

## 12.09 Introducción a la ciberseguridad



La Ciberseguridad es la seguridad de la información aplicada a los riesgos derivados del uso de Internet y las nuevas tecnologías, referidos a los ejes de la protección de la confidencialidad, integridad y la disponibilidad de la información

**Autores: Raúl Lopez Martinez.**

*Jefe de Servicio de Proyectos y Servicios. Hospital Gregorio Marañón.*

**Marina Medela Fernández**

*Abogada especializada en TIC*

**Manuel Pérez Vallina.**

*Subdirector de Sistemas de Información. Hospital Gregorio Marañón.*

Se recomienda imprimir 2 páginas por hoja

### **Citación recomendada:**

Lopez Martinez R., Medela Fernández M., Perez Vallina M. Introducción a la ciberseguridad [Internet]. Madrid: Escuela Nacional de Sanidad; 2023 [consultado día mes año]. Tema 12.09. Disponible en: [direccion url del pdf.](#)



TEXTOS DE ADMINISTRACION SANITARIA Y GESTIÓN CLINICA  
by UNED Y ESCUELA NACIONAL DE SANIDAD  
is licensed under a Creative Commons  
Reconocimiento- No comercial-Sin obra Derivada  
3.0 Unported License.



### 1.- Introducción

#### **¿A qué nos enfrentamos?**

Actualmente convivimos con multitud de indeseables y peligrosas amenazas informáticas que pueden afectar muy negativamente a los sistemas informáticos de una compañía, pero también a los dispositivos que utilizamos en nuestra vida privada para realizar tareas cotidianas (como, *por ejemplo, realizar una transferencia o una compra "on line"*).

La Ciberseguridad es la seguridad de la información aplicada a los

riesgos derivados del uso de Internet y las nuevas tecnologías.

## Índice

- 1 INTRODUCCIÓN
- 2 DESARROLLO
  - 2.1 Los pilares de la seguridad
  - 2.2 Principales riesgos y amenazas
    - 2.2.1 Conceptos básicos
    - 2.2.2 Vulnerabilidad
    - 2.2.3 Amenaza
  - 2.3 Legislación
    - 2.3.1 Protección de Datos
    - 2.3.2 Esquema Nacional de Seguridad
    - 2.3.3 Otras normas relevantes:
  - 2.4 Buenas prácticas
    - 2.4.1 Caso práctico
    - 2.4.2 Errores comunes
    - 2.4.3 Recomendaciones
  - 2.5 Retos
    - 2.5.1 Incremento del riesgo por una mayor y necesaria exposición empresarial y de los ciudadanos
    - 2.5.2 Desarrollo del 5G
    - 2.5.3 Teletrabajo
    - 2.5.4 Uso de Inteligencia Artificial (IA) para atacar y defender infracciones
    - 2.5.5 Computación cuántica
  - 2.6 Propuestas
    - 2.6.1 Concienciación
    - 2.6.2 Gestión del riesgo desde un inicio
    - 2.6.3 Promover el desarrollo de modelos de gobernanza de la ciberseguridad
    - 2.6.4 Regulación

## Aspectos básicos a tener en cuenta:

- ✓ La seguridad de la información se basa en 3 dimensiones (principales): **C o n f i d e n c i a l i d a d**, Integridad y Disponibilidad.
- ✓ Las medidas de seguridad reducen el riesgo de que la información se vea afectada en alguna de esas dimensiones.
- ✓ No es posible lograr un riesgo 0, pero si minimizarlo mediante esas medidas.
- ✓ El uso de redes incrementa el riesgo de sufrir un ataque, este crece si la red es Internet.
- ✓ Las políticas de seguridad establecen las directrices globales, son de obligado cumplimiento y todas las medidas de seguridad deben ir alineadas con estas.
- ✓ La concienciación de las personas usuarias es esencial para minimizar los riesgos.

