema localizado dentro del SGSI. En concreto, este control reconociendo el Ciclo de Deming o PDCA propuesto por la OCDE en la norma ISO/IEC 27001, Anexo A, se desglosa invocando precisamente controles de la norma ISO/IEC 27002, lo cual no es una contradicción , sino fruto de la aplicación del PDCA en la superación del riesgo detectado

- Capítulo III:

Los *activos legales* extraídos de la propia legislación en la jerarquía ordenada que se las reconociera encuentran en el *Documento de Seguridad* su máximo exponente en lo que respecta al Tratamiento de Datos de Carácter Personal, y así mismo en el Marco de la e-Sanidad. A excepción de la Legislación y de los documentos emitidos por las Agencias Nacionales de Regulación, en este caso, *Agencias de Protección de Datos,* con distinciones por Comunidades Autónomas , se ha escrito bien poco al respecto, deseando contribuir al conocimiento que entraña este instrumento jurídico, siendo éste auditable tanto por el anterior Organismo como por el *Centro Nacional de Inteligencia*, y que idénticamente cuenta con sus respectivas *Guías.*

Precisamente , como instrumento, y sin forzar su resultado, se observa que debe de encontrar su sitio en la *e-Aministración*, lo cual nos llevaría a hablar de la Administración Electrónica del *Derecho Informático*, por ejemplo. Esta idea no se desdice del Contexto del *SGSI* en el que nos estamos moviendo, por cuanto se puede considerar parte de él.

En tal perspectiva, y al menos, aconsejamos localizar su identidad en el *Diccionario* del *SGSI*, y con vistas a desarrollar otro tipo de actividad, como se documenta en el expuesto *Estudio de Viabilidad del Sistema* apoyándonos en *Métrica* v3, registrando la G*estión del Cambio* en un *Documento de Seguridad* por medio de un Anexo (conforme propone la Agencia Española de Protección de Datos), encuentra idénticamente su contenido en la relación de legislación con Nota indicativa del Cambio , propuesto también por el índice 15.1.1 de la ISO 27002 y, que se propone acompañe al Documento denominado *Política de*

Seguridad del SGSI.

Pensando en el modo en cómo hablaremos de un 'Documento de Seguridad' cuando decidamos analizar una EIDP con lenguaje de controles ISO/IEC 27002 extraemos unos Indices Semánticos de las propias Guías emitidas por la Agencia de Protección de Datos, y que en esta Tesis encuentra dos expresiones, al menos, en diferentes capítulos III y IV, respectivamente:

- una genérica, en relación a la Figura del *Documento de Seguridad*

- una concreta, focalizando la atención sobre el Soporte BBDD, Base de Datos, debido a la conclusión de que los datos, i.e., en una Transferencia Internacional precisan de ampliación de atención y cuidado

- Capítulo IV:

Se realiza una recopilación de todas las aportaciones que se van identificando en torno al *SGSI* a lo largo de la Tesis y en el Contexto de la *e-Sanidad*. La definición de *Actores* y *Taxonomías* nos ayudan a la concrección de los denominados 'Casos de Uso' , y que por decirlo de forma simplificada , identifica la interacción del Usuario con el Sistema, hábil en una 'Impugnación de Valoraciones'.

La alimentación que va produciéndose en el *Diccionario* de Datos en la faceta de Gestión Documental del *SGSI*, tanto por los activos legales como por los Motivadores de un Cambio (hipotético, actualizable, correctivo), nos ayuda a mantener nuestro SGSI actualizado, sirviendo de Soporte tanto para la *Política de Seguridad* como en la Auditoría Legal.

La materialización de la idea de que si encontramos un desequilibrio suficientemente apreciable en el Desarrollo actual de la e-Sanidad en el Tratamiento de Datos de Carácter

Personal, debe orientarse por una solución EIDP: ya desde el desarrollo de las Taxonomías queda fundamentado su esbozo.

Las líneas de trabajo futuras contemplan principalmente:

- el Soporte de los Estándares Internacionales en relación a Sistemas Informáticos

- cualesquiera Infraestructura Tecnológica pública o privada que precise de Capas de Seguridad, y cuya normativa sea regularizable legalmente.

- aplicaciones en materia de Protección de Datos de Carácter Personal, habiéndole dedicado en este caso su atención al dato de la 'Historia Clínica' por considerarle de mayor aplicación de *Nivel de Seguridad*

- el Escenario ampliado que nos ocupa de la e-HC

A día de hoy la difusión de textos en torno a la ISO/IEC 27001 e ISO/IEC 27002 , así como en relación al *Documento de Seguridad* son mínimas, queriendo haber contribuido a su Divulgación.

ANEXOS

ANEXO 1: Articulo 1. Responsabilidad Taxonómica en la Historia Clínica

Revista: RDUNED, nº 11

Resumen:

El compromiso de separar las competencias que proponen, literalmente, por una parte un paciente y por otra, un e-técnico ante la observación de una dato clínico concluye con la exposición, al menos, de dos grupos taxonómicos .

La necesidad de cada taxonomía conduce a actuar de un modo muy diferente con el mismo dato de modo que la legislación que origina en el primer grupo desarrolla la 'Summary Patient' , y en el segundo grupo empuja a incrementar la generación de auditorías dentro y fuera de cada unidad de sección de la Administración Electrónica.

Finalmente, se recogen aquellos principios que parecen contemplar estas consideraciones en relación exclusiva al Consentimiento Informado

Abstract:

The difficulty to split the competences between the perspective of , literally, a patient, and an informatic e-technician on the observance of a clinical data concludes with the definition of two , at least, taxonomic groups.

The necesity of each taxonomy compelles to act in a very different way with the same data and produces such a legislation that on the first group developes the 'Summary Patient', and on the second one pushes to increase the management of auditories inside and outside the unit of the e-section of the Electronic Administration.

In exclusive relationship with the informed consentment are compilled that foundations that seem to consider the proposed view.

Claves:

taxonomía, agente, privacidad, grupo taxonómico, derechos ARCO, seguridad del paciente, incidencia, consentimiento informado, historia clínica

Key Words:

taxonomy, agent, privacy, taxonomic group, ARCO rights, summary patient, incidence, informed consent, health and medical record

Sumario: I.Premisas de la Taxonomía II.Grupos Taxonómicos III.Consideración del Consentimiento Informado

I.Premisas de la Taxonomía

Del reconocimiento de la importancia del desarrollo de las Taxonomías , podemos extraer algunos principios o consideraciones generales que nos pueden servir a modo de guía previo a exponer el discurso vigente acerca de las responsabilidades tanto desde el campo legal como desde el técnico en el área de tratamiento de la Historia Clinica:

- resaltando la importancia de los *agentes*[184] identificados en cada época en torno a la percepción y tratamiento de la privacidad y su posterior consideración desde un estado inicial de bienestar, y ampliando el campo de observación cuando el ciudadano hubiera alcanzado el horizonte de paciente resulta factible detectar más facilmente aquellas situaciones por las que debe discurrir el desarrollo del dogma legislativo , la labor del legislador y la de un supervisor técnico que adoptará medidas de salvaguarda a fin de sobrellevar posibles incidencias en el tratamiento de estos especialísimos datos de caracter personal

- a fin de poder detectar aquellos posibles *Niveles de Intimidad* que el individuo considera equilibrio entre su percepción , anteriormente descrita, y la consiguiente manipulación del dato clínico no se deberá olvidar , sino más bien registrar aquellos escenarios y contextos en los que se extraen estos significados

- con independencia del *status quo* en el que se encontrara el ciudadano , éste debiera preguntarse en qué medida se es *consciente* de lo que ocurre, bien fuera en relación al

184 "Agent Jurisprudence". Michael N. Huhns, Munindar P. Singh. IEEE Internet Computing. March – April 1998. http:/computer.org/internet (Acceso URL: Julio 2012)
"A Formal Model of Legal Argumentation". Giovanni Sartor

Gobierno, a la familia, al Empleo, a las políticas de cada comunidad, etc.

- Reconociendo la *Naturaleza* de la Información y de cómo se crean intereses sobre ellla, resultará factible superar la perspectiva de cómo cada Sociedad protege los problemas en torno a la Intimidad Personal frente al denominado 'bien social'

- se puede concluir que cada Taxonomía debiera decir más bien poco más allá de su propio contexto

- advertencia de los posibles peligros , para cada Grupo Humano, que participe en la manipulación del dato médico del posible *Uso Secundario* que se le pudiera dar

- de modo genérico se identifican tres grandes *grupos* en torno a lo que se ha venido en llamar estructura de la e-Sanidad: el propio paciente, el técnico más o menos caracterizado en su profesión y que debe evitar la perdida de información; y, la del asistente sanitario no informático que en el día a día interacciona y trata la salud del paciente.

