PROTECCION DE DATOS PERSONALES EN LA HISTORIA CLINICA.

EL DOCUMENTO DE SEGURIDAD EN LA NORMA ISO/IEC 27 002

LAMINA 1

El rótulo de la Tesis se presenta en dos fases que no separan sino que permiten integrar las facetas que la caracterizan: el *Derecho Informático* en la *e-Sanidad* desde su vertiente de la Protección de Datos, y el Análisis del Instrumento Jurídico que es el *Documento de Seguridad* en torno a los controles *ISO 27 002* que constituyen el Anexo de la norma *ISO 27 001* como garante certificable de un *Sistema de Seguridad del Sistema Informático, SGSI.* En realidad , no estamos sino profundizando en las especificaciones y requerimientos técnicos que la legislación nos aconseja practicar en la aplicación de *Medidas de Seguridad* conforme al *Esquema Nacional de Seguridad*, ENS, especificado en el *RD 03/2010,* que a su vez da desarrollo a la Ley que permite el acceso a los ciudadanos a la Administración Electrónica o *Ley 11/2007*.

Indice

- Taxonomías:

  Grupos Taxonómicos (incorporación ISO 27002)

- Escenarios (RD 1720/2007, Medidas de Seguridad):
  - Actores y Sistemas Informáticos, SIs
  - Orientación de Propuesta SGSI
- Gestión de Riesgos (ctrl. 15.2.1 ISO 27001):

  Motivadores Gestión del Cambio EVS, Indices-DocSeg

- El SGSI, Sistema de Gestión de la Seguridad de la Información

  Integración SGSI: Componente SW con especificación Control ISO 27002

LAMINA 2

El índice de la Tesis debe reflejar claramente una estructura que permita apoyar y versar la transversalidad del tema que nos ocupa, que no es una dificultad perseguida , sino que precisamente intenta ayudar a dilucidar las claras fronteras que existen entre el campo de las tecnologías y el de la legislación indicando contrafuertes de uno hacia el otro lado, pretendiendo simplificar en el Indice que presentamos, por un lado, el Método de introducción de los requerimientos legales en el Ciclo de Vida del Sistema Informático, y , por otro, participar de requerimientos técnicos, fundamentalmente en términos de Auditoría a la Doctrina legal..

La incorporación del estudio de un estándar internacional, y en este caso, pertenecientes a la familia ISO 27 000, normalmente condiciona en mayor o menor grado a expresar, al menos una *Taxonomía* que permita una especificación de un comportamiento deseado que no vaya mucho más allá de ella. Por lo que no debemos confundir que la necesidad de su expresión venga exclusivamente de una profundización de la aplicación y tradicción histórica de la Protección de Datos. Es una práctica usual en muchas de las áreas que abarcan las Ingenierías cuando se aplican estándares.

Puesto que nuestro objetivo es ir pautando el camino de la aplicación de las *Medidas de Seguridad* que minimicen o anulen el impacto de una *Incidencia* ocurrida sobre el *Activo* del *Sistema de Información*, que en este caso, es el dato clínico, debemos inicialmente reconocer todos aquellos *Escenarios* en los que se expresa la Operativa Sanitaria con una conexión directa en el *Tratamiento de los Datos Personales*, incluso cuando este se percibiera de forma aislada. En este punto aparecerán identificaciones concretas de responsabilidades de los *Actores* participantes, así como de Sistemas Informáticos con regulación propia más o menos desarrollada.

De entrada, la percepción del *Diseño* y *Análisis* de una *Salvaguarda Técnica* o *Medida de Seguridad* puede resultar un tanto abrupta para un profano , si no se maneja en el lenguaje concreto que trata la *Gestión de Riesgos*, su formulación legal, la Metodología empleada por la Administración Española en este caso, *Métrica* v. 3, y un estándar internacionalmente reconocido en Auditorías recomendado en ambos casos , como *ISO 27 001* en 'Tecnologías de la Seguridad' sobre el *Sistema de Información*. Analizados e incorporados todos estos aspectos, elevamos el *Riesgo* a 'Legal' por cuanto existe una clausula específica en *ISO 27 001*, en concreto la 15.1 que cita la persecucción de requerimientos legales, y cuando estos no se cumplen, nos encontramos expuestos con el consiguiente *Riesgo*.

Finalmente, y puesto que el Trabajo del estándar *ISO 27 001* es continuo sobre aquel Sistema que garantiza la Seguridad del *Sistema de Información*, no podemos dejar de recopilar aquellas integraciones que se van perfilando en el desarrollo de la Tesis sobre el *SGSI*. ISO *27 001* cuenta con un Anexo de una relación de *Controles* sobre los que se implementa y que, de no considerarse en la definición del *SGSI*, así deberá de indicarse en la denominada *Declaración de Confidencialidad*, donde aparece una relación completa de los mismos. El desarrollo semántico de dichos controles se encuentra recopilado en otro estándar, en este caso, no certificable, que es el *ISO 27 002* , y cuya expresión encuentra finalmente su localización en una propuesta a una Solución de un problema demasiado vistoso cuando se realizan los suficientes equilibrios en el conjunto de las conclusiones que se narran. Dicha solución no es sino un mero *Componente* Software, que nos ayuda en la comprensión de su Interoperabilidad en una visión más global del *SGSI*.

Tecnología de la Información.

Técnicas de Seguridad

ISO/IEC 27001- Sistemas de Gestión de la Seguridad de la Información(SGSI). Requisitos. (certificable)

ISO/IEC 27002- 'Código de Práctica' para el SGSI (no certificable)

ISO/IEC 27799- Health Informatics (línea de implementación: Telemedicina)

Ciclo de Deming P(Plan).D(Do).C(Check).A(Act)

LAMINA 3

En la finalización de la exposición de cada uno de los cuatro capítulos de los que consta la Tesis Doctoral, apuntamos a aquellas fases dentro del *Ciclo de Deming* que *ISO 27 001* e *ISO 27 002* desarrollan en la presentación de su Esquema de Clausulas o Controles. El Ciclo es conocido como de Planificación, Ejercicio, Revisión y Actuación en un proceso de Feedback hasta que resulte un óptimo la apreciación de la Seguridad del *Sistema de Información*.

Se recomienda siempre no utilizar el Esquema como una Checklist, sino como un apoyo flexible sobre el que apoyar la Auditoría, y acompañarlo, en lo posible, de algún otro estándar que lo relacione directamente con el área concreta sobre el que se desarolla. En este caso , y afortunadamente contamos con un buen punto de partida al reconocerse a *ISO 27 002* como un 'Código de Buenas Prácticas' en el *SGSI*, y a ISO 27 799 como una probable aplicación en el campo de los *Sistemas de Información* sobre los que se carga el dato médico. *ISO 27 002* resulta profuso , por tanto, en la exposición de los Controles sobre los que se apoya *ISO 27 001*, e *ISO 27 799* prácticamente un recordatorio en alguna línea de implementación concreta de la e-Salud , como puede ser la Telemedicina.

Indice: Cap.I, ejemplo de Taxonomias

Seguridad del Paciente:

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

Seguridad en el Trabajo del ISW:

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

LAMINA 4

Nos podemos preguntar a quién le puede costar más realizar el esfuerzo de desarrollar una Taxonomía, a un *Ciudadano* que se ponga en el lado hipotético de un Paciente, o a un *Ingeniero de Software* involucrado en alguna cierta medida en alguna responsabilidad del Tratamiento de Datos de la *Historia Clínica*? El ciudadano puede experimentar hasta una cierta sensación de bienestar al reconocer que no debe perseguir sino el sentirse igualmente de bien que en el momento que realiza su introspección y garantizarse ésta. Pero el *Ingeniero de Software* puede llegar a chocar con muchos tópicos, como el creer que un dato médico puede, a la larga, causarle algún daño indirectamente. Precisamente , esa falta de perspectiva y objetividad es la que intenta cubrir la Taxonomía que se publica, y contribuir , en lo posible, en la selección de este tipo de Recurso Humano.

No podemos, pues , concluir en este capítulo y hacer una crítica, que no se esté haciendo un esfuerzo aún no demasiado visible en los trabajos en el segundo campo mencionado, y sin embargo, sean profusos y saludables las Publicaciones sobre la *Seguridad del Paciente*, término reconocido para apuntar a su *Taxonomía*.

Ni tampoco se debe obviar los trabajos precedentes a lo largo de la historia en cómo las Sociedades han ido apreciando su *Privacidad*, pues en estas expresiones no reconocemos sino un escalón más hacia el estado del bienestar que hoy conocemos.

Es precisamente la *Historia Clínica* como prueba judicial la que consigue elevar a la HC a la transcendencia de respeto hacia su Administración electrónica, y el ejercicio de los *Derechos ARCO, de Acceso, Rectificación, Cancelación y Omisión,* resultan más claramente apreciables que en otras Secciones de la *e-Administración*.

El *Ingeniero de Software* con una suficiente y adecuada Formación en la legislación pertinente alcanzaría por su parte, el grado de tranquilidad que precisa.

Cap.I,

Ciclo P.D.C.A.

1.- Fase P(Plan): Ambito del SGSI

2.- clausulas 13, 13.2. 13.2.1 en ISO 27002:

responsabilidades y procedimientos en SGSI

Ejemplo:

- *Ciudadano*: amenaza fuga dato en la red
- *E-Técnico*: 'derecho al olvido' ---> ' right to be de-listed'
  (WP nº 223 Gt29 D 95/46/CE)

LAMINA 5

En consideración al *Ciclo de Deming* , también conocido como *P.D.C.A*, situamos el capítulo en la primera fase o correspondiente a la Planificación, donde se consigue iniciar la estructura de las funcionalidades en seguridad en relación al tratamiento de datos en el área de la e-Sanidad, y que, más adelante, puden convertirse , si se considerara certificable algúno de los Productos derivables de desarrollo de la Tesis en *Perfiles de Seguridad,* como reconoce el *Esquema de Certificación*.