## 2.- Desarrollo

### 2.1 Los pilares de la seguridad



La Ciberseguridad es la seguridad de la información aplicada a los riesgos derivados del uso de Internet y las nuevas tecnologías, referidos a los ejes de la protección de la confidencialidad, integridad y la disponibilidad de la información:

- ✓ **CONFIDENCIALIDAD:** propiedad que dispone que la información no se encuentre a disposición de cualquier persona o que pueda ser divulgada.
  - ✓ Por ejemplo, la [filtración de los datos de la víctima de "La Manada"](#).
  - ✓ Otro ejemplo fue el [error de seguridad en la web de vacunación COVID](#) de Cataluña ha expuesto datos personales de la ciudadanía.
- ✓ **INTEGRIDAD:** propiedad de conservar la exactitud de los activos de información.
  - ✓ Por ejemplo, [el SEPE sufre un ataque de ransomware](#) que cifra todos sus datos con lo que no pueden prestar servicio.
- ✓ **DISPONIBILIDAD:** propiedad de ser accesibles y utilizables ante cualquier persona que los solicite.
  - ✓ [Wannacry](#): "La amenaza de ciberataque causa el "caos" en juzgados de Castellón".

### 2.2.- Principales riesgos y amenazas

#### 2.2.1.- Conceptos básicos

La información de nuestra organización es el activo más importante a proteger debido a que un incidente, como fugas de información o revelación de datos confidenciales, podría producir

grandes pérdidas (económicas, reputacionales, etc..).

Un riesgo es el potencial de que una amenaza, explote las vulnerabilidades de un activo o grupo de activos, causando daño o pérdida.

El riesgo está asociado con dos conceptos clave: vulnerabilidades y amenazas.

---

### 2.2.2. Vulnerabilidad

---

La vulnerabilidad la entendemos como una debilidad que puede ser aprovechada, y que por sí misma no produce daños.

*Por ejemplo, si no tenemos copias de seguridad nos arriesgamos a que cuando falle un disco perdamos información.*

Las vulnerabilidades pueden ser muy diversas, *por ejemplo, si dejamos la puerta de oficina abierta por la noche tenemos una vulnerabilidad que posibilita que se materialice una amenaza, en este caso que alguien entre a robar.*

En este sentido la formación y la concienciación del personal juegan un papel fundamental para prevenir las amenazas intencionadas

#### **Algunos ejemplos de vulnerabilidades:**

- ✓ No formar ni concienciar periódicamente al personal.
- ✓ No realizar copias de seguridad corporativas, o con la suficiente frecuencia.
- ✓ Política de contraseñas muy laxa.
- ✓ Que no haya control de acceso a los sistemas de información.
- ✓ Tener aplicaciones obsoletas y desactualizadas.

### 2.2.3.- Amenaza

Una amenaza es un evento que puede causar daños a los sistemas de información.

Por ejemplo, una [inundación en el Centro de Proceso de Datos \(CPD\)](#) es una amenaza dado que puede inutilizar los servidores e interrumpir el servicio.

No necesitamos ser expertos en seguridad, pero sí ser conscientes de las amenazas a las cuales estamos expuestos y evitar caer en los engaños de los ciberdelincuentes aprendiendo unos pocos hábitos seguros.

Hay 4 tipos de amenazas, los tres primeros no son intencionadas pero el ultimo tipo sí.

- ✓ **DESASTRES:** Accidente natural, terrorismo, fuego...
- ✓ **ERRORES:** Error humano, error en la configuración, etc.
- ✓ **FALLOS:** Corte de energía, fallo en la climatización, etc.
- ✓ **AMENAZAS INTENCIONADAS:** Software malicioso, intrusión, *phishing*, robo de información...



#### Virus

Programa diseñado que se adhiere a apps existentes en el sistema y, cuando se ejecuta, se propaga a otros archivos



#### Troyano

Software que se caracteriza por no dar muestras de mal funcionamiento del sistema infectado. Abre canales de comunicación hacia otros equipos.



#### Gusano

Aprovecha vulnerabilidades del sistema o de aplicaciones conocidas para replicarse de manera exponencial, sin necesidad de interacción humana, puede llegar a colapsar las redes



#### Spyware

Recopila información del sistema de forma automatizada, para posteriormente enviar un reporte de la misma a un atacante sin el consentimiento ni conocimiento del usuario



#### Ransomware

Cifra los archivos de un ordenador, pidiendo un rescate económico a modo de extorsión, a cambio de liberar la información que tiene en su poder.