- para el reconocimiento de principios y agentes debemos mantener continuamente activo el *Ciclo de Deming*[185] o "*Plan.Do.Check.Act"*

- reconociendo la necesariedad de la actualización y colaboración en la elaboración de los *Códigos de Buenas Prácticas*[186], así como de la importancia de recabar adecuamente aquellos *Requerimientos Informados*[187] correspondientes a cada Sistema Nacional de Salud cada Grupo Humano de Taxonomía que participa en el soporte de la e-Salud[188] detectará con mayor nitidez aquellas entradas y salidas para los activos que hubiera que proteger o vigilar

185 ISO/IEC 27 001

186 Código de Buenas Prácticas Clínicas. CPMP/ICH/135/95, (pag. 18) http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guidel ine/2009/09/WC500002874.pdf (Acceso URL: Agosto 2012)

187 Jurisprudencia de Telecomunicaciones. Editorial Aranzadi. Coleccion: Jurisprudencia Comentada. Cap IV. II. „Naturaleza Jurídica de los Requerimientos de Información". 2008 (pag. 250)

188 La OMS define la *e-health* como el uso en el sector de la salud de aquella información digital , transmitida, almacenada u obtenida electrónicamente para el apoyo al cuidado de la salud tanto a nivel local como a distancia.
No se fabula si se decide que la e-health salva vidas, dado que permite el envío de datos online vitales en situaciones donde unos pocos minutos son los que separan a un paciente de la vida a la muerte.
Existe un Observatorio global de la e-heatlh conocido como *Goe*, nacido a principios de 2005 y que publica un informe anual , así como directrices dirijidas a los países interesados
http://www.who.int/kms/initiatives/ehealth/en/ (Acceso URL: Octubre 2012)

dentro de su Grupo. Es de este modo, como el Tecnólogo sabe de antemano que nunca es un plus el manejo y aplicación de estándares reconocidos internacionalmente

A modo de ejemplo, exponemos algunos de los esquemas que resulta factible deducir sobre las directrices anteriormente expuestas:

II.Grupos Taxonómicos

Percepción del modo en cómo se recopila su *PII*[189], *Personal Informatic Information*	se presenta voluntariamente a la consulta y se recopila su información
Intervencion sucesiva en la verificación de sus datos en la *HC, Historia Clínica*	puede validar actualmente la veracidad de sus datos en la HC en el mismo momento de la anamnesis, por intervención posterior, por propia voluntad de acceso a la plataforma de la e-Administración o por petición del ejercicio de sus derechos ARCO, o acceso, rectificación, cancelación u omisión
Voluntariedad de participación en programas científicos o de videovigilancia	e.g. es solicitado por constar en la BBDD, Base de Datos, en un estudio de videovigilancia clínica
Ejercicio de Derechos ARCO[190] y Medicina Legal	se le notifica que se ha producido un incidente con e- HC y hay o no consecuencias para su salud
Percepción en Feedback del tratamiento de datos que le llega de la Sociedad a la que pertenece	e.g. a través de noticias se hace consciente de que su información puede ser accesible por otras personas que las meramente de asistencia, por personal no autorizado sanitario, y se puede hacer un uso indebido de ellos
Participación en la *Seguridad del Paciente*[191]	se le plantean diversas formas de actuación en la Defensa de sus Derechos ARCO, de los que fue Formado y ha de elegir el modo de interlocución por el Servicio que le compete, independientemente de producirse un incidente con su HC
Uso de la HC en el ejercicio de sus Derechos	no existe negligencia de ningun dato en su HC, pero se ha producido una negligencia médica: la HC como prueba judicial
Responsabilidad Civil	procedimiento por fallecimiento de un ciudadano
Manejo de otros derechos que el de su Estado y Jurisprudencia	e.g. se dedice optar por la medicina privada y ha de ser informado de las diferencias de tratamiento respecto de su HC en la e-Sanidad, aunque el ejercicio del derecho le protege idénticamente

Tabla 1. Taxonomía del Paciente

189 PII, Personal identificable information .http://en.wikipedia.org/wiki/Personally_identifiable_información (Acceso URL: Julio 2012)

190 LOPD (art. 5.1.d), L 41/2002 (art.18), L 56/2007 (art. 1.d)

191 Enlaces. http://formacion.seguridaddelpaciente.es/Enlaces.aspx http://www.who.int/patientsafety/es/ (Acceso URL: Julio 2012)

Responsabilidad de Impermutabilidad de Información	debe responder de la veracidad de los datos que maneja y que no experimentan modificaciones
Colaboración Auditada	debe poder proporcionar y filtar en el documento curricular propuesto aquellos datos de los que con autorización formulada ya aceptada se ejerciera la defensa de los Derechos ARCO
Conocimiento de la Legislación a la que asiste	debe responder a la dinámica de las Auditorías Internas y Externas en materia de protección de datos
Responsabilidad de Incidencia	como responsable de un incidente debe , conforme al procedimiento establecido en la Política de sus Empresa, comunicarlo, y tratarlo minimizando su suceso
Aportación de su experiencia en la Optimización de la e-Administración	debe cooperar en el tratamiento de otros incidentes que se produjeran y en los que pudiera aportar conocimiento de causa y efecto
Monitorización de Incidencias	como responsable de una salvaguarda se exige vigilancia constante en su cumplimiento, debiendo reportar oportunamente su fallo
Análisis y Supervisión de la Medida de Control de la que es responsable	debe corroborar que la salvaguarda cumple escrupulosamente la normativa legal y el marco de interoperabilidad en el que desempeñe su trabajo
Manejo de Alertas de Incidentes[192]	Capacidad de Respuesta Informada de su actuación conjunta

Tabla 2. Taxonomía del e-Técnico

III.Observación del Consentimiento Informado

Conforme al *Convenio de Oviedo de 1997*[193] propuesto por el *Consejo de Europa* se establece en su *art. 5* que una intervención en el ámbito de la sanidad tan solo podrá efectuarse después de que la persona afectada haya emitido su expreso consentimiento, consentimiento que por otra parte podrá ser retirado en cualquier momento.

A continuación y sin la consideración esta del paciente, por ejemplo, en situaciones de 'urgencia' y

192 RD 1720/2007 (arts.90 y 100), RD 03/2010 (Anexo 2.4)

193 Propuesto por el Consejo de Europa establece en su art. *5* que una intervención en el ámbito de la sanidad tan sólo podrá efectuarse después de que que la persona afectada haya emitido su expreso consentimiento, consentimiento que por otra parte podrá ser retirado en cualquier momento. Es el primer instrumento internacional con carácter *público vinculante* para los países que lo subscriben. De manera que, el derecho a la protección a la salud queda reforzado en el terreno de la documentación clínica

desde el punto de vista médico podrá ser llevada a cabo cualquier intervención en favor de la salud de la persona afectada. Debiendo, no obstante, observarse los deseos anteriores del paciente si asi constara, *art. 9*.

Toda persona tiene derecho a que se respete su vida privada respecto a la información en materias de salud, respetándose en cualquier caso, la voluntad del paciente a no ser informado.

El *art. 23* reconoce la contravención precisamente de estos derechos o principios garantizando una protección jurisdiccional[194] de los preceptos que propone. Y es su *art. 26* el que no admite restricción a tales derechos establecidos.

El paciente podrá manifestar en el 'documento de instrucciones previas' su voluntad manifiesta con objeto de que esta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de hacerlo personalmente o bien una vez llegado el fallecimiento sobre el destino de su cuerpo o de los órganos del mismo. Este derecho reconocido en el *art. 11* que se otorga al paciente puede designar, además, un interlocutor que mediara entre él y el médico pertinente o equipo sanitario. Creara, por consiguiente, el *Ministerio de Sanidad y Consumo* el *Registro Nacional de Instrucciones Previas*, previo acuerdo del *Consejo Interterritorial del Sistema Nacional de Salud*.

Por su parte la Ley *L 11/2007* reconoce al ciudadano el derecho a manifestar consentimiento, pudiendo este emitirse y recabarse también por medios electrónicos.

Casos más complejos que incluso deberían poder justificarse judicialmente nos lo presenta la Agencia de Protección de Datos en su 'Informe 488/2004' planteando, por ejemplo, la tesitura de la comunicación de los datos a otro facultativo de la misma especialidad que una consultante, motivada por el cese de su actividad.

Debe recordarse, nos recuerda su argumento, que de la interpretación del ya mencionado *art. 17.1* y del *art. 18.1* de la Ley, que dispone que "El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella", se desprende que los datos sólo podrían ser comunicados a otros facultativos en caso de que los mismos fueran a realizar una actividad de diagnóstico o tratamiento del paciente o el propio paciente solicitara la transmisión de su historia a su nuevo

194 D 95/46/CE (ar. 10) , LOPD (art. 6),L 41/2002 (art. 3 y rt. 8), RD 223/2002 (art.6.2), L 11/2007 (a.22)

médico, sin perjuicio del deber de conservación del anterior.