Encontramos mencionables en este capítulo y en relación a la observación de la norma ISO 27 002 las clausulas numeradas siguientes:

- 13. Gestión de Incidencia en la Seguridad de la Información
- 13.2.Gestión de las Mejoras e Incidencias en el SGSI
- 13.2.1. Responsabilidades y Procedimientos

de especial interés, por cuanto en el análisis e identificación de la causa de la incidencia, en la especificación e implementación de la acción correctiva para evitar su recurrencia, una incorrecta interpretación de la *Taxonomía* puede derivar en una incorrecta selección de los recursos humanos y en las operaciones que practiquen.

La *Taxonomía de la Seguridad del Paciente*, recoge , además , algunas percepciones de comportamiento respecto del ejercicio de los *Derechos ARCO*, consentimiento informado, impugnación de valoraciones, responsabilidad civil, algunas otras de la esfera de la *Privacidad* (e.g. "a través de noticias, se hace consciente de que su información puede resultar accesible por otras personas"). Desde el lado de la Taxonomía del e-Técnico, y aunque no encontramos publicada una percepción equiparable, sí que aparece recogida en la finalización del texto de este primer capítulo una alusión recopilable, al recordarnos, tal y como se hace desde el documento de trabajo nº 223 emitido por el *Grupo de Trabajo correspondiente al Art. 29 de la Directiva de Protección de Datos, Gt29,* y en alusión a la 'Internet de las Cosas'. Dicha mención , y más concretamente, sobre los 'Smart Devices' utilizados en *Telemedicina*, puede hacer reconsiderar su postura a un e-Técnico al detectar que, efectivamente, existe la posibilidad de fuga de dato clínico en la red. Con lo que dicha nueva postura le reconfirme el refuerzo de su apoyo al impulso del ejercicio del 'Derecho al Olvido' , y haciéndose consciente de que el reconocimiento de urgencia de actuación debería posibilitar la regulación de un 'Right to be-DeListed' (término aparecido en una noticia publicada por el CNIL en

fecha de 18 de Setiembre de 2014).

Indice: Cap.II,

Marco Operacional en Gestión de Riesgos

(llevanza del documento de seguridad,
delegación de responsabilidades)

<<activo>>: dato HC (carácter estadístico, ctrl. 11.7.2. ISO 27002 Telemedicina)

Niveles de Seguridad , RD 03/2010. Anexo I:

<<perjuicio>>: limitado ..... bajo

grave ..... medio

muy grave ..... alto

Dimensiones de Seguridad (Resolución de Madrid, ENS, Métrica):

disponibilidad: "requerimientos informados" autorizan el acceso

autenticidad: garantía del origen de datos

integridad: modificación del activo con autorización

confidencialidad: disposición informada de la información

trazabilidad: imputación de autorización

LAMINA 6

Introducimos el Capítulo II con la siguiente apreciación: probablemente si en el inicio del dato médico se le hubiera reconocido a éste un mayor carácter estadístico como le corresponde, la regulación de la *Telemedicina* hubiera sido otra muy diferente, y la definición de los *Sistemas Informáticos Europeos* hubieran tomado otro aspecto. *ISO 27 002* sí que le presta su consideración a este tema en la *clausula nº 11.7.2* exigiendo, si cabe, una petición de mayor aseguramiento en la existencia de los controles de seguridad necesarios para asegurar el servicio que en otros ámbitos, reforzando la seguridad física (hardware), inventariando aquellas delimitaciones que garantizan su cobertura, y con importantes excepciones que nos plantean nuevas preguntas en el campo legal como puede ser el chequeo de la seguridad de un equipo que es de propiedad privada . Con esta indicación no pretendemos sino marcar la suficiente distancia respecto a las definiciones que en este capítulo se presentan y son extensas, y con el fin de resultar lo suficientemente flexibles para detectar otras posibilidades que, precisamente en el *Marco Operacional* de *Gestión de Riesgos* es necesaria por dejar el legislador abierta la determinación de las responsabilidades no sólo en la *Llevanza* del *Documento de Seguridad*, sino en la *Delegación de Responsabilidades* en el Tratamiento de Datos Personales, eso sí, proporcionando sus propias funcionalidades.

Cada elemento que tiene un determinado valor para el Sistema Informático, SI, lo denominamos *Activo*, siendo en la Administración de la *e-Sanidad* el dato médico el *Activo* por excelencia sobre el que la *Constitución* le caracteriza con un Nivel de Protección 'Alto' y al que le corresponde su supervisión, según el *art. 81 del RD 1720/2007 de Medidas de Seguridad* en el Tratamiento de la Protección de Datos.

Debemos realizar una pequeña aclaración en relación a la aplicación de estos niveles, por cuanto y fuera de la generalidad, el dato de discapacidad comunicado en una mutua , por ejemplo, está considerado se le aplique un nivel 'bajo' , así como a los perfiles de protección de determinadas cateforías profesionales sanitarias. Sin embargo, en el ahondamiento de las prácticas de seguridad que las Autoridades Reguladoras y Auditoras en materia de protección de Datos nos recomiendan practicar , figura un manejo más preciso de aplicación de dichas *Medidas de Seguridad* en torno a las posibles *Dimensiones de Seguridad* que pueden afectarse en relación a un *Activo* y debido a la *amenaza* analizada real de que se produzca una daño sobre el *Activo*, identificado como *Riesgo.* Debiendo producirse y diferenciarse *Capas de Seguridad* que respeten dichas Dimensiones. Entre estas , recordamos las que el Marco de la *Resolución de Madrid* decidió adoptar y que se ajustan a

las exigidas tanto desde la *Gestión de Riesgos* gestionada por la Administración Electrónica Española, denominada *Métrica*, como por el *Esquema Nacional de Seguridad*, anteriormente citado y el *Esquema de Interoperabilidad*, reflejado en el *RD 04/2010*, siendo ambos reales decretos desarrollos que dan cumplimiento a la *Ley de acceso electrónico de los ciudadanos a los Servicios Públicos, L 11/2007.* La noción de dichas Dimensiones aparecen mejor orientadas en los siguientes apartados :

1.- *disponibilidad*:

las entidades autorizadas tienen tienen acceso cuando los 'requerimientos informados' de la Operativa del Sistema de Información así lo determine. Pudiendo ser reconocido como Entidad, bien una persona fisica o jurídica, Organismo Oficial o Empresa. La recopilación del término requerimiento informado responde a la Doctrina de la denominada *Comisión del Mercado de las Telecomunicaciones, CMT*, y que actualmente se encuentra integrada en la nueva *Comisión Nacional de los Mercados y la Competencia , CNMC*. Es un término que encuentra su paralelismo con el de <<Requisito Informático>> proporcionado por el *Comité de Estándares de Ingeniería de la Sociedad de la Computación de la IEEE, Institute of Electrical and Electronical Engineer* , salvo que puede resultar punible su defectuosa especificación, y que están sometidos a una actualización cada dos años.

2.- *autenticidad*:

garantía del origen de los datos. En esta *Dimensión de Seguridad* cobra especial importancia la Arquitectura incorporada al 'Modelo de Datos', dejando la dependencia de tiempos y proporción de exactitudes al Estudio de dichos Modelos como algunos tipos aceptados de 'Federados' (ref. 172: Internet of Subject Foundations), etc.

3.- *integridad*:

el activo no ha sido alterado de forma no autorizada. Para su probatoria se cuenta con tecnologías y protocolos de seguridad reconocidos, Capas de Seguridad actuando en Background, y empresas a terceros como refuerzo de monitorizaciones.

En un supuesto de aplicación de esta dimensión de seguridad, nos obliga a reconsiderar una figura introducida en el *RD 1651/2008* (en lo relativo a la interconexión y al acceso a las redes públicas y a la numeración), que dió desarrollo a la *Ley 11/1998* (Ley General de Telecomunicaciones), y que se sustituyó por la *L 32/2003* , y conocida como *Grupo Cerrado de Usuarios* o *GCU*, y que no aparece reconocida en la estructura del *e-SNS*,

administración electrónica del *Sistema Nacional de Seguridad*. Convergemos con la *Sentencia de la Audiencia Nacionl, SAN* , de 10 de febrero de de 2004, en aplicar su definición:" una o varias personas físicas o jurídicas que se dedican a la realización común de una determinada actividad, de forma que sus equipos y terminales tienen por objeto el establecimiento de comunicaciones entre los componentes del grupo". Más adelante se expondrá la importancia de su correcta regulación y su relación con la *e-Sanidad*. Las *Políticas de Seguridad* que recogen esta figura adquieren una elevada complejidad, sobre todo, en relación a la determinación de los 'registros de acceso contemplados en regimenes de *outsourcing*. De modo, que en muchos caso, los *Acuerdos de Confidencialidad* se resuelven con la incorporación de dispositivos físicos, como puede ser el uso y manejo de tarjetas hardware.

4.- *confidencialidad*:

la información sólo se encuentra a disposición de entidades autorizadas.De modo que, podríamos crear clausulas contractuales y/o de procedimiento en cuanto a la generación de recursos gráficos en las interfaces a fin de que fueran exclusivamente visibles para aquellos 'perfiles VIP' que se establecieran y aplicables idénticamente, por protocolos regulados, tanto al Personal de la Categoría Profesional Sanitaria como al establecimiento de Sustituciones por diferentes causas entre la plantilla de *Ingenieros de Software*.