---

## 2.3.- Legislación

---

---

### 2.3.1.- Protección de Datos

---

La Protección de datos personales es un derecho fundamental consagrado en el artículo 18 de nuestra Constitución. Además, su regulación está basada principalmente en dos normas:

El *Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD)*, cuyos objetivos principales son:

1. Establecer un marco normativo para regular los datos de las personas y su libre circulación.
2. Regular los tratamientos de datos personales de interesados que se encuentren en la UE.
3. La circulación de los datos no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas, en lo que respecta a los tratamientos de datos personales.

El RGPD permite armonizar y nivelar las distintas legislaciones de los países miembros con el establecimiento de un marco común.

La *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)*, cuyos objetivos son:

1. Adaptar el RGPD a la legislación nacional.
2. Regular aquellos aspectos que el RGPD deja abiertos para que los EE.MM legislen (Ej. La edad para consentir el tratamiento de datos personales)
3. Regula las obligaciones de los intervinientes en todo proceso de transferencia de datos personales.
4. Garantizar los derechos digitales.

---

### 2.3.3.- Esquema Nacional de Seguridad

---

Los objetivos del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad*, y que resulta aplicable principalmente a las Administraciones Públicas y aquellos que presten servicios para las mismas, son:

- ✓ Establecer los principios que regulan y aseguran el acceso, integridad, disponibilidad y veracidad de la información
- ✓ Crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- ✓ Promover la gestión continuada de la seguridad.
- ✓ Promover la prevención, detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques.
- ✓ Promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades.
- ✓ Servir de modelo de buenas prácticas

---

### 2.3.3.- Otras normas relevantes:

---

- *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas* à establecer las estrategias adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la pre-

vención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas.

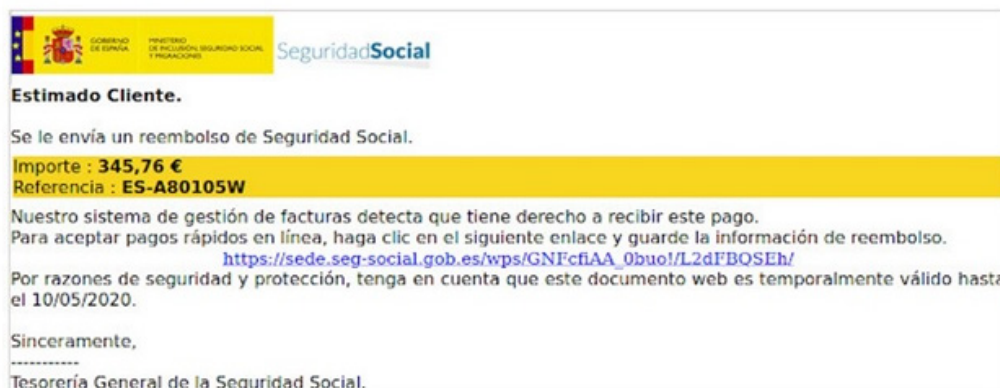
- *Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.* Supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.
- *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.* Establece obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

## 1.1 Buenas prácticas

### 2.4.1.- Caso práctico

## Análisis de Phishing suplantando a la SS.SS

De: Seguridad Social  
Enviado: miércoles, 29 de abril de 2020 3:54  
Para: [Redacted]  
Asunto: Se le envía un reembolso de Seguridad Social.



The screenshot shows a phishing email from 'Seguridad Social' (Social Security). The header includes the logo of the Spanish Government and the Ministry of Inclusion, Social Security, and Equal Opportunities. The body of the email addresses the recipient as 'Estimado Cliente' and states that they are sending a refund. The amount is listed as 'Importe : 345,76 €' and the reference is 'Referencia : ES-A80105W'. The email includes a link to a website for accepting payments and a warning that the document is only valid until 10/05/2020. The email is signed 'Sinceramente, Tesorería General de la Seguridad Social.'