La Ley, por otra parte, no impide otros usos posteriores de los datos médicos, sin perjuicio de que se introduzcan salvaguardias para garantizar la confidencialidad del paciente. Así, en su *art. 16.3* se contempla el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, siendo obligado preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente.

Existe una necesidad de consentimiento expreso, aunque no necesariamente escrito para los datos relacionados con la salud, el origen racial y la vida sexual.

En caso de datos no especialmente protegidos se le otorga al afectado un plazo de treinta días para manifestar su tratamiento.

La solicitud de consentimiento respecto de un tipo de datos no podrá ser nuevamente ejecutada en el plazo de un año a contar desde la fecha de su solicitud. Tanto el derecho de acceso como el otorgamiento del consentimiento informado prescriben al de un año.

No será necesario el consentimiento del interesado en caso de urgencia relativa a la salud o para la realización de estudios epidemiológicos en los casos legalmente previstos.

En casos de trasferencias internacionales, el consentimiento informado se hace necesario para establecer la relación contractual entre el afectado y el responsable del fichero, debiéndose, no obstante:

- notificar a la Agencia Española de Protección de Datos
- e informar al interesado

Históricamente el consentimiento informado tiene su origen en el denominado *Código de Núremberg*[195].

De acuerdo con el *Código de Buenas Prácticas Clínicas*[196]' tanto las entrevistas

del consentimiento informado como su expresión escrita debe contener las siguientes indicaciones de alguna forma:

- que el estudio implica investigación
- el propósito del estudio
- el acuerdo del estudio
- procedimientos a seguir
- responsabilidades del sujeto
- indicaciones de aquellos aspectos del estudio que resultan experimentales
- razonables riesgos que se prevén para el sujeto
- los beneficios esperados
- procedimientos alternativos del tratamiento
- compensaciones por perjuicios

195 Código de Nuremberg. http://www.pcb.ub.edu/bioeticaidret/archivos/norm/CodigoNuremberg.pdf (Acceso URL: Julio 2012)

196 Código de Buenas Prácticas Clínicas. CPMP/ICH/135/95, (pag. 18)

- indicación del pago prorrateado, en su caso, por la participación
- la posibilidad de abandonar en cualquier momento el ensayo
- la identificación de la responsabilidad de la confidencialidad del sujeto en el acceso a sus datos
- duración
- número de sujetos

Un paciente puede precisar requerir el conocimiento de determinada información acerca de su historia clínica para la aplicación del tratamiento médico correspondiente que se le decida aplicar en una determinada zona geográfica de nuestro planeta. La contextura del Centro donde se pueda producir este hecho puede ser de carácter público o privado.

Cualesquiera fuera la naturaleza jurídica de los casos, se precisará la observación de la colaboración de la aplicación de la legislación de los países origen y demandante del servicio informático. Entre ambos cuerpos y apoyándose en la dinamización internacional entre ambos que se hubiera decidido existirán, además, normalizaciones y regulaciones de Organismos reconocidos que en el trascurso de la dialéctica se hubiera decidido aplicar como garantes y acompañantes en su desempeño.

El nivel de acuerdo decidido desde el Gobierno de ambos países decidirá el grado de traba a la hora de proporcionar dicha información y el formato en que será recibido por parte del Centro de Atención Médica.

Habida cuenta de la posibilidad de Acceso por parte del ciudadano de la información necesaria acerca de su Historia Clínica, se le puede plantear al mismo el ejercicio o la determinación de sus propios criterios de filtrado de su información en la medida contemplada por la *Ley General de Sanidad* que se le aplicara. Tal derecho es reconocido como ejercicio de los *Derechos ARCO*[197], esto es, de *Acceso, Rectificación, Cancelación y Oposició*n, resumiendo en cierto modo la defensa que le

197 LOPD (art. 5.1.d), L 41/2002 (art.18), L 56/2007 (art. 1.d)

está permitida en materia de protección de datos.

Tanto es más cuando se puede ver ampliada esta perspectiva de aplicabilidad con fines de estudio de carácter estadístico. Y, de igual modo, qué ocurre en el desarrollo de la intervención médica con el manejo de los *Consentimientos Informados*, idénticamente se puede aplicar el concepto del tratamiento de su Historia Clínica, *HC,* en el contexto de la e-Administración.

Ya en último término se podrá provocar el bloqueo de datos o cancelación, quedando esta información tan sólo a disposición de la Administración Pública, Jueces y Tribunales. Quedando siempre amparado el paciente ante la Agencia de Protección de Datos.

El derecho de acceso contempla el conocimiento del fin último para el que se estuviera desestimado un tratamiento de datos, pudiendo ejercerse en su caso un derecho de oposición, y conocimiento exacto de las características del fichero en el que se encuentra invocado.

Los accesos restringidos podrán obtenerse por escrito, y por visualización de pantalla de ordenador .

Existen otros derechos considerados en relación a la seguridad del paciente dentro en el contexto de la e-Sanidad si tenemos en cuenta el modo en que todo ciudadano es destinatario de una *Tarjeta Sanitaria Electrónica*[198] en la que reside una identificación digital y por medio de la cual puede identificarse en el marco de su sistema sanitario con revocación de firma electrónica.

En este punto son las Comunidades Autónomas las que se hacen responsables tanto de la tramitación de la tarjeta como de las autentificaciones realizadas en el contexto de la operativa, debiendo proporcionar idénticamente un Servicio de Atención al Cliente.

Por otra parte y dependiendo del desarrollo que haya alcanzado la aplicación de la Telemedicina en su Comunidad Autónoma, podrá disponer de otra serie de dispositivos médicos como localizadores , servicios de domótica, pdas, etc.

La interoperabilidad entre Comunidades Autónomas permite al usuario de la e-Sanidad el acceso y obtención de informes clínicos determinados a fin de ser almacenados en dispositivos electrónicos,

198 L 16/ 2003, cap. V (a.57)

no considerando necesaria la citación de las copias impresas por considerarlas siempre hábiles y obvias.

Se encuentra el ciudadano con la posibilidad de vetar el acceso de determinados informes entre Comunidades y de la utilización de un sistema de alertas que le indique siempre cuál es el curso de sus diligencias incluidos las denegaciones del derecho que hubiera podido recibir.

El modelo de acceso a esta tipo de información deberá encontrarlo habilitado las veinticuatro horas del día y a lo largo de toda la semana.

Una tercera clasificación de los derechos del ciudadano se puede presentar desde el punto de vista de los *Sistemas de Prevención Laboral* como puede ser el caso de las Mutuas y Aseguradoras, del que siempre se deberá poder obtener el 'prorrateo' del seguro que le ampara y aquel 'Código Tipo' al que se encuentra adscrito un Promotor en un Sistema de Vigilancia Médica o Farmacovigilancia independientemente de que se produzca el tratamiento de datos de su HC fuera o dentro del país donde reside.

El sujeto participante en el marco sanitario también conocido como *Trial Subject,* puede por su parte, adoptar otra posición respecto de la defensa de sus derechos, haciéndose consciente que ni el investigador ni ningún otro miembro de la plantilla del centro sanitario donde se le deben respetar los derechos como ciudadano de la Unión Europea debieran influir en la decisión de su continuidad en el estudio o tratamiento.

No parece justo realizar una desligazón entre la figura del consumidor y el proceso concreto de generación y tratamiento de los consentimientos informados, puesto que entraña una responsabilidad manifiesta por parte del paciente no sólo el ejercicio de los Derechos ARCO sino la participación completa en el proceso de asistencia sanitario con las correspondientes afirmaciones o denegaciones de las fases de toda asistencia.

Por otra parte, podremos analizar la oportunidad de las coberturas que el Estado ha querido otorgar al papel del consumidor como usuario del servicio sanitario informático que le ofrece la Sociedad en la que vive.

Manifestamos las siguientes caracterizaciones que pueden llegar a condicionar la figura del consumidor en el ámbito de la e-Sanidad:

- el ejercicio de los Derechos Arco

- por el ejercicio de los derechos a Sanidad y derechos de las Telecomunicaciones

ANEXO 2: Articulo 2. La Semántica en el Derecho de la Informática en la Historia Clínica

Revista: DIARIO LA LEY, Nº 8011

Resumen:

Desde el inicio en la legislación española el concepto de autodeterminación del ejercicio de los derechos de acceso, y posteriormente reconocidos como *Derechos ARCO* encontró precisamente en el campo de la e-Sanidad la integración de la tradicional exposición Libertad informativa vs. Autodeterminación.