5.- *trazabilidad*:

las actuaciones de una entidad puden ser imputadas exclusivamente a dicha entidad. En este caso , la *Política de Firmas Electrónicas*, reconozco, deberá elevarse aún más en el mapa de la nueva <<Gobernanza>> de la Administración electrónica, configurada desde la publicación en el *Boletín Oficial del Estado,* en el *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*. En el texto de la Tesis la definición de la *Firma Electrónica* se realiza conforme al *art.3 de la L 11/2007* , destacándose como prueba documental de soporte según el *art. 51 de la L 56/2007* de *Medidas de Impulso de la Sociedad de la Información,* y que encuentra su específica regulación en la *L 59/2003*. Siendo el objeto doble de protección en *salud pública* y en relación a personas jurídicas que tengan la condición de *consumidores* y usuarios.

Por su parte, el *art. 33* correspondiente al *RD 03/2010* por el que se regula el *Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica,* postula que la 'Política de Firma Electrónica' concretará , además, los procesos de generación, validación y conservación de firma , los servicios de sellado de tiempo, y otros elementos de soporte de las firmas como el envío de ficheros por e-mail o fax. Debiendo 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 RD 1720/2007 de desarrollo de la LOPD*, exigiendo en un Nivel Medio el conocimiento de la información de envío , y en un Nivel Alto, *art.101*, el cifrado de datos.

La determinación de un *Nivel de Seguridad* en una *Dimensión* elevará su consideración en la *Categoría*.

Por otra parte, podemos exigir una menor complejidad a la aplicación de dichos Niveles si nos adscribimos a la definición escueta de cada nivel, a saber y actuando sobre el Activo:

1.- *Bajo*:

suponiendo un perjuicio 'limitado'

[El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable]

2.- *Medio*:

supongan un perjuicio 'grave'

[El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.]

3.- *Alto*:

supongan un perjuicio 'muy grave'

[El incumplimiento grave de alguna ley o regulación]

Indice: Cap.II, SIs y Autorizaciones

Delegación de Responsabilidades en e-Sanidad: RD 223/2004, Código de Buenas Prácticas Clínicas, v. 2002

Binding Corporate Rules, BCRs o Reglas Corporativas Vinculantes (Controlador , Pocesador)

*El Supervisor Europeo de Protección de Datos (*EDPS)

*Sistemas Informáticos Europeos como el IMI (*Lisos)

*Marco Nacional de Seguridad e Interoperabilidad (*responsable de información, de seguridad, de fichero*)*

Agencias Españolas de Protección de Datos, APDs (Director, responsable de Ficheros)

*Gobernanza de la Administración Electrónica(*Dirección Tecnologías de la Información, Comisión de Estrategia TIC,CMAD, Unidades TIC*)*

*El Sistema Nacional de Salud, SNS(*Investigador, Asistente e-Sanidad, ISW, CEIC, Agencia de Medicamentos*)*

*Farmacovigilancia(*Promotor, Monitor*)*

Regulaciones SIs Europeos:

Decisión Comitológica 1999/468/CE .....> req. Informado (ANR: Control de Introducción de Schengen)

1.- Artículo Publicado Anexo 2: “La Semántica ...”

2.- Solución Control PDCA: Seguridad en el Trabajo del ISW

LAMINA 7

Detectamos , por tanto , en la forma de aplicar *Niveles de Seguridad* además de la complejidad que encierran, la habilitación de los permisos de *autorización* en clave de 'acceso' al Sistema de Información. De momento es el *RD 223/2004 por el que se regulan los ensayos clínicos con medicamentos*, así como el *Código de Buenas Prácticas Clínicas* los que resuelven dichas autorizaciones en cuanto identifican de forma oficial, aquellos *Actores* o *Perfiles de Acceso* que son reconocidos en el ámbito de la *e-Sanidad*. Para el caso de la *Telemedicina* debieran considerarse procedimientos y protocolos específicos a tal fín.

Otra posible forma de obtener la especificación de dichos *Actores* o Entidades, por emplear una palabra de la *Ingeniería del Software*, ya que nos estamos moviendo en la esfera del Diseño y Análisis del Sistema de Información, sería acudiendo a las regulaciones de los Sistemas Informáticos hábiles en el Espacio Europeo, que es donde inicialmente se experimenta y persigue la *Interoperabilidad*. Sin embargo , bien sea por la forma de afrontar la *Decisión Comitológica* , procedimiento de reglamentación *1999/468/CE,* que, por ejemplo, no hace una alusión directa a determinados Sistemas Informáticos como puede ser el correspondiente al del *Mercado Interior, IMI,* como posteriormente aludiremos, o bien porque internamente desde cada Estado se considera subjetivamente que es mera competencia pública con responsabilidad de las Autoridades Reguladoras, no encontramos esta indicación.

Con lo que , y no queriendo dejar tan huérfana nuestra obra, se decide , como se aprecia en el *Artículo 2* del *Anexo* de la *Tesis* potenciar alguna de las premisas o especificaciones que caracterizaron el inicio de los Sistemas Informáticos Europeos, aludiendo al denominado *Control de Introducción* del que la Agencia de Protección de Datos es responsable desde la parte nacional del *Sistema de Schengen*.

Observado el curso de dicha publicación en el tiempo se decide, en consecuencia potenciar su aplicación en la Solución que se propone como ejemplo en la Semántica de los Controles de la norma *ISO 27 002*, y que confiere uniformidad no sólo al escrito, sino a la integración del *Sistema de Seguridad del Sistema de Información* que se va perfilando a lo largo del texto. *ISO 27 002* es una norma o estándar internacional no certificable que desarrolla los controles que son *Anexo* de la norma sí certificable *ISO 27 001* en 'Técnicas de Seguridad' implementables sobre un hipotético *Sistema de Seguridad del Sistema de Información*. Al desenvolvernos en el campo de la *Protección de Datos* y, concretamente, al reconocer la legislación la necesidad de aplicar *Medidas de*

Seguridad para perseguir tal fin, esta es una de las normas mayormente auditadas en nuestro territorio a día de hoy.

Se expresa a continuación el Esquema Supranacional que se debe considerar, ampliando esta consideración a la de Transferencia Internacional de Datos:

- *Binding Corporate Rules, BCRs o Reglas Corporativas Vinculantes*:
  Tradicionalmente, y en el ámbito de las Multinacionales son clausulas que se resuelven de mutuo acuerdo entre delegaciones del mismo o diferentes Estados, aplicando , en lo posible, la caracterización jurisprudencial que se les presume. Es en este espacio, donde inicialmente surgen las Figuras del *Controlador* y del *Procesador* elevadas a la máxima exposición en el Documento de Trabajo *n º WP 195* del Grupo de Trabajo *Gt29* de la *Comisión Europea* correspondiente a la articulación de la *D 95/46/CE,* y que, de existir su delegación, el formato de la relación deberá resultar cotractual.

- *El Supervisor Europeo de Protección de Datos, EDPS*:
  Como máximo supervisor de la Administración Electrónica en su conjunto, y consejero en *Políticas de Seguridad* para la Comisión Europea. Cuenta con la interlocución del Controlador .

- *Sistemas Informáticos Europeos como el IMI*:
  Aparece en este Sistema de Información, la figura del *Liso*, *Local Informatics Security Officer*, que aplica la denominada *Privacy Statement,* Clausula de Privacidad, sobre los *Derechos ARCO* cubriendo las responsabilidades sobre los Estados Miembros. Su reglamento ,además, de realizar una apuesta definitiva por *ISO 27 001*, amplia su ámbito de aplicación al del *Teletrabajo,* como primera clara referencia en este campo.

- *Marco Nacional de Seguridad e Interoperabilidad*:
  El *Documento 801* del *Centro Criptológico Nacional, CCN*, 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. La *Política de Seguridad* de la Organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos. El *art. 10* del *ENS*, *RD 03/2010*, *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 *Análisis de Riesgos* establecido en su *Anexo II* 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 de Seguridad* que recoge la especificación completa de las Medidas de Seguridad implementadas, pudiendo solicitar mejoras del mismo. El Documento estará a disposición de los *Auditores*.

Si se hubiera contratado la prestación de servicios con la totalidad o parcialidad de ficheros, en el contrato celebrado al amparo del *art. 12 de la LOPD* con especificación de los ficheros trasladados, el *art. 88* se refiere a la delegación de dicha llevanza, apoyada a su vez, por la especificación que proporcional el *RD 1720/2007*, *art. 81, 82, 84, 86* y *Título VIII, cap. II y III* (niveles de seguridad).

Además, 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 y enténdiéndose por este término la responsabilidad de monitorización y responsabilidad de actuación en su salvaguarda.

- Agencias Españolas de Protección de Datos, APDs:

  No solo auditarán sino registrarán aquellos *Ficheros* que siendo oficialmente publicados en el *Boletín oficial del Estado*, cuenten con datos médicos, incluidos los de Centros de Investigación o Función Estadística como los provenientes de los Proyectos de Investigación de las Universidades, y cuyas reglamentaciones deberán supervisar. También encuentran su protagonismo en los permisos de transferencias internacionales de datos.

- *Gobernanza de la Administración Electrónica*:

  Existe una declaración de los proyectos de 'interés prioritario', en los términos establecidos en el *art. 11 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*)*, a propuesta de los ministerios y sus organismos públicos adscritos previo informe de la *Dirección de Tecnologías de la Información y las Comunicaciones* elevado este desde la *Comisión de Estrategia TIC*. Existiendo así mismo *Comisiones Interministeriales y Unidades TIC,* por Sección.

- *El Sistema Nacional de Salud, SNS*:

  Encuentra en este espacio la figura del *Investigador* una mayor aplicabilidad que lo que puede resultar el ámbito privado de la Farmacovigilancia, encontrándose con un denotada

responsabilidad en torno al *consentimiento informado ,* resultando supervisor de los mismos , interlocutor con el *Comité Etico de Investigación Cínica,* y con responsabilidad sobre la Formación en 'Seguridad del Paciente' sobre el ciudadano.