- ✓ Intenta explotar los siguientes sentimientos:
  - Urgencia: hay una fecha límite relativamente cercana a la fecha de recepción del mensaje.
  - Miedo: la posibilidad de no cobrar una cantidad a la que supuestamente tenemos derecho.
  - Curiosidad: es una cantidad relativamente grande como para no hacerle caso.
- ✓ La Seguridad Social nunca se va a dirigir a nosotros mediante un correo electrónico y menos, si no hemos dado nuestro consentimiento para ello.
- ✓ Nunca se va a dirigir a nosotros con la fórmula "Estimado Cliente".
- ✓ Tampoco hay nada en el mensaje que lo personalice hacia nosotros. Ni nombre ni DNI.
- ✓ Nosotros, como personas físicas, no emitimos facturas (únicamente autónomos y empresas).

### **¿En qué debemos fijarnos entonces?**

*¿Quién nos lo manda? ¿Somos clientes?*

*¿Ese correo tiene un contenido inesperado, aporta algo?*

*¿Su lectura nos despierta curiosidad, morbo, una urgencia inesperada ...?*

*¿Está personalizado, o es un correo que podría recibir cualquier persona sin ser modificado?*

*¿Tiene faltas de ortografía o errores de sintaxis?*

*¿Existe esa organización y son correctos las direcciones de contacto?*

---

### **2.4.2.- Errores comunes**

---

- ✓ Abrir emails procedentes de fuentes desconocidas, infectando los terminales (PCs, Móviles, Tablet, etc.) que

pueden contener software malicioso o virus.

Por ejemplo, el [fraude del Ceo](#) en el que ciberdelincuentes simulan ser el CEO de la empresa para engañar a los empleados.

- ✓ Visitar webs no confiables y/o redireccionamiento a las mismas por enlaces sospechosos.

Por ejemplo, páginas ilegales de descarga de software o contenidos (Torrents, eMule...)

- ✓ No actualizar los equipos lo que concierne a sistema operativo, antivirus y aplicaciones.

Por ejemplo, los [papeles de Panamá](#) se obtuvieron debido a que el atacante se aprovechó de que el servidor de correo de la empresa que lo gestionaba llevaba años sin actualizarse y tenía una vulnerabilidad crítica para la que sí existía un parche que no se había instalado.

- ✓ La pérdida de discos USB no cifrados puede suponer que terceros accedan a información sensible.
- ✓ No apagar o reiniciar equipos, lo que conlleva a tener desactualizados algunos sistemas.
- ✓ Instalar aplicaciones no seguras y no autorizadas por el organismo, tanto en ordenadores como en dispositivos móviles corporativos.
- ✓ Uso de contraseñas evidentes y no variación de las mismas ([Top contraseñas usadas 2022](#)).
- ✓ Compartir las contraseñas con otras personas.
- ✓ Almacenamiento de información "en nube no corporativa" (Dropbox, Google Drive, etc.), exponiendo información sensible fuera de los mecanismos de protección del organismo.
- ✓ Dejar equipos desatendidos sin bloquear la sesión, permitiendo a cualquiera acceder a nuestras cuentas, servicios y documentos.

- ✓ Utilizar redes públicas para acceder a información sensible.
- ✓ Utilizar mensajería online para hablar o enviar información sensible (WhatsApp, Telegram, etc).
- ✓ Dejar información sensible expuestas a la vista (post-it con nombres de cuentas y contraseñas, informes confidenciales, etc...).
- ✓ Conectar discos USB o móviles no autorizados en nuestros equipos puede suponer que se instale malware.

---

### **2.4.3.- Recomendaciones**

---

---

#### **2.4.3.1.- Uso de contraseñas**

---

Las contraseñas son el principal mecanismo de autenticación en los sistemas de información por lo que deben ser complejas, cambiadas periódicamente y mantenerlas protegidas.

- ✓ Las personas usuarias son responsables de proteger las contraseñas, manteniendo su confidencialidad.
- ✓ Guardarlas en lugar seguro, evitando soportes legibles.
- ✓ Modificarla siempre que sospechemos que se haya visto comprometida.

---

#### **2.4.3.3.- Correo electrónico**

---

El correo electrónico es la principal vía de entrada de ataques de tipo de phishing, por ello es necesario prestar especial atención a los correos sospechosos.