Claves:

requisito informado, e-health, SNS, código tipo, consentimiento informado, autodeterminación informativa, libertad informatica, right to privacy, persona jurídica, derecho arco, principio de transparencia, documento de seguridad, incidencia

Sumario: I.Requisito Informado II.Autodeterminación Informática por Consentimiento III. Ejercicio de los Derechos Arco

I.Requisito Informado

El concepto *Requisitos Informado*[199] que se recoge y defiende desde la *Comisión de las Telecomunicaciones*, CMT, nos recuerda la necesidad de recopilar en fehaciente labor aquellas operativas , distinguidas en este caso observadas por la Legislación a fin de no incurrir en dobles propósitos

definitorios y poder responder con mayor exactitud al Diseño del Sistema Informático.

Recordemos que la base de la propia definición del concepto indicado, el de requisito informado ,

199 Ley General de Telecomunicaciones 32/2003, (art. 53 y 55)

por parte de los operadores de Telecomunicaciones a dicha Comisión, exige un alto conocimiento técnico, económico y jurídico en el momento de su exposición. La actualización está sometida a dos años de actualización. La propia Audiencia Nacional recuerda que se deben observar dos criterios a la hora de determinar la proporcionalidad del requerimiento solicitado: objetivo y subjetivo.

En el caso concreto de la Historia Clínica existe la posibilidad de la existencia de la historia en forma no digital y de que las diferentes Comunidades Autónomas se encuentren en fases varias de implantaciones y pruebas de su Sistema de Información en la plataforma de la e-Sanidad , teniendo que garantizar, en cualquier caso, aquellas situaciones en las que el ciudadano pueda interaccionar con su Historia Clínica sin recurrir a dicha plataforma en el contexto de los centros sanitarios.

Por otra parte, y ya en el Contexto de la e-Sanidad, es el *Sistema Nacional de Sanidad o SNS* el que delimita el procedimiento, Ley L 16/2003 , art. 1, incluido la interfaz por medio de la cual tiene acceso al mismo.

Ahora bien, el dato de la historia clínica por el que el ciudadano puede inferir especial interés en el ejercicio de sus derechos puede tener orígenes bien distintos: el de una *anamnesis* básica de su médico de atención primaria bien se trate la entidad a la que acuda de pública o privada, o el de un dato correspondiente a la Atención Especializada. Además, hemos de integrar los ámbitos de la Farmacovigilancia, el de los Estudios Clínicos y la Protección de Riesgos laborales que típicamente llevan asociados la relación con una Mutua.

Se puede aseverar sin género de duda, que resulta de vital importancia el poder tener acceso a unos no suficientes sino decentes y adecuados *Requerimientos de la Unidad del Sistema Informático Médico* que se pretende afrontar. La importancia de esta observación está recogida, no olvidemos, en la Doctrina de la Jurisprudencia desarrollada en torno a la Comisión del Mercado de las Telecomunicaciones o CMT, para la que una no veraz información puede reconocer el perjuicio causado sobre un ciudadano, y en consecuencia resultar penalizado el origen de la mala información.

La correcta expresión de los requerimientos citados que han de recoger, por otra parte, las Operativas

del Personal de Recursos Humanos que la Soportan, puede exigir en tal medida un Buen Diseño de su Arquitectura. La experiencia futura llegará a demostrar cómo una incorrecta definición de esta arquitectura puede ayudar en colaborar en extender una confusión que mal manejadas puede incurrir en grave perjuicio para el ciudadano-paciente, y por extensión, al colectivo de la población.

En ocasiones, los *Códigos Tipos*[200] pueden ayudar a corregir esta tendencia, viéndose obligados a reforzar la dinámica del Personal Corporativo por no verse reflejada en la Aplicación Informática que manipulan.

Por su parte el Sistema de Mutuas y Seguros Médicos permite añadir un punto de seguridad que el Empresario decida en qué grado aplicar ante la inseguridad que pude ofrecerle un trabajador, y que bien tratada puede reforzar la tranquilidad del asegurado.

II.Autodeterminación Informática por Consentimiento

Con especial cuidado debemos referirnos a la multiplicidad de significados que algunos términos pueden encontrar como es el caso de la palabra autodeterminación en el contexto en el que nos expresamos. Por una parte contamos con la explicación que hizo en su momento la Exposición de motivos de la LORTAD[201] refiriéndose a:

- "Las garantías de la persona son los nutrientes nucleares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de *autodeterminación*, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático"

- Por su parte, el principio de *consentimiento*[202], o de autodeterminación, otorga a la persona la

200 LOPD, Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, (art.32)
201 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, derogada e invocada desde la LOPD
202 LOPD (art.6), D 95/46/CE (art.2, art.10), L 41/2002 (art.3, a.8, art.10), L 32/2003 (art.38), RDL 223/2004 (art.1, art.6.2), L 11/2007 (art.22)

posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita; sus contornos, por otro lado, se refuerzan singularmente en los denominados *datos sensibles*, como pueden ser, de una parte, la ideología o creencias religiosas, cuya privacidad está expresamente garantizada por la Constitución en su art. 16.2 y, de otra parte, la raza, la salud y la vida sexual

Queda expresado el modo en cómo la inicial legislación en materia de protección de datos y recogida la LORTAD tras su derogación en la actual Ley de Protección de Datos, LOPD, y en cómo entendía el derecho a la autodeterminación informativa , según sentencia del Tribunal Constitucional Alemán, STFCA de 15 de Diciembre de 1983*:*

- "la facultad del individuo, derivada de la idea de *autodeterminación* de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida. De este modo, un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo las condiciones de la elaboración automática de datos, ninguno *sin interés.* A consecuencia de lo que antecede, el grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad

- Hace falta, más bien, conocer la relación de utilización de un dato para poder determinar sus implicaciones para el derecho de la personalidad. Sólo cuando reine la claridad sobre la finalidad con la cual se reclaman los datos y qué posibilidades de interconexión y de utilización existen se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la *autodeterminación informativa*

Precisando en todo caso de una disertación la separación entre este concepto y lo que se vino en llamar *libertad informativa* como más adelante se comentará.

La legislación estadounidense viene a desarrollar lo que se denomina un *right to privacy* , expresando el derecho a la intimidad entendido como separación y defensa del individuo frente a la sociedad a través de su *Privacy Act* de 1974 y que incorporó las recomendaciones recogidas un año antes por el Departamento de Salud, Educación y Bienestar de un estudio de "Registros, computadoras y derechos de los ciudadanos" en el que se proponía un código *federal fair information practices* encaminado a salvaguardar la intimidad personal aconsejando la creación de registros , observando el mantenimiento de copias , regulando cada consentimiento informado y el consiguiente ejercicio de los derechos de acceso.

En la legislación española el término que se maneja es el de intimidad y concretamente y vinculadas al principio de derecho de libertad informática contamos con , al menos, las expresiones STC 110/1984 y STC 11/1998.

Observando el devenir legislativo, el art. 12 de la *Carta Internacional de los Derechos Humanos* de 1948 establece que nadie será objeto de injerencias arbitrarias en su vida privada, su domicilio o su correspondencia ni de ataques a su honor y su reputación y que toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques. Como fuerza moral no conlleva vinculación jurídica expresa, excepto para los Estados que la han incluido en su propia Constitución.

Veinte años después, en el Convenio de Europa surge, como consecuencia, la emisión de una serie de resoluciones:

- nº 22/1973, respecto a los datos de titularidad *privada*
- nº 29/1974, de titularidad *pública*

, provocadas a su vez por La Recomendación 509 de la Asamblea del Consejo de Europa dirigida al Comité de Ministros con el propósito de que la Convención Europea para la Protección de los Derechos Humanos buscara la forma de proteger los derechos de la persona.

No pudiendo entrar en contradicción la interpretación de las normas constitucionales en relación a

estos principios:

- art. 8.1: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”

- art. 8.2: “No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás”

III. Ejercicio de los Derechos Arco

En 1985 se habla ya del primer *Sistema de información inter-países europeo* permitiendo la emisión de visados y revisión de documentación trasfronteriza con soporte a fines policiales. El denominado *SIS* en su fase II, nos sugiere en el *art. 118* de su estatuto una serie de observaciones que ratificado el acuerdo e incorporado a la legislación nacional quedó integrado tras la derogación de la LORTAD en la LOPD y cuyas indicaciones son factiblemente auditables desde los nuevos desarrollos en la legislación competente a la *Sociedad de la Información* por la Ley que regula el Esquema Nacional de Seguridad o L 11/2007[203] y sus desarrollos a posteriori en los RD 03/2010 y RD 04/2010 :

- control de entrada en las instalaciones

- control de los soportes de datos

- control de la introducción

- control de utilización

- control de acceso

203 L 32/2003 (art. 9.b), 2006/24/CE (art.10), L 41/2002 (art.23)

- control de la transmisión
- control de introducción
- control de transporte

La responsabilidad civil, art. 1902 del Código Civil, se fundamentaba en la existencia de daño efectivo y comprobable como presupuesto de cualquier reclamación de perjuicios causados: si se comprobaba el daño, se presumía que el agresor era el culpable. Su posterior formulación legal en 1982 en la Ley Orgánica de Protección Civil de Derecho al Honor, a la Intimidad Personal y familiar y a la propia Imagen refleja en su art. 9.3 la existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima, refiriéndose al daño moral.