- *Farmacovigilancia*:

  Resulta el Promotor responsable de la contratación del *Seguro de Responsabilidad* . 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 (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 externos), y así mismo, responsable del aseguramiento del *Plan de Calidad*.

  En el escenario de Farmacovigilancia se habrá de declarar un fichero que recoja todos los 'acontecimientos adversos' que se fueran produciendo.

Cap. II,
Ciclo P.D.C.A.

1.- Fase P(Plan):

Escenario de la Aplicabilidad

Fase A(Hacer):

Formación de la Plantilla, Gestión de Operaciones con el SGSI

2.- clausula 7.10.1 , ISO 27799:

Reporte de la incidencia (intercambio de información, Seguridad en el Soporte: control crítico 7.7.10 de logging y monitorización)

Ejemplo:

Extenso desarrollo de la *Seguridad del Paciente*

Consideraciones del Indice (integración de Sistemas, aumento de la Interoperabilidad(alarmas), regulación de la Telemedicina)

LAMINA 8

Creemos haber encontrado una razón para justificar positivamente la mayor difusión que encuentra la Taxonomía denominada *Seguridad del Paciente*, expresándola a continuación:

La clausula *7.10.1* de la ISO *27 799* viene a confirmarnos lo mismo que la sinopsis del *Ciclo P. D.C.A* que se observa en el desarrollo del capítulo: los escenarios de aplicabilidad y la formación de la plantilla en base a las operaciones del *SGSI*. Recuerda que aquellas organizaciones involucradas en el cuidado de la Salud deberían desarrollar procedimientos con el objetivo de proporcionar rápido soporte en la resolución de incidentes, produciendo efectivas actuaciones en los tiempos y circunstancias adecuadas y recopilando aquella información adecuada a fin de generar logs de auditoría. Postula que dentro de las Incidencias de la Información de la Seguridad se considera la 'corrupción personal' con la consiguiente inhabilitación de parte o la totalidad del Sistema de Información, razón por la que debemos reforzar la acción en la parte de la *Seguridad del Paciente* o 'Patient Security'.

Con la misma lógica el estándar apunta a la regular evaluación de las contramedidas adoptadas midiendo su eficacia.

Acompañando al esquema *ISO 27 001*, contamos con el primero de los apoyos documentales proporcionados desde la *Agencia de Protección de Datos* para mitigar o hacer desaparecer en lo posible el impacto ocsionado por un riesgo activo sobre el *Sistema de Información*, y que especialmente se aconseja implementar en caso de transferencias de datos a países fuera del espacio europeo, por cesiones o comunicaciones a terceros a países, cunando se consideran datos de menores, por compromiso con las *Dimensiones de Seguridad*, inevitable en redes de Telecomunicaciones, etc. En definitiva, si consideramos el espacio abierto de las transferencias internacionales en el ámbito sanitario y por aplicación del nivel de seguridad 'alto' que caracteriza al dato médico, no podemos dejar de practicar este tipo de solución, refiriéndonos a lo que con anterioridad al reconocimiento por la Autoridad Reguladora conocíamos como *Privacy Issues Assessments* o *PIAs*, y ahora como herramienta de evaluación de impacto en la Protección de Datos o *EIPD*.

Más aún, la aplicación en la *salud informática* de la norma *ISO 27 002* y complemento de la misma, *ISO 27 799*, nos indica 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 todas formas y aunque apliquemos un *P.D.C.A* sobre la propuesta no debemos olvidar que en relación a las clausulas de la *ISO 27 002* y el Servicio Informático Sanitario, se considera de mayor necesidad de observaciçon y vigilancia:

1. I*ntercambios de Información*:
2. *Seguridad en el Soporte y Procesos de Desarrollo*:

Y de todos los requerimientos relacionados con la seguridad del dato clínico, nos confirma la clausula 7.7.10 de Monitoreo en la ISO *27 799*, que, entre los más importantes se cuentan con los de:

• auditoría
• logging

Efectivamente, un 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.

A los derechos que se citaron desde a perspectiva de la *Seguridad del Paciente*, se ha añadido una exposición de la 'autodeterminación por consentimiento' y que, en el área de la Asistencia Médico-Sanitaria encuentra el mínimo rechazo.

Se amplia el concepto de la 'Responsabilidad Técnica y Legal' con la introducción del

'reconocimiento por representación' , de modo que podemos hablar del 'Documento de Instrucciones Previas'.

La regulación específica de la *Telemedicina* no provocará sino el desarrollo de la segunda Taxonomía, algo obvio desde la observación de la aplicación del Caso Práctico de un 'Grupo Cerrado de Usuarios o GCU' (resultando un supercontrol en el ámbito mencionado).

Con la aparición y detección de los actores de la *e-Sanidad* aparecen otras competencias que las meramente expresadas en las *Taxonomías*, como son el responsable del fichero, el cuadro de dependencias en la monitorización del consentimiento informado, las responsabilidades del mapa de transferencias a terceros países, la contratación o no de un 'seguro de respinsabilidades' en la Farmacovigilanacia,etc.

En cuanto a la presentación en el Indice de la Tesis de los Sistemas Informáticos, cabe imaginar, que el modo en como se alude a la 'Vía Marítima', 'Vía Aérea', la 'Protección de Menores', etc, y debido a la integración e interoperabilidad que se presume se vaya produciendo en los Sistemas, no aprarecerán estos como Sistemas aparte, sino como parte de la especificaicón de un 'Sistema Superior'.

Y, aunque en el Sistema de Alertas , por ejemplo, en torno a acontecimientos adversos se aproxima un poco más al modelo americano (con completa inclinación en su especificación hacia la figura del consumidor) , continúa siendo el IMI el más avanzado en cuanto a recopilación de requerimientos informados en Telemedicina, al menos de forma pública, (e.g. Formulario de Pregunta-Aplicación de los Derechos de los Pacientes en la Asistencia Transfronteriza)

Indice: Cap. III

Gestión de Riesgos ---> Riesgo Legal

riesgo

(cuantificables: probabilidad, amenaza, daño, activo, impacto)

activos (Magerit v.3)

Sistema Informático, SI	Sistema de Seguridad del SI, SGSI
<<activo: dato clínico>> <<nivel de seguridad: alto>>	<<salvaguarda técnica o medida de seguridad>> <<dimensiones de seguridad>>

LAMINA 9

Se debe iniciar este amplio capítulo con la introducción del concepto de <<riesgo>>, siendo este considerado como aquella <<probabilidad>> de que una determinada <<amenaza>> identificada produzca un <<daño>> sobre algún <<activo>> del sistema que estemos considerando. Los elementos riesgo, probabilidad, amenaza y daño deben resultar cuantificables, por tanto, pudiendo hablar idénticamente del <<impacto>> del riesgo.

Considerando que el *Sistema Informático, SI*, que se está analizando es un *Sistema de Seguridad* del propio Sistema, bajo la garantía de una certificación de la norma *ISO 27 001*, válida por tres años, observamos que es el dato del sistema, en nuestro caso, el dato clínico, el que debe resultar protegido de no ser borrado, de ser accesible y sólo por aquellas personas con un perfil aceptado desde *Códigos Tipo* internacionales, de poder ser recuperado, de poder ser cedido o comunicado y de poder ser auditado. Precisamente es el dato clínico el propio activo del sistema, consideración que se obtiene tal y como lo hace la metodología de *Gestión de Riesgos* de la Administración Española, *Magerit*, hoy en día en su versión 3. Esta metodología la que nos conduce a afirmar que el *Sistema de Seguridad del Sistema de Información, SGSI*, es un *Activo* del Sistema global y que el Sistema completo se puede tratar como un único activo.

Así mismo, este activo , el *SGSI*, es una *Medida de Salvaguarda Técnica* que debe respetar y dar respuesta a la protección del tratamiento de datos clínicos, datos personales a su vez, pero a los que la Legislación en tal materia le concede un *Nivel de Seguridad* 'Alto'.

A su vez, cada *Salvaguarda Técnica* que conforma un *SGSI* da respuesta a la Gestión de , al menos un riesgo, o encadenamiento de ellos, que afectan de diferente formas cada *Activo* en las *Dimensiones de Seguridad* reconocidas por Métrica: Disponibilidad, Integridad, Confidencialidad y Autenticidad y Trazabilidad.

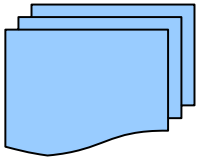
Indice: Cap. III

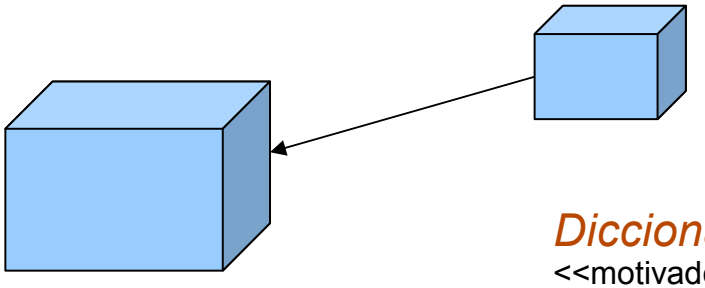
Sistema de Configuración del SI, SGSI

EVS,

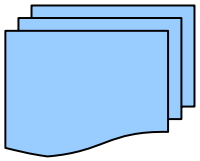
Estudio de Viabilidad del SI

Herramienta CASE





Documento de Seguridad



Diccionario

<<motivadores, categorías>>

Ejemplo GCU:
(Cap. III):
estructura e-SNS
(Cap. IV):
derechos del Consumidor

Certificable (ISO 27001, controles 27002)

Auditable (Guías CCN, AEPD)

{ estructura de ficheros, relación de ficheros

Medidas de seguridad, llevanza del documento

(ENS, a. 12 LOPD, RD 1720/2007) }

LAMINA 10

Cuando en alguno de los *Servicios Informáticos, SIs*, que soportan las diferentes Comunidades Autónomas se procede a iniciar un Proyecto que proporciona Solución a alguno de estos Riesgos, de entrada, debe de existir un denominado *Estudio de Viabilidad del Sistema, EVS*, que puede haber sido registrado con precedencia y tiempo en el *Sistema de Configuración* del *SI*. En términos de la *Ingeniería del Software* esto supone una <<Modificación>> del Sistema que precisa de su correspondiente gestión o *Gestión del Cambio*.