- ✓ Ante la duda, no abrir links o ficheros adjuntos y avisar al responsable de seguridad.
- ✓ No debe emplearse el correo electrónico para el almacenamiento de ficheros.
- ✓ Cuando sea posible, evitar enviar archivos adjuntos, sustituyéndose por enlaces a los ficheros en el

almacenamiento corporativo.

---

#### **2.4.3.3.- Puesto de trabajo**

---

- ✓ La pantalla del ordenador debe estar orientada de modo que el contenido no pueda verse desde una zona de paso pública.
- ✓ Si se imprime documentos con información sensible, acudir a la impresora sin esperar a que se termine de imprimir para recogerlos.
- ✓ Para destruir documentos impresos sensibles, se utilizarán destructoras de papel u otro método que impida su recuperación.
- ✓ Se debe bloquear el ordenador cuando se ausente del puesto de trabajo.
- ✓ En caso de encontrar información en papel o material informático sin custodiar, se ha de avisar al superior inmediato.
- ✓ No deshabilitar los mecanismos de seguridad instalados en los ordenadores.
- ✓ Evitar conectar dispositivos no autorizados.

---

#### **2.4.3.4.- Proveedores**

---

- ✓ Uno de los principales riesgos que se identifica en cuanto a la seguridad de la información y, sobre lo cual, es preciso aplicar medidas correctoras o mitigadoras es el acceso por parte de personas no autorizadas a la información.
- ✓ Se debe asegurar de que todos aquellos proveedores que trabajen con la organización deben firmar los preceptivos acuerdos de confidencialidad y compromisos de adoptar las medidas de seguridad necesarias.

---

### 2.4.3.5.- Documentación sensible

---

- ✓ Es común que en ciertas situaciones algunos empleados hagan uso de **información sensible**, *por ejemplo, datos de facturación, nóminas o ideas de nuevos productos o servicios.*
- ✓ Si se encuentra en formato físico, **debe quedar guardada en un lugar seguro** al finalizar la jornada laboral.
- ✓ **Únicamente** debe estar **accesible para el personal autorizado**, bien sea por medio de permisos de usuario o por cualquier otro método que evite miradas indiscretas.
- ✓ La **destrucción** de la información al terminar su ciclo de vida también **es un proceso crítico**, que si no se realiza correctamente **puede derivar en una fuga de información.**
- ✓ Cuando se destruye información que contiene datos sensibles o confidenciales, debe hacerse de forma segura utilizando **destructoras de papel o por medio de empresas especializadas que ofrezcan garantías.**

---

## 2.5.- Retos

---

---

### 2.5.1.- Incremento del riesgo por una mayor y necesaria exposición empresarial y de los ciudadanos

---

Aquellos puntos de una **organización** que pueden ser utilizados como puerta de entrada para un ataque cibernético u obtener acceso no autorizado a datos confidenciales (vulnerabilidades en las personas, entornos físicos, de red o de software, incluidos sistemas operativos, aplicaciones web, IoT y dispositivos móviles, etc.).

La digitalización de los procesos de una compañía hace que la exposición sea mayor que hace años, y es necesaria para que la organización pueda seguir desarrollando sus actividades.

Hace 25 años las empresas tenían sus redes internas completamente separadas del mundo exterior, los firewalls hacían de muralla a la red y no era necesario la exposición que existe actualmente, Además, la atención personalizada en un horario acotado era lo más común.

Ahora, los clientes exigen una atención online en tiempo real y de calidad. Esto provoca que los sistemas de BackOffice, los más críticos que tienen los datos de los clientes (sistemas que deben estar menos expuestos) estén a dos pasos de Internet. La interfaz entre el cliente y la empresa que antes hacía un operador, ahora también se puede efectuar a través de una web u otro sistema automático: bots, apps, whastapp, correo electrónico, SMS, etc.

Todo ello, hace necesario tener implementadas estrategias y medidas que minimicen la existencia de agujeros de seguridad, especialmente en las etapas de diseño, pruebas y puesta en producción.

Las vulnerabilidades de Software deben estar perfectamente controladas y los sistemas parcheados a la última versión, implementando mecanismos de auditoría y control para la identificación de las vulnerabilidades, que permitan agilizar el proceso de mitigación y tratamiento de las mismas.