La inicial y posterior sustituida Ley de Protección de Datos de 1992 conocida como LORTAD formula el denominado concepto de *dato sensible* que no tendría que ser declarado, art. 16.2, salvo por consentimiento de la persona y por escrito a excepción de lo establecido en el art. 20.3 según la cual las Fuerzas y Cuerpos de Seguridad podrán recoger esta clase de información sin su consentimiento, excediendo en principio a lo propuesto en el texto europeo lo que motivó recursos de inconstitucionalidad por parte del Defensor del Pueblo.

Las disposiciones de Schengen quedan salvaguardadas por el Real Decreto 1332/1994 conforme consta en el art. 4.1.b donde así mismo se indican las pautas para el tratamiento de datos en ficheros de carácter estadístico. Igualmente queda reglamentada la obligación de notificar la creación de un fichero, en los supuestos de titularidad pública y en los de titularidad privada.

El texto precedente de la actual Ley en materia de Protección de Datos, la Directiva D 95/46/CE da paso a otra, la D 97/66/CEE ampliada al sector de las Telecomunicaciones, que quedarán incorporadas a Derecho legal en 1999 en la referida LOPD. En la categorización de datos la LOPD inicia la definición de dato sensible haciéndose coincidir con la proporcionada por la Directiva D 95/46/CEE como cualquier información concerniente a personas físicas identificadas o

identificables, siguiendo con una categorización de especialmente protegidos en nuestro ámbito a aquellos referidos a la salud y los manejados por la Administración.

En el ámbito europeo el Convenio 108 se permite en virtud de su art. 3.2 b que los Estados, con ocasión de la firma, del depósito, del instrumento de ratificación, aceptación, aprobación o adhesión o con posterioridad, pudieran manifestar que aplicarán

"también el presente convenio a informaciones relativas a agrupaciones, asociaciones, fundamentos, sociedades, corporaciones y cualquier otro organismo, formado directa o indirectamente por personas físicas, tuvieren o no personalidad jurídica"

Algunos países incluyeron rápidamente esta clausula respecto a la protección de datos de las "personas jurídicas" , art. 3.2 de la ley austríaco, el art. 2 de la ley luxemburguesa, sin embargo, la mayoría no la contemplaron tan inmediatamente: Alemania, Australia, Reino Unido, etc.

Debiendo observar claramente cuáles son los casos en cada momento de observancia de definición de un fichero, que como reitera la LOPD quedan excluidos, de la necesidad de integrarse en un fichero automatizado para los siguientes supuestos como :

- aquellos que posean las personas físicas en el ejercicio de actividades exclusivamente personales o domésticas , por ejemplo, los de una agenda electrónica o PDA

- los sometidos a la normativa sobre protección de materias clasificadas, por ejemplo, los secretos del CESID

- los establecidos para la investigación del terrorismo, aunque el Ministerio del Interior debe comunicar su existencia y su finalidad a la Agencia de Protección de Datos

- los regulados por la legislación de régimen electoral , sobre todo, el censo

- los que se utilicen para *fines estadísticos*[204]

- los que almacenen datos en informes personales de calificación que se encuentren amparados por la legislación del Régimen del personal de las Fuerzas Armadas, etc.

En todo caso, el ciudadano tiene el derecho a estar informado acerca de la existencia, finalidad y de los destinatarios de la información, estando legislativamente prohibido otorgarlos por la fuerza. Sin embargo, conforme a su art. 11.2.d y f no se precisará un consentimiento cuando la comunicación tuviera como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas, o bien por motivos de urgencia en una actuación sanitaria.

La existencia de un fichero implica su archivo y conocimiento auditado ante el Registro de la Agencia de Protección de Datos a fin de encontrarse hábil en un posible ejercicio de la defensa de los *Derechos ARCO*[205].

De registro e idénticamente que en el caso anterior han de ser inscritos y depositados los *Códigos Deontológicos* o de buena práctica empresarial.

Va a ser el *real decreto RD 994/1999* de Medidas de Seguridad el que inicia el trabajo de un *Documento de Seguridad*[206] siempre y cuando se manejen datos de carácter personal donde habrán de estar bien definidas y documentadas las funciones y obligaciones de cada persona, la estructura de los ficheros y descripción de los sistemas de información; procedimiento de notificación, gestión y respuesta ante incidencias y de realización de copias de respaldo y de recuperación de datos.

204 L 32/2003 (art. 9.b), 2006/24/CE (art.10), L 41/2002 (art.23)
205 LOPD (art. 5.1.d), L 41/2002 (art.18), L 56/2007 (art. 1.d)
206 RD 994/1999 (art.8)

Para la notificación y gestión correspondiente, se contará con el haber de un *Registro de Incidencia.* Los tres niveles de seguridad que establece bajo, medio y alto serán posteriormente analizados y desarrollados en el *RD 03/2010*–conforme a la métrica que ha venido siendo observada en la Administración.

El concepto de Privacidad aparece explícito nuevamente en la identidad de la *Directiva 2002/58* integrada *ya* en la D 2006/24/CE *o* al que se le añade el concepto de *Comunicaciones Electrónicas* ampliando el campo de operación de este concepto en el contexto de las Telecomunicaciones actuales. Es en este caso cuando el campo se amplía a las *personas jurídica*s que había sido obviado en la D 95/46/CEE.

Se produce en este nivel la aparición de los

- *servicios de valor añadido* como todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación

- *datos de localización* como cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público

Conforme a las Sentencias STC 202/1999 y la 292/2000 la LOPD no había fijado como le impone la Constitución los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas sino que se había limitado a identificar la norma que puede hacerlo en su lugar que, aunque puede ser reglamentaria y de rango superior, con mayor razón para el caso de que la modificación lo sea por una norma de similar rango a la que crea el fichero (y esta basta que sea una disposición general, que no una Ley, publicada en un Boletín o Diario Oficial) la que pueda autorizar esa cesión inconsentida de datos personales, contrario a la Constitución.

Según el art. 13 de la propia LOPD, los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad; resulta dificilmente compatible con la denegación del derecho a ser informado del art. 5 LOPD acordada por la Administración Pública con el único fundamento de la persecución de una infracción administrativa .

El artículo 18.4 de la Constitución en el que se quiso fundar el nuevo derecho de autodeterminación informativa, que aun estudiando la corriente de doctrina no estableció ningún nuevo derecho, sino un límite a una facultad , "el uso de la informática" derivable del derecho general de la libertad, art. 17.1 C o de la libertad específica de comunicación, art. 20.1 CE sobre la base de derechos expresamente consagrados en la Constitución ("el honor y la intimidad personal y familiar", art. 18.1 CE). Se trata pues de una clausula que establece límites expresos en el ejercicio de derechos fundamentales. Dicho límite quedó registrado en la sentencia STC 254/1993 cuyo título recoge expresamente las palabras *libertad informativa*.

Además, la solución escogida ofrece la ventaja de favorecer la construcción de un régimen jurídico más eficaz y la elaboración de una doctrina más coherente y sistemática al acotarse, con precisión, los campos propios de uno y otra. Concluyendo, en cualquier caso, que no pareció conveniente una ampliación del campo de protección del derecho a la intimidad. Su discurso quedó focalizado en la dialéctica *autodeterminación informática vs. libertad informática* introducida en la sentencia del Tribunal Constitucional alemán STFCA de 15 de Diciembre de 1983. Esta aceptada apertura a posteriores desarrollos en orden a otorgar protección frente a nuevas situaciones de peligro que puedan surgir con el desarrollo tecnológico y social quedó perfectamente reflejada en sentencia STC 292/2000 a respuesta de recurso de inconstitucionalidad por parte del Defensor del Pueblo postulando la necesidad del *habeas data*.

El tratamiento del recién definido dato sensible que no cuenta parangón similar en EEUU, sí cuenta con el apoyo de la *Directiva 2002/58/CE* en materia de cooperación de este tipo de datos entre Administraciones Públicas.