En la adecuación y aplicación de la Legislación en materia de Protección de Datos, se recopilarán ,de antemano, (normalmente desde una *Herramienta CASE*), aquellas posibles Entradas o *Motivadores* de la *Gestión del Cambio* en el correspondiente *Diccionario* del *SGSI*, siendo función de un buen *Analista Funcional* en la estructura del Servicio Informático, contratado o no en régimen de *Outsourcing*, el responsable de extraer, habida la legislación, dichos *Motivadores* recopilados por *Categorías* que identifiquen el *Histórico* del Cambio (existe motivación del momento).

Las *Categorías de los Motivadores de la Gestión del Cambio en un Estudio de Viabilidad del Sistema* precisan de la recopilación completa de la legislación afín, así como la identificación de la respuesta en un entorno supranacional o marco que pueda conllevar, de primeras, el *Marco de Interoperabilidad* aprobado en nuestro *Esquema Nacional de Seguridad, ENS*.

La Metodología utilizada para determinar los *Motivadores* es la que se expone:

- extracción y actualización de aquella legislación directamente relacionada con la protección de datos en el ámbito de la historia clínica

- de cada relación publicada en el *Boletín Oficial del Estado, BOE,* extracción de aquel contenido que, bien por otorgar diferenciación o, bien carácter marcado a la legislación , la denota, siendo esta una aportación identificada en el *Ciclo de Vida de la Aplicaciones Software* como *Especificación de Requisito* , desde la perspectiva de la *Ingeniería del Software*, o bien como *Requisito Informado* como se precisa en el contexto más amplio de las Telecomunicaciones, *CMT*

- Elevación Funcional de la expresión de la anotación asociada a cada legislación, considerando que nos estamos refiriendo al agente principal motivador del Cambio en la *Especificación* de un *Sistema Informático, SI*. En nuestro caso, llamamos *Categoría* de los Motivadores de la Gestión del Cambio a aquellas 'líneas de definición' que pautan fuertemente el *Indice* de la Tesis, en concreto 24 categorías identificadas.

- Cada anotación, con su correspondiente identificador y categoría asociada se considerará un elemento/item del *Diccionario* de *SGSI*, estructura sobre la que trabajará la norma ISO 27 001

Por su parte, el establecimiento de las *Categorías de los Motivadores de la Gestión del Cambio* ayudarán al *legislador* en su labor de priorizar A*gentes*.

La legislación nos dice, que la existencia de *Medidas de Seguridad* en el Tratamiento de Protección de Datos exige la existencia de un Instrumento jurídico, esto es, auditable desde al menos dos Organismos, como son la *Agencia de Protección de Datos, APD*, y el *Centro Criptológico Nacional, CCN*. Dicho instrumento se denomina *Documento de Seguridad*, exigible en cualquier caso en el Nivel Alto de Seguridad aplicado al dato correspondiente a la Administración Electrónica Sanitaria o *e-Sanidad*.

En el *Documento de Seguridad* figurarán y desarrollarán las características de dichas *Medidas de Seguridad*, la legislación que se les aplica, así como la relación y estructura de los *Ficheros* afectados , conjuntamente con la identficación de las diferentes responsabilidades en materia de protección de datos.

Aun cuando la 'llevanza del documento de seguridad' es una cuestión a resolver desde el *Marco Organizacional*, este capítulo de la Tesis no le dedica mayor desarrollo por cuanto en los Capítulos I y II se recopilan el conjunto de los Escenarios en el que se desenvuelven los *Actores* identificados con sus correspondientes responsabilidades, y en el Capítulo IV se manifiesta y se suma un análisis practicado desde la perspectiva que nos proporciona el *Documento WP nº195 correspondiente al Grupo de Trabajo Gt29*, que resuelve la *Directiva D 95/46/CE*. Este documento es símbolo y sinopsis del trabajo completo que se realiza en torno a las responsabilidades funcionales identificadas en el ámbito de las transferencias internacionales por dicho Grupo de Trabajo a lo largo de los años. Por lo tanto un recuerdo, de que son las funcionalidades las que deben ser escrupulosamente

respetadas y el número de delegaciones no implicaría una mayor corrección en su aplicación.

Repartidos en los capítulos precedentes hemos presentado dos casos prácticos de 'Motivadores de la Gestión del Cambio':

Cap. III) estructrura tecnológica del *e-SNS*
Cap. IV) defensa del consumidor

Por otro lado, la aplicación y análisis de un requisito legal aparece como ejemplo en la T*abla 5*, representando un mero *checkbox*.

Se pretende indicar que, aunque en principio, podemos englobar diferentes problemas de forma genérica bajo el rótulo 'Defensa del Consumidor', suponiendo un conjunto extenso de recursos en una interfaz gráfica, con sus consiguientes motivadores y categorías asociadas por recurso gráfico. Este es el grado de finura de diseño al que nos debemos de referir, pudiéndose encontrar en una misma página (aludiendo a la web), diferentes categorías y motivadores asociados a la existencia de cada recurso.

Cuando en el capítulo II desarrollamos la noción de la 'Dimensión de Seguridad' conocidad como Integridad, incorporamos la figura del *Grupo Cerrado de Ususarios, GCU*. Pues bien, esta figura , o mejor dicho , la implementación del *GCU* requiere de la combinación de la presentación de ambos ejemplos. A esta complejidad, se le suma la actuación de la jurisprudencia que sobre ella versa, a saber, el derecho sancionador y la defensa de la competencia.

En el caso europeo, las normas de la competencia se basan en los *art. 81 y 82* del *Tratado del Comunidad Europea,* CE. El principal objetivo es promover la eficiencia económica y el bienestar social evitando que las empresas con poder de mercado lo ejerzan en detrimento de la eficiencia económica y el bienestar de los consumidores.

Podría suceder, en la recopilación de las especificaciones de este caso práctico , que la elevación de la petición desde el *Consejo de Consumidores* estuviera solicitado por la aplicación de la 'Justicia impulsada desde Asociaciones', como proyecto-piloto de *Caso de Uso*.

Indice: Cap. III,
Documento de Seguridad-Indices

Taxonomía del Ciudadano:

Autodeterminción por Consentimiento, Impugnación por Valoraciones, Consentimiento Informado

Taxonomía del e-Técnico:

Documento de Seguridad

Ind.1.- Formato

Ind.2.- Política de acceso: registros

Ind.3.- Soportes: selección y albergue

Ind.4.- Modelo de datos: normas de etiquetado

Ind.5.- Aseguramiento del Plan de Calidad (HW, SW)

Ind.6.- Unidades lógicas: ficheros

Ind.7.- Periodicidades: Informes

Ind.8.- Estándares: Semántica Aplicada

Ind.9.- Responsabilidades de Supervisión en el Tratamiento de Datos

Ind.10.- Auditorías

Expresiones

Semánticas

De una Solución

Ejemplo: BBDD

LAMINA 11

De idéntica forma que desde la perspectiva del Paciente podemos esgrimir la Defensa de los *Derechos ARCO*, el derecho por *Impugnación de Valoraciones* y el *Consentimiento Informado* como elementos de derecho a analizar y ejercer, idénticamente el e-Tecnico, más comunmente conocido como *Ingeniero de Software* encuentra en el Soporte y Mantenimiento del *Documento de Seguridad* el instrumento jurídico sobre el que debe profundizar en conocimiento y aplicación a fin de poder garantizar una protección de datos de carácter personal adecuada en el *Sistema de Información* sobre el que opera.

Con la perspectiva semántica que nos permite la extracción de unos determinados índices-constantes de las Guías emitidas desde la *Agencia de Protección de Datos* a fin de elaborar y mantener un *Documento de Seguridad*, queremos garantizar la expresión de posibles discusiones de dichos Documentos en un proceso de feedback que no deje indiferente, por no dominarlo holísticamente, la observación de ninguna parte constituyente del *Sistema de Información*, en nuestro caso *SGSI*.

Pongamos un ejemplo: como albergue de datos, una *Base de Datos* se conforma como un Soporte tanto lógico como físico que precisará de las consiguientes *Medidas de Seguridad* dentro del *Plan de Gestión de la Seguridad del Sistema Informático.* En este caso, la aplicación del denominado *Indice* 'Soporte' quedará aparentemente redundante en cuanto a su definición, más lo que se impone es una elevación de una de sus características, pidiéndose, en este caso, la CERTIFICACION del NO REPUDIO de la aplicación de un determinado 'Nivel de Seguridad', pudiendo ser observado, i.e., en la acualización de un dato separado. La elevación de la aplicación de la Semántica es, además, un tema recurrente en el ámbito de la Sanidad, como idénticamente practicamos en el *Artículo* publicado *2* del Anexo de la Tesis, y la expresión de estos Indices aplicados deberán practicarla.

Cap. III,
Ciclo P.D.C.A.

1.- Fase P(Plan):

Procedimientos(Incidencias),

Política deSeguridad(RD263/2006: precepto legal de Gestión de Riesgos)

Valoración y aceptación de Activos (Diccionario y Métricas),

Opciones tratamientos Riesgos

Fase D(Hacer):

Plan Tratamiento de Riesgos y Salvaguardas

Fase C(Revisión):

Monitorización y Auditoría

2.- clausula 7 ISO 27001:

revisiones del SGSI

Ejemplo:

Desarrollo Taxonomía e-Técnico: consentimientos en GCU

Control de Registros(4.3.3) y de Documentos(4.3.2): motivadores, etc.