El **ciudadano** también está más expuesto a nivel tecnológico, ya que siempre lleva un dispositivo móvil en el bolsillo, que no deja de ser un ordenador que contiene, procesadores muy potentes, GPS capaz de saber conocer la ubicación exacta y almacenar el trayecto completo, sensores de huella, de reconocimiento facial, cámara de video, acelerómetro, barómetro, brújula, etc.

Cuando los móviles se utilizan, la exposición es mayor, ya que se interactúa con webs que pueden fraudulentas o que recopilen información sin consentimiento. Así, toda la información

proporcionada a terceros puede ser utilizada de buena fe o por mafias organizadas que la analizan y utilizan contra los ciudadanos con el fin de realizar ataques dirigidos o ataques generalizados de los que obtienen suculentos beneficios.

**Al contrario de lo que ocurre con los minerales y piedras preciosas, los datos son más valiosos cuanto más cantidad y variedad se dispone de ellos.**

---

### 2.5.2.- Desarrollo del 5G

---

La implantación de esta tecnología supondrá un incremento notable en la velocidad de navegación (entre 10 y 20 veces más rápido), en el número de dispositivos conectados por km<sup>2</sup> donde la red será capaz de soportar (hasta 1 millón de dispositivos, frente a los 1000 del 4G) ([Comisión Europea: 5G Global Developments Accompanying the document "Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions 5g for europe: an action plan"](#)). Todo ello hará que se incremente la capacidad de los ataques, *por ejemplo, multiplicando por 10 o 20 el número de correos maliciosos que se pueden enviar por segundo, aumentando el número de dispositivos que pueden ejecutar un ataque de denegación de servicio.*

A favor del desarrollo de las Redes 5G es que actualmente estamos mucho más concienciados que cuando se construyeron e implementaron las redes 3G y 4G. La UE y los gobiernos de cada Estado obligan a realizar un análisis de riesgo exhaustivo a todas las compañías antes de implantar y poner en marcha estas redes y se están desarrollando planes y aprobando normativa para garantizar una evolución tecnológica más sostenible. No hay seguridad 100% pero si serán mucho más seguras que las redes precedentes en el momento de su implantación y puesta en marcha.

---

### 2.5.3.- Teletrabajo

---

En el ámbito de la ciberseguridad, todos y cada uno de los eslabones tienen una importancia capital, incluido el eslabón que supone el componente humano, que tiene la consideración del más débil. En este punto, la formación y la concienciación de las personas en materia de ciberseguridad es fundamental.

A lo anterior, hay que sumarle el aumento de nuevas formas de organización del trabajo, como es el **teletrabajo** ([Parlamento Europeo: The impact of teleworking and digital work on workers and society.](#)), que ha ido en aumento desde la declaración de la pandemia, y que acarrea nuevos retos tecnológicos relativos a conexiones, uso de dispositivos personales, descentralización, etc.

---

### 2.5.4.-Uso de Inteligencia Artificial (IA) para atacar y defender infracciones

---

El ámbito del desarrollo y aplicación de la Inteligencia Artificial supone al mismo tiempo una amenaza y una solución ([Harvard Kennedy School: Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It](#)). Por un lado, los ciberataques se vuelven cada vez más sofisticados con el uso de este tipo de tecnologías, pero también con la ayuda de la IA los sistemas automatizados pueden detectar cualquier irregularidad y proteger los sistemas que pueden ser objeto de un ciberataque. En la actualidad, muchos de los sistemas de identificación de riesgos utilizan IA para detectar nuevas amenazas. La Inteligencia Artificial también se puede utilizar como un método de prueba y error para realizar ataques predefinidos, realizar seguimiento y encontrar soluciones que puedan ayudar a las organizaciones a prepararse para enfrentar cualquier tipo de ataque en el futuro.

---

### 2.5.5.- Computación cuántica

---

La computación cuántica supondrá en un futuro más o menos



cercano, una auténtica revolución pues, si bien todavía está en una etapa de construcción y exploración de las posibilidades su tecnología, se tiene casi la certeza de que los esquemas de cifrado actuales podrían no ser totalmente seguros una vez entren en uso las tecnologías cuánticas del futuro. Esto pondría en peligro la información confidencial actual, ya que los atacantes podrían recolectar datos actuales para descifrarlos en el futuro. No obstante, la buena noticia es que ya contamos con los primeros protocolos para el desarrollo de los estándares de ciberseguridad cuánticos, cuyos algoritmos tendrán que ser ahora revisados y mejorados en los próximos años.