Como observación final, comentar que la Ley de Bonn de 1977 y reformada en 1999 explica por vía

jurisprudencial una serie de causas que no se dan en España,

- No recoge expresamente un derecho a la intimidad
- Reconoce que la dignidad de la persona es un derecho fundamental

De modo que el *Tribunal Constitucional Federal Alemán, TFCA*, ha creado nuevos derechos entendiéndolos como desarrollo del derecho a la dignidad de la persona postulando la facultad del individuo, derivada de la idea de autodeterminación de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida.

En nuestro país se ha optado finalmente por, independientemente de que la intimidad comparta con otros derechos el nivel de fundamental, porque este derecho permanezca abierto , flexible y capaz de acomodación para ulteriores desarrollos en orden a otorgar protección frente a las nuevas situaciones de peligro que puedan surgir con el desarrollo técnico y social. De no encontrar conexión directa con alguno de los derechos fundamentales consagrados por la CE, ese derecho nuevo podría verse privado de la significación propia de los derechos fundamentales. Desde esta perspectiva, sí se consideró más útil el estimarla comprendida en un derecho fundamental ya reconocido, el de la intimidad.

En junio de 1969, un diario alemán publicó un artículo en el cual se advertía sobre los peligros que la informática planteaba a los derechos de los ciudadanos. El artículo concluía planteando la necesidad de una ley. El Primer Ministro del estado de Hesse leyó la noticia e inmediatamente ordenó que se elaborara una ley que tratara el problema de las bases de datos públicas que contenían datos de todos los ciudadanos. En ese entonces, el gobierno apoyaba la existencia de un banco de datos centralizado que contuviera la información de los ciudadanos. La publicidad del gobierno citaba el siguiente ejemplo: "Si Vd. en ruta tiene un accidente y, como consecuencia, se encuentra inconsciente, con un solo acceso al ordenador será posible conocer sus antecedentes, su historia clínica, sus enfermedades, etc. Las chances de sobrevivir se incrementarán significativamente."

A raíz de esta nota periodística, el tema se instauró en la opinión pública y el 7 de octubre de 1970, el estado alemán de Hesse ya tenía su ley aprobada. Surgía así la primera ley de protección de datos del mundo.

No resulta demasiado alejado observar que mientras en las empresas no se apueste por otorgarle un derecho fundamental a la personalidad jurídica, y siga bajo el amparo de otras ramas del derecho: de patentes, de marcas, civil y penal no se alcanzará un principio de trasparencia negativo en todo caso para la protección del secreto de los negocios. Distando la situación del *Principio de Trasparencia*[207] *propuesto en la Resolución de Madrid (ya recogida en una cita anterior de la LORTAD) ,*

> 1. Toda persona responsable deberá contar con políticas transparentes en lo que a los tratamientos de datos de carácter personal que realice se refiere.
>
> 2. La persona responsable deberá facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente Documento, así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.
>
> 3. Cuando los datos de carácter personal hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en el momento de la recogida, salvo que se hubiera facilitado con anterioridad.
>
> 4. Cuando los datos de carácter personal no hayan sido obtenidos directamente del interesado, la información deberá ser facilitada en un plazo prudencial de tiempo, si bien podrá sustituirse por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado a la persona responsable.
>
> 5. Cualquier información que se proporcione al interesado deberá facilitarse de

207 L 11/2007 (art.4)

forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad.

6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.

BIBLIOGRAFIA

[criterios de *ISO 690: 2010. Information and Documentation- Guidelines for Bibliographic references and citations to information resources*]

DOCUMENTOS Y ARTICULOS

Agencia de Informática y Comunicaciones de la Comunidad de Madrid, ICM. Unidad de Arquitectura y Soporte de Aplicaciones. "Proceso de disociación de datos personales. LOPD. Versión 2.0." 2011

AIBAR REMON Carlos, ARANANZ Andres Jesus M.. "Seguridad del Paciente y prevención de eventos adversos relacionados con la asistencia sanitaria. Unidad Didáctica 2: La Seguridad del Paciente: Una dimensión esencial de la calidad asistencial". Ministerio de Sanidad . 2010. Disponible en:
http://www.seguridaddelpaciente.es/formacion/tutoriales/MSCCD1/pdfs/UNIDAD2.pdf

AMIA, Informatics Professionals. " Privacy Taxonomy For The Nationwide Health Information Network". Enero de 2005.
Disponible en: http://www.amia.org/sites/amia.org/files/2006-Policy-Meeting-nhin-paper.pdf

AMUTIO Miguel Angel. ASTIC, Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas. Fundación ASTIC. Revista de la Asociación Profesional de los Cuerpos Superiores de Tecnologías de la Información en la Administración

"Reutilización de Activos de la Administración", BOLETIC Nº 63.

"El Esquema Nacional de Seguridad. Cinco retos próximos", BOLETIC Nº 73

ANDREE LOPEZ María, G.BENAVIDES Fernando, ALONSO Jordi, ESPALLARGUES Mireia, DURAN Xabier, MARTINEZ Jose Miguel. "La utilidad del uso de datos administrativos en la investigación de salud pública: la Muestra continua de vidas laborales". Gaceta Sanitaria. Vol.28 nº 4.

Boletín de Asesoría Gerencial. "Riesgo Legal desde la Perspectiva del Riesgo Operacional". Nº 8. Espiñeira, Sheldon y asociados. Firma miembro de PriceWaterHouseCoopers. 2008

Circular e-Landwell 001: La dirección IP como dato disociado

Código de Nuremberg.
Disponible en: http://www.bioeticayderecho.ub.edu/archivos/norm/CodigoNuremberg.pdf

DELGADO Francisco. "Intercambios Internacionacionales de datos". BOLETIC Nº 66. ASTIC, Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas

"Eli Lilly Settles FTC Charges Concerning Security Breach". Release January 18, 2002.
Disponible en: http://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach

European Commission. Frequently asked questions from the EU/EEA to third countries". Disponibleen:
http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

GARCIA-CUEVAS ROQUE, Elena. "Las Transferencias Internacionales de datos y las libertades individuales. Un acercamiento a las normas de protección de datos". Revista de la Universidad de Deusto. Vol. 60 nº 2. 2012

GODKIN E.L. "The Right to Privacy". Scribner's Magazine Vol 8, pag. 58-68, 1890

GONZALEZ MURUA, Ana Rosa. "El Derecho a la Intimidad, el Derecho a la Autodeterminación Informativa y la L.O. 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de Datos Personales". Universidad del País Vasco. Working Paper nº 96. Barcelona 1994. Disponible en: http://ddd.uab.cat/pub/worpap/1994/hdl_2072_1371/ICPS96.pdf

Information and Privacy Commissioner, Ontario, Canada. Information Commissionaries office, ICO.

"Privacy by Design". CAVOUKIAN Ann . 2008,
Disponible en: http://www.ipc.on.ca/images/Resources/privacybydesign.pdf
"Privacy-Enhancing Tecnologies: The Path to Anonymity Volume II". Ann Cavoukian
Disponible en: www.ipc.on.ca/images/Resources/anoni-v2.pdf

ISTEPANIAN, R. "Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-care Connectivity". IEEE Transactions on Information Technology in Biomedicine, 8(4), 405-413. 2004

Organización Mundial de la Salud . Reglamento Sanitario Internacional. 2005 . Segunda Edición. Ginebra 2008
Disponible en: http://www.who.int/ihr/es/index.html

PII, Personally identifiable information,
Disponible en: http://en.wikipedia.org/wiki/Personally_identifiable_information

P3P, W3C Technology and Society domain. Privacy Activity Statement..
Disponible en: http://www.w3.org/Privacy/Activity.html

SAINZ DE ABAJO Beatriz, P.C.Rodrigues Joel, GARCIA SALCINES Enrique, BURON FERNANDEZ F.Javier, CORONADO Miguel, DE CASTRO LOZANO Carlos. "M-Health y T-Health. La Evolución Natural del E-Health" . Revista e-Salud.com. Vol 7, No 25 , Disponible en: http://dialnet.unirioja.es/servlet/revista?codigo=14656

SEMAYNE Case. Wikipedia, the Free Encyclopedia

"Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea". Disponible en:
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es

The 25th Silver 59 Anniversary International Conference of the IEEE Engineering in Medicine and Biology Society . ISTEPANIAN R., LACAL. 2003

MAPHRE. Gerencia de Riesgos y Seguros, nº 112. 2012. "Risk Management drives credibility and Transparency"

Ministerio de Sanidad y Política Social. “Analisis de Requerimientos del Sistema, ARS. Historia Clínica Digital del Sistema Nacional de Salud”. vs. 2.8.1. 2010

National Commision on Terrorist Attacks upon the U.S. “The 9/11 Commission Report 394” . 2004

N. HUHNS Michael, P Singh Munindar. "Agent Jurisprudence". IEEE Internet Computing. March – April 1998.

Plan de Calidad para el Sistema Nacional de Salud. “Indicadores Clave del Sistema Nacional de Salud”. Marzo 2007

RUBENFELD Jed. “The Right of Privacy”. Faculty Scholarship Series. Paper 1569. 1989

SAMUEL, BRANDEIS. “The Right to be Alone”. December 1890

SARTOR Giovanni. "A Formal Model of Legal Argumentation". 1994

Universidad de Deusto. Derecho y Nuevas Tecnologías. 2011.