LAMINA 12

La clausula nº 7 de la *ISO 27 001* dice que a fin de poder implementar las sucesivas revisiones de un *SGSI* la información de la gestión deberá contemplar técnicas, productos y procedimientos dedicados a la mejora del comportamiento y eficacia del *SGSI,* además, el estado de las medidas preventivas y correctivas, los resultados de patrones eficaces , así como el seguimiento de versiones existentes.

Con esta aclaración podemos corroborar que el capítulo III debe poder contener tres de las cuartas fases del *Ciclo P.D.C.A*, tal y como se expone en la diapositiva.

Una *Sentencia del Tribunal Supremo, STS*, de 14 de febrero de 2007 nos recuerda un par de cosas, en relación al *Grupo Cerrado de Usuarios, GCU*:

> 1.- la *Comisión del Mercado de las Telecomunicaciones, CMT*, debe extremar el rigor en la salvaguarda día a día de los intereses público spara evitar dar respuesta a aquellas prácticas que pueden desnaturalizar la finalidad a que atiende este tipo de servicio de valor añadido
>
> 2.- La compañía debe proceder a verificar las condiciones de configuración del *GCU*, recabando la aportacion formal del *consentimiento* de las entidades o clientes asociados adscritos.

Se retoma la noción del consentimiento desde la parte de la Taxonomía del e-Técnico, y elevamos su consideración por cuanto, además, en España, la regulación de las Autoridades de Regulación de las Telecomunicaciones no recae sobre un único (recogidas en el *art. 46* de la *Ley General de Telecomunicaciones o L 32/2003*: el Gobierno, Organos Superiores del Ministerio de Ciencia y Tenología, Organos Superiores y Directores del Ministerio de Economía, la CMT y la Agencia Estatal de Radiocomunicaciones).

Se apunta como dato curioso, que el año correspondiente a la regulación de la *Comisión Informática de la Salud Pública* coincide con el de la aparición del precepto legal de realización del *Análisis de Riesgos* (RD 263/1996, por el que se regula la utilización de técnicas electrónicas informáticas y telemáticas por la Administración General del Estado).

La aparición de los *Requisitos de Seguridad* nos determina a hablar de las *Auditorías* sobre los

activos del Sistema.

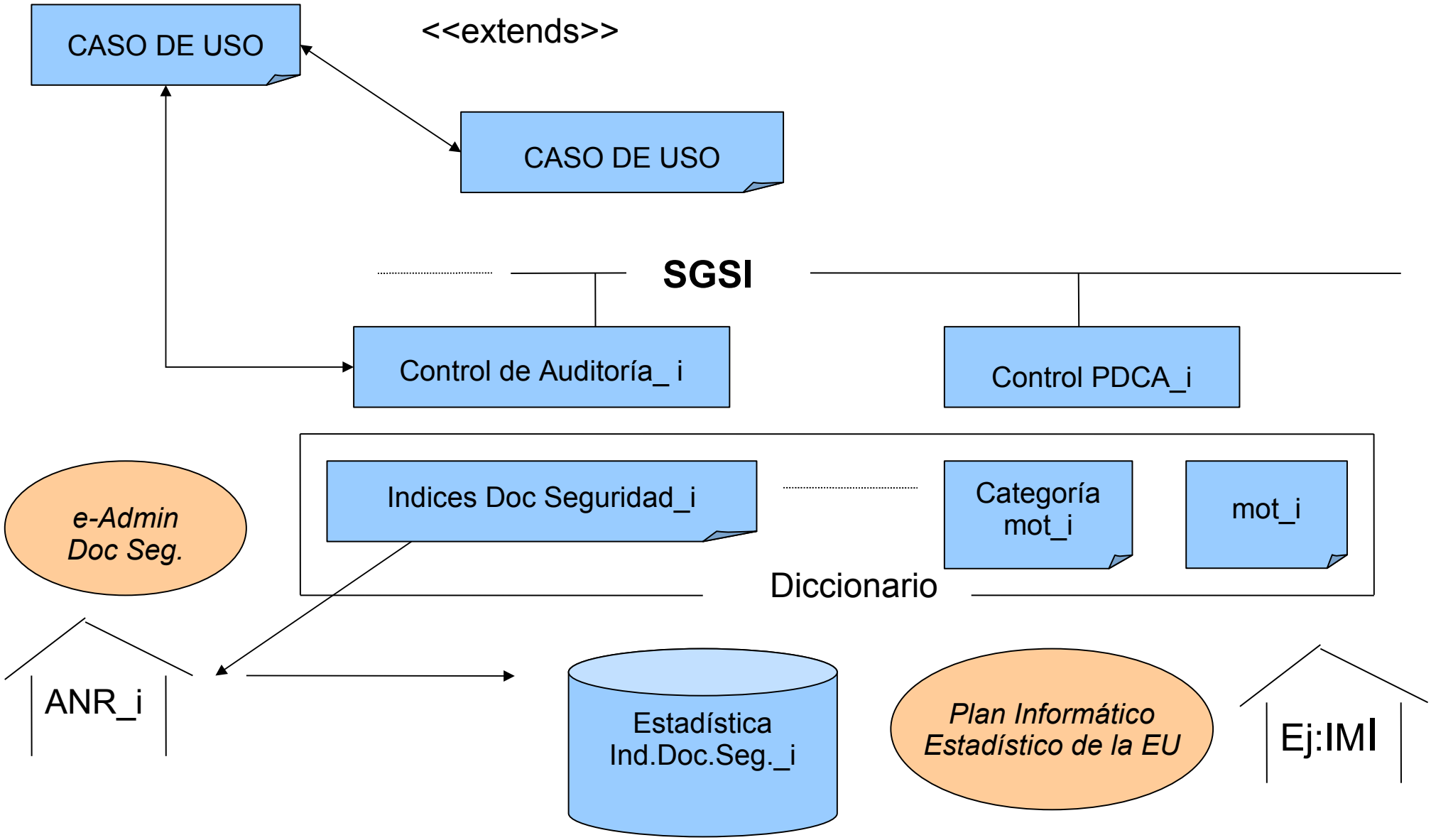
En este caso, se produce la diferenciación entre el responsable de datos, el del sistema de información, y los responsables de operación. Y la aparición de los dos organismos reguladores en el tratamiento de datos, como son: la Agencia de Protección de Datos y el Centro Criptológico Nacional.

En el capítulo II la incorporación de *Actores* encuentra diversidad de orígenes, como vimos, mientras que las funcionalidades se extraen de un r*equerimiento informado legal*. Así, el responsable de seguridad deberá presentar en su *Informe Periódico de Seguridad*, los incidentes más relevantes del problema descrito. A la hora de incorporar requisitos legales a nuestro Sistema de Seguridad contamos con una *Herramienta CASE* denominada *Diccionario*, y desde el lado de la Metodología de *Gestión de Riesgos,* conocida como *Métrica*, con el documento registrable en el *Sistema de Configuración del Sistema de Información,* y denominado *Estudio de Viabilidad del Sistema o EVS*.

Puesto que los nuevos elementos que van a aparecer son básicamente documentos de texto y estamos hablando de *Motivadores* y *Categorías* de la *Gestión del Cambio* en un *EVS*, o bien de Indices de la expresión de un *Documento de Seguridad*, hablaremos tambien de un *Control de Registros* , *clausula 4.3.3* de la *ISO 27 001* y de la *clausula 4.3.2 .i* relativa al *Control de Documentos*.

Indice: Cap. IV,

Modelo optimo de Auditoría (Usuario), Resolución de Madrid



LAMINA 13

La práctica sucesiva de auditorías sobre determinadas secciones de la *e-Administracción* puede, a lo largo del tiempo, dar lugar a la implementación de nuevos controles específicos que ayudarán a la auditoría. Estos controles, en principio, se diferenciarán de la colección de los ya existentes, contándose desde los más simples a la sucesión de encadenados.

Precisamente estos nuevos controles de auditoría podrían responder a patrones de 'Casos de Uso' , que, ampliados o no, proporcionarán una explicación, por ejemplo, en el ejercicio de una *Impugnación de Valoraciones*.