---

## **2.6.- Propuestas**

---

---

### **2.6.1.- Concienciación**

---

- ✓ Para la ciudadanía, desde todos los niveles de la Administración (general, autonómica y local), incorporando todos los rangos de edad, así como fomentar el desarrollo de profesionales y expertos en materia de ciberseguridad incorporando esta materia dentro de los planes de formación académicos de enseñanza básica y media e, incluso, como una opción de especialización universitaria (la demanda de "ingeniero de ciberseguridad"), charlas de concienciación en colegios, etc.
- ✓ Para las PYMES, a través de asociaciones, consultoría personalizada, etc., con contenidos producidos por las autoridades competentes en la materia (ej. INCIBE), y aprovechando distintos medios de comunicación estatales y privados. Este tipo de actuaciones deben dirigirse no sólo a personal TI, sino también a gerentes y mandos intermedios de las empresas dado su papel en la toma de decisiones.

- ✓ Para organizaciones grandes, mediante la colaboración los centros de referencia de las Administraciones Públicas y los Cuerpos y Fuerzas de Seguridad del Estado, y la cooperación entre las diferentes industrias, *por ejemplo, mediante campañas conjuntas, así como mejorar las medidas técnicas relacionadas con la ciberseguridad, de forma que se favorezca la robustez y resiliencia de los servicios digitales, especialmente aquellos prestados por los organismos públicos y prestadores de servicios esenciales.*

---

### **2.6.2.- Gestión del riesgo desde un inicio**

---

- ✓ Impulsando y promoviendo la gestión del riesgo en la cadena de suministro: siendo fundamental, la formación y certificación de las personas y proveedores, así como fomentar la creación de entornos seguros por defecto y acuerdos de niveles de servicio robustos.
- ✓ Promoviendo la Seguridad "by design" y "by default": Aplicando las medidas técnicas y organizativas necesarias y adecuadas para garantizar la protección y privacidad de los datos de los ciudadanos antes de llevar a cabo el tratamiento de la información, realizando auditorías normativas y técnicas que permitan detectar las vulnerabilidades y debilidades de seguridad que pueden ser utilizadas por terceros malintencionados para robar información, o en general, causar daños a la empresa o al ciudadano.

---

### **2.6.3.- Promover el desarrollo de modelos de gobernanza de la ciberseguridad**

---

Desarrollando una estructura que cuente con una composición mínima que esté adaptada a la situación de cada compañía, permitiendo capturar información sobre la identificación, respuesta y recuperación sobre los principales nuevos ciberataques padecidos durante la crisis y tomar las medidas oportunas para

poder quedar protegidos ante su eventual repetición incluyendo la automatización de las respuestas y de “lecciones aprendidas”, compartiéndolas siempre que sea posible.

---

#### **2.6.4.- Regulación**

---

- ✓ Asegurar un elevado nivel de armonización en la normativa de aplicación a nivel nacional y europeo, fomentando la estandarización y colaboración a nivel mundial, mediante la implementación de mecanismos formales y eficaces de cooperación internacional.
- ✓ Difundir en el entorno empresarial iniciativas, regulaciones y estándares existentes a nivel europeo para la protección de las infraestructuras IT frente a ataques (i.e. programas de estandarización IoT, requisitos de ciberseguridad en evaluaciones físicas, etc.).
- ✓ Impulsar una nueva ética en el uso de los datos y la IA, en línea con los trabajos realizados en el ámbito de la UE, entre los que se incluye el de la UNESCO ([UNESCO: Ética de la Inteligencia Artificial](#)), con el fin de mitigar los posibles sesgos que se pueden generar con su implementación.
- ✓ Promover que las certificaciones y estándares actuales de seguridad se adapten a una visión más real de la ciberseguridad.

## Referencias de interes

1. <https://www.ccn.cni.es/index.php/es/menu-ccn-es/consejo-nacional-de-ciberseguridad>
2. <https://www.aepd.es/es>