WTEC report. Bekey. et. al. 2006

NORMAS Y ESTANDARES

Agencia de Protección de Datos.

Codigos Tipo. Código Tipo de Farmaindustria.

Disponible en:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index- ides-

idphp.php

Elaboración de Códigos Tipo.
Disponibleen:
https://www.agpd.es/portalwebAGPD/canalresponsable/elaboracion_codigos_tipo/index-ides-idphp.php

Guía de Seguridad de Datos. 2010

Guía para una Evaluación del Impacto en la Protección de Datos Personales, EIPD. 2014

Informes Jurídicos:

253/2006, Responsabilidad de los ficheros en una sociedad médica

655/2008, Acceso a datos de salud por delegados de prevención

463/2009, necesidad de consentimiento del asegurador para que el corredor del seguro pueda seguir utilizándolos

CCN-STIC. Guías

801, Responsabilidades y Funciones en el ENS

802, Auditoría del Esquema Nacional de Seguridad

803, Valoración de Sistemas en el ENS

804, Medidas de Implantación del ENS

805, Política de Seguridad de la Informaación

813, Componentes Certificados en el ENS

815, Métricas e Indicadores. ENS

Disponible en: https://www.ccn-cert.cni.es

Código de Buenas Prácticas Clínicas. CPMP/ICH/135/95
Disponible en: http://ec.europa.eu/health/files/eudralex/vol-10/3cc1aen_en.pdf

Commission Nationale de l'Informatique et des Libertés, CNIL . Metodology for Privacy Risk Management. How to Implement the Data Protection Act. Edicion 2012

Comité de Ministros a los Estados Miembros. Recomendación CM/Rec (2010) 13 en relación al Profiling y la automatización de datos personales, (1099th meeting)

EDPS, European Data Protection Supervisor,

position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies,14 July 2014

Privacy Statement. Internal Market Information System – Imi

Grupo de Trabajo Gt29 en el relación a la Protección de Datos Personales D 95/46/CE. Documentos:

WP 12, Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive

WP 74, Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers

, WP 107,Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"

WP 133, Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data

WP 153, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules

WP 154, Working Document setting up a framework for the structure of Binding Corporate Rules

WP 155, Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rule

WP 195, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules

WP 196, Opinion 05/2012 on Cloud Computing

WP 199, Opinion 08/2012 providing further input on the data protectio reform discussions

WP 202, Opinion 02/2013 on apps on smart devices

WP 204, Explanatory Documetn on the Processor Binding Corporate Rules

WP 207, Opinio 06/2013 on open data and public sector information (PSI) reuse

WP 211, Opinion 01/2014 on the application of necessity and proponionality concepts and data protection within the law enforcement sectort Ad hic contractual clauses “EU data processor to non -EU sub-processor”

WP 214, Working document 01/2014 on Draf

WP 215,Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes

WP 217, Opinion 06/2014 on the notion of legitimattive interests of the data controller under Article 7of Directive 95/46/CE

WP 218, Statement on the role of a risk-based aproach in data protection legal frameworks

WP 223, Opinion 8/2014 on the Recent Developments on the Internet of Things

EU-OSHAS“A practical Guide European Agency and Health at Work”. Worker Participation in Occupational Safety an Health. 2012

IEEE,

IEEE Computer Society,

Guide for Developing Systems Requirements Specifications. IEEE Std 123

Guide for Software Quality Assurance Planning . ANSI/IECC Std 983-1986

Guide to the Software Enginneering Body of Knowledge, SWEBOK

Recommended Practice for Software Requirements . IEEE Std 830-1998

Information Commissioner's Office, ICO. Code of Practice. Data Protection Act. Conducting Privacy Impact Assessmentes . Version 1.0. February 2014

Instituto Nacional de las Tecnologías de las Comunicaciones, INTECO,

Curso de Introducción a la Gestión de Proyectos. Laboratorio Nacional de Calidad del Software. Junio 2009

Metodología de Certificación Common Criteria y Perfiles de Protección del DNIe.Mayo 2012

International Electrotechnical Commission, CEI/IEC 62304:2006 Medical device software – Software life cycle processes, Geneva, 2006.

International Health Terminology Standards Development Organisation.

Disponible en: http://www.ihtsdo.org/join-us/affiliate/

Interpol. Documento COM/FS/2012-02/FS-01

Ministerio de Hacienda y Administraciones Públicas. Agencia Estatal de Evaluación de las Políticas Públicas y la Calidad de los Servicios, AEVAL. Mejora de las organizaciones públicas por medio de la autoevaluación, CAF 2013

Organización Mundial de la Salud, OMS. La Farmacovigilancia : garantía de seguridad en el uso de los medicamentos. Perspectivas Políticas de la OMS sobre Medicamentos", WHO/EDM/2004.8. Octubre 2004

Project Management Institute, PMI, Norma Americana Nacional ANSI . PMBOK, Guía de los Fundamentos de la Dirección de Proyectos. 3º Edición. 2004

Systematized Nomenclature of Medicine, Snomed
Disponible en: http://www.ihtsdo.org/fileadmin/user_upload/doc/

The International Standard for Internationalization, ISO:

ISO/IEC 27001, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)

ISO/IEC 27002, Tecnología de la Información. Técnicas de Seguridad. Código para la Práctica de la Gestión de la Seguridad de la Información

ISO/IEC 27004, Tecnología de la Información-Medición

ISO/IEC 27799, Health Informatics. Information Security Mangement in Health using ISO/IEC 27002

UDA. Utilidades de Desarrollo de Aplicaciones v.1.0 Guía de Desarrollo . Eusko Jaurlaritzaren Informatika Elkartea, EJIE, Servicios Informáticos del Gobierno Vasco. Administración Electrónica del País Vasco. 06/06/2011

UNESPA. Código Inscripción Registro Agencia Protección de Datos *CT/0002/2000*

LEGISLACION

Declaración Universal de los Derechos Humanos, DUDH

Convención de Viena, de 18 de Abril de 1961, sobre Relaciones Diplomáticas
Legislación Europea en materia de Difusión de la Información
http://eur-lex.europa.eu/es/legis/latest/chap1620.htm

Convenio 108 de Estrasburgo, para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal

Constitución de 1978

Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen

Convenio de Schengen

Ley General de Sanidad L 14/1986 de 25 de abril

Ley Orgánica LO 3/1986, de medidas especiales en materia de salud pública

Decreto 272/1986 del Gobierno Vasco, por el que se regula el uso de la Historia Clínica en los Centros Hospitalarios de la Comunidad Autónoma del País Vasco

Ley 30/1992, de 26 de Noviembre, de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC)

Directiva 95/46/ CEE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Real Decreto 63/1995, de 20 de Enero, sobre Ordenación de Prestaciones Sanitarias del Sistema

Nacional de Salud

RDL 1/1996, de 12 de Junio, de Derecho Sui Generis

Ley de Propiedad Intelectual de 12 de abril de 1996

Directiva 96/9/CE en Protección de Bases de Datos

Convenio de Oviedo de 1997

Directiva 97/33/CEE, de 30 de Junio, relativa a la interconexión en las telecomunicaciones en lo que respecta a garantizar el servicio universal y la interoperabilidad mediante la aplicación de los principios de la oferta de la red abierta (ONP).

Convenio de Oviedo, de 1997, para la protección de los Derechos Humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina

Directiva 97/66/EC, de 15 de Diciembre de 1997, en lo que concierne al procesado de datos de carácter personal y de protección de la intimidad en el sector de las telecomunicaciones.
Ley 5/1998, Ley de Protección Jurídica de Base de Datos

Directiva 98/10/CE, de 26 de Febrero, sobre la aplicación de la oferta de red abierta (ONP) a la telefonía vocal y sobre el servicio universal de telecomunicaciones en un entorno competitivo.

Directiva 98/61/CE, de 24 de Setiembre, en lo que se refiere a la portabilidad de los números entre operadores y la preselección del operador.

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y su reglamento de desarrollo

Real Decreto 994/1999, el reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal.