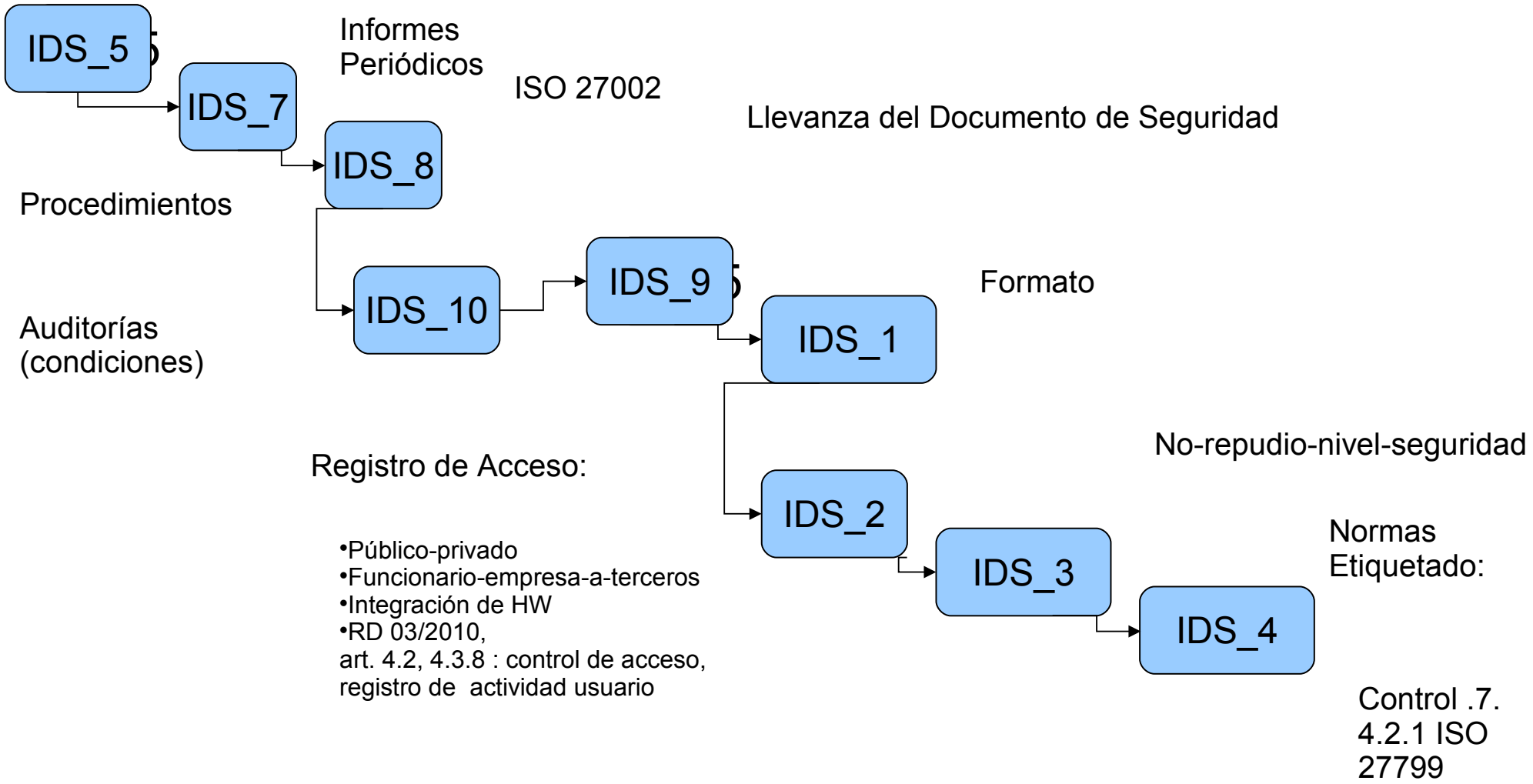
En consecuencia, podemos decir, que estamos hablando de una automatización de un Modelo Optimo de Auditoría y el Usuario-Paciente ha encontrado desarrollada su Seguridad.

Por su parte, la autoridad reguladora responsable de la definición de dichos nuevos controles, puede haber utilizado en la exposición de *Requisitos Informados* , (y recordemos que nos encontramos en una plataforma de Telecomunicaciones) los *Indices* del *Documento de Seguridad* que proponemos aplicar. Resultará una exposición que puede ser archivada , dígase <<registrada>> y empleada conjuntamente con otras en el *Plan Informático Estadístico de la EU*, y a propuesta de algún Organismo como el *IMI*, que, quizá presenta una regulación más clara e integradora, incluyendo su consideración hacia la Telemedicina.

Así, Métricas Nacionales, Estándares Internacionales, Documentos de las Agencias Reguladoras y Estadísticas Europeas, se integran en un Marco de Privacidad que puede dar respuesta a la *Resolución de Madrid*, fruto de la *31º Conferencia de Privacidad*.

Indice: Cap. IV, e-Sanidad Mundial

Función f(IDS_5[IDS_6]):



LAMINA 14

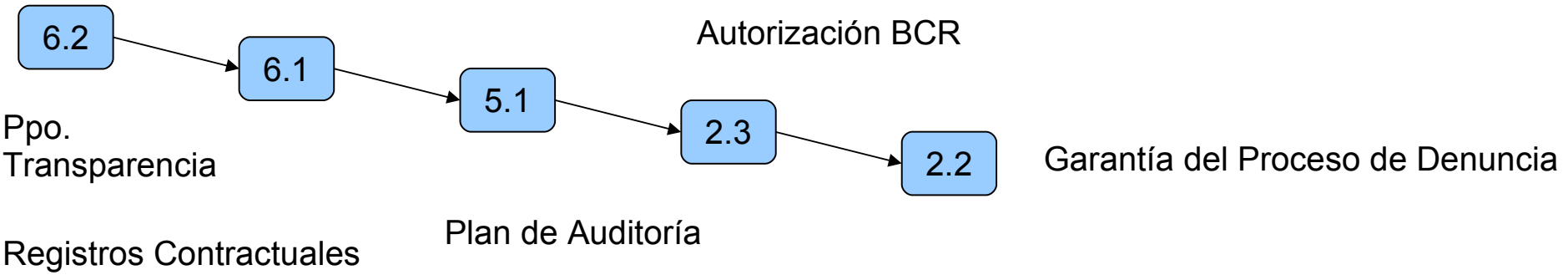
Un ejemplo de la exposición de alguno de los Documentos de Trabajo de la Autoridad Reguladora, la esbozamos en la diapositiva en función de los *Indices*:

<<Se pretende realizar una valoración de la repercusión que puede tener sobre el *Sistema Informático, SI*, en diferentes países, que no tienen por qué pertenecer al mismo ámbito de mercado (puerto seguro, ..) en relación a unos determinados Procedimientos y Ficheros Lógicos. Se esperarán como HITOS del proyecto internacional y en respuesta del trabajo, unos *Informes Periódicos*, que limitándonos al ámbito de un estandar internacional comunmente aceptado, como es el actual caso del *ISO 27 002*, facilitarán unas determinadas condiciones de las auditorías y donde quedará perfectamente delimitado la 'llevanza del Documento de Seguridad′. En este punto, ya no se encontrará discusión en torno al Formato del *Documento de Seguridad* y los registros de acceso. Con lo que los propios NO-REPUDIOS-de-los-NIVELES-DE-SEGURIDAD apuntarán a mejores y adecuadas *Normas de Etiquetado*, como conclusión>>

Método:

Modelado PDCA Control ISO 27002

Documento de Trabajo WP 195 Gt29 D 95/46/CE



Clausula Resumen: 13.2.3 de recopilación de evidencias

Clausula Equilibrio: 15.1.4 legislaciones, Marco-privacidad, Actores

LAMINA 15

El primer grafo expone que, persiguiendo todas las garantías del proceso iniciado en la lámina anterior y en colaboración con las Fuerzas de Seguridad del Estado, se comunicarán nuevos requerimientos, primero, a la autoridad competente en materia de protección de datos, y éste a su vez, a la estructura del *BCR* {6.2[1]}, delimitándose, en consecuencia, más nítidamente el término contractual entre *Procesador* y *Controlador*, y se reforzarán las condiciones de verificación de algunos de los tipos de proceso relacionados con el ejercicio de los *Derechos ARCO* {6.1}, produciéndose una sucesiva verificación de las premisas en toda la extensión del *BCR* {5.1}, y quedando la '*Privacy Function*' más claramente orientada {2.3}, garantizando, de cualquier modo, el proceso de denuncia {2.2} que persigue el documento de trabajo WP nº 195 en todo momento.

La expresión que hemos adoptado mediante estas dos últimas diapositivas consigue la obtención de una *prueba judicial* inicializando, ya un equilibrrio, con la propuesta de solución de *control P.D.C.A* implementada mediante controles *ISO 27 002* , resumida , a su vez, en una clausula o c*ontrol nº 13.2.3* de <<recopilación de evidencias>> y correspondiente a un 'Perfil de Protección' (*Common Criteria*, *CC*) como *Soporte* y que nos recomienda que, cuando una acción legal de seguimiento involucra a la consideración de las reglas de evidencia (admisibilidad, peso), y dando respuesta, en cualquier caso, a la *clausula nº 15.1.4 de la ISO 27 001*, se nos determina a obtener un equilibirio entre las legislaciones estatales, el Marco de Privacidad y la identificación de Actores.

Además, continuando con la consideración de los *Niveles de Seguridad*, habremos de observar en su aplicabilidad la *Certificación de Productos* , que indica el *Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información*, constituido al amparo de lo dispuesto en el *art. 2.2.c) del Real Decreto 421/2004.*

---

[1] *Principio de Transparencia*. Alusión en relación al Documento *CAF 2013*, que de los 'resultados' que una organización necesita realizar, en concreto el *subcriterio 6.2 del Modelo de la Excelencia*, coincide en valorar positivamente que se realizará la valoración de este resultado hacia la protección de los servicios y productos conforme a: - nº canales de información – disponibilidad y predicción de la información – disponibilidad de los objetivos de rendimiento – nº de actuaciones del Defensor del Pueblo – alcance de los esfuerzos - indicadores calidad-producto – nº y tiempo procesamiento de quejas – repeticiones de proceso

Cap. IV:

Ciclo P.D.C.A.

1.-Fase C(Revisión): Testeo, Auditoría

2.-Fase A(Actuación): Mejoras detectadas sobre el SGSI identificadas, documentadas y ejecutadas

Ejemplo:

<<claridad>> en fases PDCA

Solución practicada: recovery control (IEEE) con requerimientos informados

(Expresión de Indices del Documento de Seguridad, WP nº 195 Gt29, D95/46/CE)

Logros en Gestión de Proyectos (reducción del Impacto en RRHH: Marco de la Excelencia, Generación de Plantilla Proyecto SGSI)

LAMINA 16

Es un capítulo donde con mayor claridad se exponen las fases del *Ciclo P.D.C.A* que participan, pero, evidentemente, esto es así, puesto que estamos aplicando una solución y su integración.

El control que se propone, en términos del *Institute of Electrical, Electronical Engineer, IEEE*, es un control de recuperación o 'recovery control', cuya especificación de requisitos, por movernos ya más introducidos en la esfera de la *Ingeniería del Software* y puesto que tratamos de resolver una serie de tecnologías informáticas para alcanzar nuestro Producto viene apoyada por la aplicación de los Indices del *Documento de Seguridad* del capítulo precedente, y el análisis en el ámbito de las Transferencias Internacionales por el Documento de Trabajo correspondiente al *Grupo de Trabajo Gt29 de la Directiva D 95/46/CE, WP nº 195*, donde se desbrozan las competencias de un *Controlador* y un hipotético *Procesador*.

La *Función de Seguridad* o *Perfil de Protección* como se denominan desde los *Common Criteria*, *CC,* se corresponde con el 'Perfil nº 1' de nuestra Tesis, supuesto el caso de una pausible certificación del producto; correspondiéndose al 'Perfil nº 0', a la aplicación de una e-administración de la aplicación de Indices, cuando se hubieran obtenido suficientes extracciones estadísticas en un marco más amplio; y , finalmente, el 'Perfil nº 2' en el caso de encapsular el producto sobre soporte físico, en este caso, una tarjeta.

Apuntar, que el *control P.D.C.A* implementado está dando solución desde la *Dimensión de Seguridad* conocidad como *Confidencialidad* a otra llamada *Integridad* , desde la perspectiva de la disparidad de legislación en tema de *Derechos ARCO* , desde el lado de la *Taxonomía* del e-Técnico.

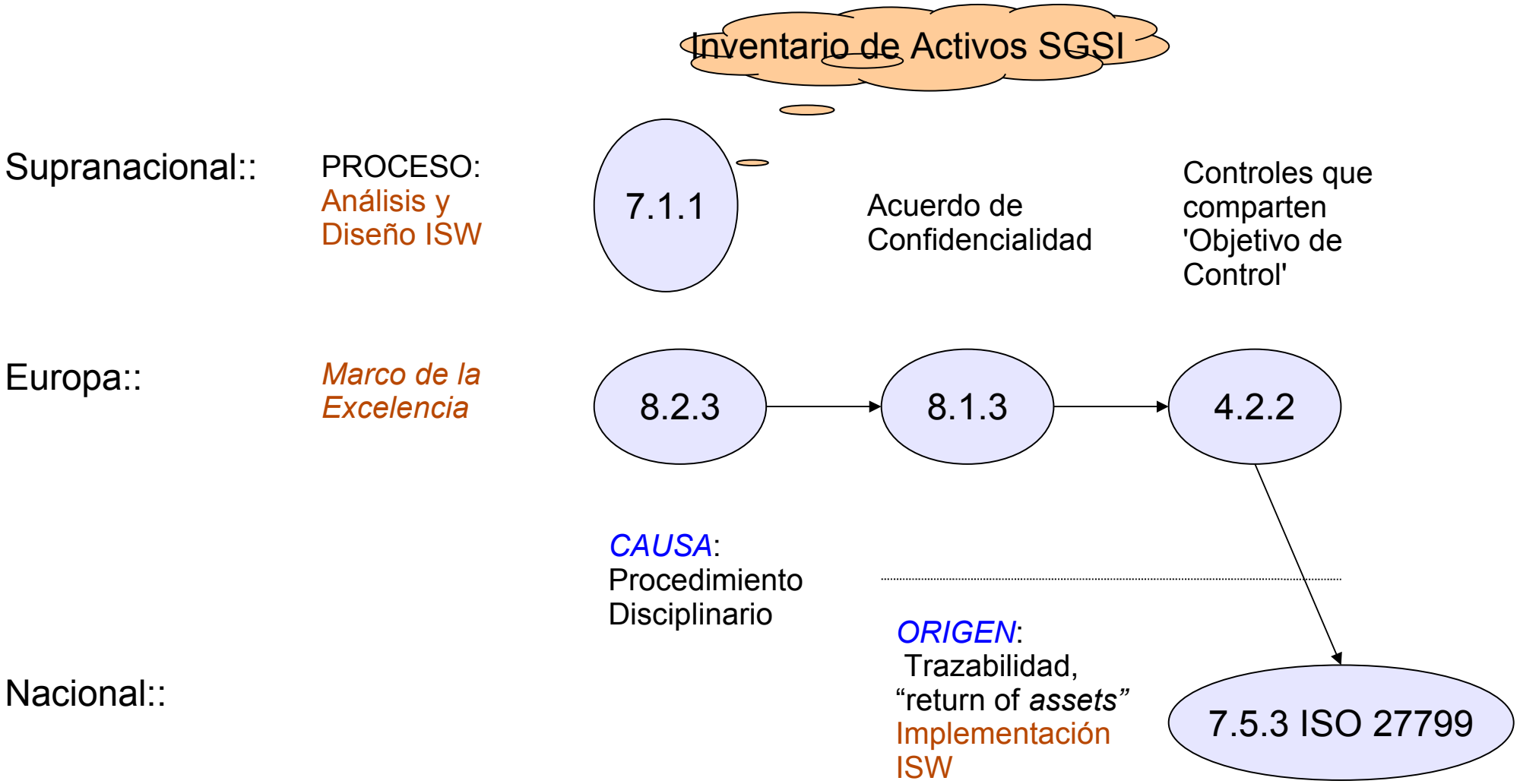
Existen dos conclusiones importantes al respecto de la Tesis en el área de la *Gestión de Proyectos*:

1.- la reducción del impacto sobre los recursos humanos existentes al introducir controles de seguridad cuando aplicamos el *Marco de la Excelencia*

2.- la incorporación de los *Productos* propios de la Tesis (Motivadores, Categorías, el control PDCA) como *Tareas* de unos *Paquetes de Trabajo* (PMBok) concretos que pueden ser utilizados en una *Plantilla* en la *Gestión de Proyectos*

Cap. IV:

Auditoría del SGSI, ISO 27001



LAMINA 17

Esta lámina resume lo que puede ser la auditoría del propio *SGSI*. El proceso completo parte de la realización de un *Inventariado* de todos los *Activos* que hemos generado como propios en la Tesis. Involucra, concretamente, a las Fases de Diseño y Análisis de la Ingeniería del Software (*ctrl. nº 7.1.1 ISO 27 001*), puesto que deberemos modelar:

- las Bases de Datos con la especificación de Actores
- Perfiles de Seguridad, por niveles de seguridad aplicados a las entidades-clases de la base de datos
- el Diccionario de Datos, extrayendo motivadores y sus categorías en un análisis funcional de *Ingeniería del Software*

Esto resulta válido en un consenso internacional.

En el ámbito europeo podemos, una vez analizados los criterios y subcriterios del *Marco de la Excelencia*, partir de la causa motivadora de una posible Defensa de la *Seguridad del Trabajador*, esto es, el Procedimiento disciplinario en una *Política de Seguridad* (*ctrl. nº* 8.2.3), continuando con un acuerdo de compromiso y confidencialidad del Trabajador de la *e-Sanidad* (*ctrl. nº* 8.1.3), y la consiguiente identificación de aquellos controles que comparten un mismo 'objetivo de control' para satisfacer tal fin (*ctrl. nº* 4.2.2).

Observar, que una vez aceptada la Tesis, y practicando un Proyecto de Investigación sobre ella en el *Marco de la Excelencia*, tan sólo nos queda dedicarle tiempo al seguimiento de la implementación, que, en realidad, es el origen del que se parte en esta Tesis como experiencia, aunque en otra Sección de la *e-Administración* , y en el campo más concreto de la *Transparencia*. Focalizando nuestras intenciones en el campo de la *e-Sanidad*, detectamos a nivel de *Auditoría* un control *ISO 27 002*, que se corresponde con el *control 7.5.3 de la ISO 27 799*, y que va encontrando sus divergencias por países, pero que podríamos resolverlo de la siguiente forma:

Si quisiéramos potenciar el factor estadístico dentro del *Plan Informático Estadístico de la EU* por pretender uniformidad en la práctica de *Derechos ARCO*, se deberán presentar resultados en torno a

Métricas, pudiendo, retomar la lámina de rótulo Cap. I, *Ciclo PDCA* completando los procedimientos con las conclusiones que se extraigan en consenso por o sin excepción.

Aportaciones

- Transversalidad
- Resolución de Madrid
- Campo de la Semántica
- Compromiso con el estándar

Conclusiones

1.- Elevación Semántica: refuerzo desde el Esquema Tecnológico

2.- Funcionalidades de Seguridad en RRHH

3.- e-Administración correctiva: Métricas

4.- Manejo extensivo de Indices en e-Sanidad

5.- Clausula 4 de la ISO 27001:

- ISW + Dcho. Informático
- Marco de Privacidad(propuesta de Resolución de Madrid)
  - Doc. WP 195 Gt29 D 95/46/CE,
  - Indices Doc.Seg.
  - Categorías (+) Motivadores de la Gestión del Cambio de un EVS
- Marco de la Excelencia, CAF 2013: !! (impacto) incorporación SGSI sobre RRHH
- Ejemplo de implementación Control PDCA ISO 27002
- Resultados Nominales Tesis se constituyen en
  - Especificaciones de Paquetes de Trabajo del EDT de un Proyecto SGSI

Anexos. Anexo I:

Responsabilidad Taxonómica en la HC. RDUNED. Nº 11

- Línea del Tiempo:

publicaciones en torno a la Privacidad

- Publicación de Taxonomías:

consentimiento informado

Anexos. Anexo II:

La Semántica en el Derecho Informática de la HC. DIARIO LA LEY.nº 8011

- Seguimiento histórico de publicaciones de regulaciones en torno a la libertad informática del 'habeas data'

- Impulso de Motivaciones Tecnológicas en el Derecho Informático