D 31/2000/CEE, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado

interior

Reglamento (CE) no 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Decisión 2001/497, Decisión de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstos en la Directiva 95/46/CE

LSSI, Ley 34/2002, de 11 de Julio. Ley de Servicios de la Información y de Comercio Electrónico

Directiva 2002/19/CEE, de 7 de Marzo, relativa al acceso de comunicaciones electrónicas y recursos asociados, y a su interconexión.

Directiva 2002/20/CEE, de 7 de Marzo, relativo a la autorización de redes y servicios de comunicaciones electrónicas.

Directiva 2002/21/CEE, de 7 de Marzo, relativo a un marco regulador común de las redes y servicios de comunicaciones electrónicas.

Directiva 2002/22/CE, de 7 de Marzo, relativo al servicio universal y a los derechos de los usuarios en relación con las redes y servicios de comunicaciones electrónicas

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativo al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas Directiva sobre la privacidad y las comunicaciones electrónicas.

Directiva 2002/77/CEE, de 16 de Setiembre, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas.

Decisión 2002/16/CE. Obligaciones del Exportador de Datos, Decisión de la Comisión, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/

L 16/2003, de cohesión y calidad del Sistema Nacional de Salud

LGT, 32/2003, de 3 de noviembre, Ley General de Telecomunicaciones,

Ley 55/2003, de 16 de diciembre, del Estatuto Marco del personal estatutario de los Servicios de Salud

Ley 59/2003, de 19 de diciembre, de Firma Electrónica

Ley 2/2004, de 25 de Febrero, de Ficheros de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos

RD 183/2004 , por el que se regula la tarjeta sanitaria individual

Real Decreto 223/2004, de 6 de Febrero, por el que se regulan los ensayos clínicos con medicamentos

Reglamento (CE) n° 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros

Decisión 2004/915/CE, Decisión de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países

RD 2296/2004, de 15 de abril, que aprueba el Reglamento sobre condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Convección Europea para la Protección de los Derechos Humanos y Libertades Fundamentales

Decreto 308/2005, por el que se desarrolla la L 2/2005, de 25 de Febrero, de Ficheros de datos de carácter Público y de Creación de la Agencia Vasca de Protección de Datos

Real Decreto RD 424/2005, por el que se aprueba el reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, le servicio universal y la protección de los usuarios

Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios

Ley 1030/2006, por la que se establece la cartera de servicios comunes del Sistema Nacional de Salud y el procedimiento para su actualización

Real Decreto RD 776/2006, de 23 de Junio, por el que se .modifican el RD 1287/1999, de 23 de Julio, por el que se aprueba el plan técnico nacional de la radiodifusión sonora digital terrenal, y el RD 42/2005, de 15 de abril, por el que se aprueba el reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios

Directiva 2006/24/CE, de 15 de Marzo, sobre conservación de datos del tráfico en las comunicaciones electrónicas

Decisión de 28 de Junio C(2006)2009 que establece las especificaciones técnicas de los estándares de medidas de seguridad y biometría en pasaportes y documentos de viaje para miembros de los Estados Miembros

Directiva 2006/123/EC del Parlamento Europeo y del Consejo de 12 de Diciembre en Servicios del Mercado Interno

Orden SCO/256/2007, de 5 de febrero, por la que se establecen los principios y las directrices detalladas de buena práctica clínica y los requisitos para autorizar la fabricación o importación de medicamentos en investigación de uso humano

Orden ITC/1030/2007 del Ministerio de Industria, Turismo y Comercio por la que se regula el procedimiento de resolución de las reclamaciones entre usuarios finales y operadores de servicios de

comunicaciones electrónicas y la atención al cliente por los operadores

Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público

Ley L 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos

Ley L 14/2007, de 3 de Julio, de Investigación Biomédica

Ley L 15/2007, de 3 de Julio, de Defensa de la Competencia

Ley L 25/2007, de 18 de Octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes de comunicaciones.

Ley 37/2007, sobre reutilización de la información en el sector público
Ley L 56/2007, de 28 de Diciembre, de Medidas de Impulso a la Sociedad de la Información.

Real Decreto RD 1/2007, de 16 de Noviembre, que aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios.

Real Decreto RD 1344/2007, de 11 de Octubre, que regula la farmacovigilancia de medicamentos de uso humano

Real Decreto RD 1345/2007, de 12 de octubre, por el que se regula el procedimiento de autorización, registro y condiciones de dispensación de los medicamentos de uso humano fabricados industrialmente

Real Decreto RD 1720/2007, de 21 de Diciembre, que aprueba el nuevo Reglamento de Protección de Datos (RLOPD)

Orden SCO/362/2008, de 4 de febrero. Modifica la Orden SCO/256/2007, de 5 de febrero, por la que se establecen los principios y las directrices detalladas de buena práctica clínica y los requisitos para autorizar la fabricación o importación de medicamentos en investigación de uso humano

Real Decreto RD 261/2008, Reglamento de Defensa de la Competencia

Real Decreto RD 331/2008, de 29 de Febrero, por la que se aprueba el Estatuto de la Comisión Nacional de Competencia.

Volumen 9 A de las Normas sobre Medicamentos de la Unión Europea

Normas de Buena Práctica Clínica (CPMP/ICH/135/95)

Buenas prácticas de farmacovigilancia para la industria farmacéutica de medicamentos de uso humano

Instrucciones de la Agencia Española de Protección de Datos y Circulares de la Agencia Española de Medicamentos y Productos Sanitarios

Reglamento de la UPV/EHU para la protección de datos de carácter personal

Orden PRE/3523/2009, por la que se regula el Registro Electrónico Común

D 2009/136/CE , de 25 de Noviembre, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) Nº 2006/2004 sobre la cooperación en materia de protección de los consumidores

D 2009/140/CE, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/21/CEE relativa a un marco regulador común de las redes de comunicaciones electrónicas , la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas

RD 1671/2009, de 6 de Noviembre, por el que se desarrolla parcialmente la Ley 11/2007,de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos

Resolución De Madrid, Estándares internacionales sobre Protección de Datos Personales y

Privacidad

L 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos

Real Decreto RD 1093/2010, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud

Real Decreto RD 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Real Decreto RD 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

RD 207/2010, por el que se establecen las condiciones del uso tutelado de técnicas,tecnologías y procedimientos sanitarios, y se modifica el RD 1207/2006 por el que se regula la gestión del Fondo de Cohesión Sanitaria

RD 1093/2010 , por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud

RD 1718/2010, sobre receta médica y órdenes de dispensación

Directiva 2011/24/CE, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza

RD 1495/2011, por el que se desarrolla la Ley 37/2007, sobre reutilización de la información del sector público para el ámbito del sector público estatal

Orden HAP/566/2013, por la que se regula el Registro Electrónico Común

Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno

Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía

Ley 3/2014, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007

Ley 15/2014, de racionalización del sector público y otras medidas de reforma administrativa

RD 806/2014, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos

Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil

LIBROS

CALDER Alan, WATKINGS Steve. IT Governance. A Manager's Guide to Data Security and ISO 27001/ISO 27002. 4th Edition.

CANALES GIL, Alvaro y PIÑAR MAÑAS, Jose Luis. Legislación de Protección de Datos(adaptada a la Ley 2/2011). IUSTEL. 2011

CARNICERO JIMENEZ DE AZCARATE Javier. El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica. Thomson Reuters.Aranzadi.2009

DAVARA RODRIGUEZ Miguel Angel. Manual de Derecho Informatico .Editorial Aranzadi.2002

DEL PESO NAVARRO Emilio, RAMOS GONZALEZ Miguel Angel, DEL PESO Ruiz Mar. El Documento de Seguridad. Análisis Técnico y Jurídico. Modelo. IEEE,Informaticos Europeos Expertos. Ed. Díaz de Santos. 2004

Jurisprudencia Comentada Jurisprudencia de Telecomunicaciones. Editorial Aranzadi. 2008

MERINO BADA Cristina, CAÑIZARES SALES Ricardo. Implantación de un Sistema de Gestión de Seguridad de la Información según ISO 27001.Un Enfoque Práctico. FC Editorial. Fundación ConfeMetal. 2011

PIÑAR MAÑAS, Jose Luis (director) y autores varios. "Transparencia, acceso a la Información y Protección de Datos". REUS. 2015

PRESSMAN Roger. "Ingeniería del Software: Un Enfoque Práctico". 7º ed. 2010. University of Connecticut

SELLAS I Benvigut. El Régimen Jurídico del Teletrabajo en España. Ed. Aranzadi. 2001

SOMMERVILLE Ian. Ingeniería del Software. Ed. Pearson-Addison-Wesley. 7ª ed. 2005.

ULL PONT Eugenio.Derecho Público de la Informática. Protección de Datos de Caracter Personal. . UNED Ediciones. 2003

SOLOVE Daniel J. "Understanding Privacy". Harvard University Press, 2008