## Palabras clave:

Ciberseguridad, ciberincidente, vulnerabilidad, acceso remoto, teletrabajo, ENS, ransomware, IoT, inteligencia artificial, desinformación, CCN-CERT, CERT, CSIRT, transformación digital, técnicas, tácticas y procedimientos.

# Cybersecurity. Developments and trends

## Abstract:

*The challenges we face with the constant development of the information society in the 21st century is closely linked to the concept of cybersecurity. This essay shows the evolution of this idea of information security and its regulation as technology and threats to it have changed. They are threating whose evolution is also analysed and whose consequences have made the objective of guaranteeing and implementing security in cyberspace, while at the same time respecting the privacy and freedom of individuals, unavoidable. This has been understood by the main governments that have made cybersecurity one of their strategic priorities, due to its direct impact on national security, on the competitiveness of companies, and on the prosperity of society.*

*While digital transformation was already a challenge that organisations had to face with greater or lesser haste, the outbreak of the Covid19 pandemic in 2020 brought about the need to adapt technological and human resources to this new reality at an accelerated pace. A reality that, in the case of Spain, will be marked in the coming years by the development of the National Cybersecurity Strategy, the new National Security Scheme that is in the process of being approved and the governance by the public and private actors responsible for implementing and facilitating a secure and reliable cyberspace.*

## Keywords:

*Cybersecurity, cyber incident, vulnerability, remote access, telework, ENS, ransomware, IoT, Artificial Intelligence, disinformation, CCN-CERT, CERT, CSIRT, digital transformation, TTP (Techniques, Tactics and Procedures).*

## Introducción

El término ciberseguridad se define como la habilidad de proteger y defender las redes o sistemas de los ciberataques[1]. No obstante, este concepto ha tenido una evolución significativa en los últimos treinta años.

Los conceptos iniciales asociados a la ciberseguridad datan de finales del siglo pasado. A partir de 1990, la OTAN aglutina las definiciones de seguridad de transmisión (TRANSEC), seguridad de redes (NETSEC) y seguridad de ordenadores (COMPUSEC) en un concepto único denominado seguridad de la información (INFOSEC) que debe proteger la información en sus tres dimensiones de confidencialidad, integridad y disponibilidad.

Posteriormente, en 2002, Estados Unidos propone enriquecer este concepto con el de aseguramiento de la información (*information assurance*) e introduce dos nociones más: autenticidad y no repudio (traducido como trazabilidad). Estos se incorporan a la Seguridad de las Tecnologías de Información y Comunicaciones (STIC) debiendo proteger la información y los sistemas que la manejan en las cinco dimensiones:

- Confidencialidad[2]
- Integridad[3]
- Disponibilidad[4]
- Autenticidad[5]
- Trazabilidad[6]

[1] Ciberataque: Uso de redes y comunicaciones para acceder a información y servicios sin autorización con el ánimo de robar, abusar o destruir.
[2] Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados [UNE-ISO/IEC 27000:2014].
[3] Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada [UNE-71504:2008].
[4] Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren [UNE-71504:2008].
[5] Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos [UNE-71504:2008].
[6] Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad [UNE-71504:2008].


Figura 1. Evolución del concepto de ciberseguridad.

Hasta 2005 (figura 1), prácticamente toda la doctrina emanaba de la OTAN y el objetivo era proteger la información clasificada manejada por los sistemas. La idea más utilizada era la prohibición de que un sistema manejara información clasificada sin la inspección correspondiente, para lo que se exigían numerosos documentos descriptivos del sistema y de sus medidas de seguridad que pronto se quedaban obsoletos.

A partir de entonces se constata el interés de la Unión Europea en la seguridad de los sistemas cambiando del concepto INFOSEC/INFO ASSURANCE al de ciberseguridad. Quizá la definición más clara de este término nos la proporciona la OTAN al asegurar que la ciberseguridad es la implantación práctica del *information assurance*; un concepto más operativo basado en la responsabilidad compartida entre la autoridad que debe autorizar el sistema a manejar información clasificada y aquella responsable de su manejo. Con la ciberseguridad se afianzan conceptos como vigilancia y respuesta; auditoría continua y notificación de incidentes. Estos son los principios básicos que recogen la mayoría de las normas de ciberseguridad nacionales (Esquema Nacional de Seguridad, ENS) e internacionales (Directiva de Seguridad en Redes de la Unión Europea —Directiva NIS— y Regulación de Protección de Datos de la UE).

Debemos reseñar que el ENS, cuya actualización está ultimándose en estos momentos, es la primera norma en un país europeo que establece unos principios básicos (6), unos requisitos mínimos (15) y unas medidas de seguridad de obligado cumplimiento (75).

Establece además la obligación de notificar incidentes, da al CCN-CERT[7] el mandato de actuar con celeridad ante cualquier agresión recibida y fija el deber de superar una auditoría cada dos años, estableciendo un proceso de certificación en el esquema de todos los sistemas afectados.

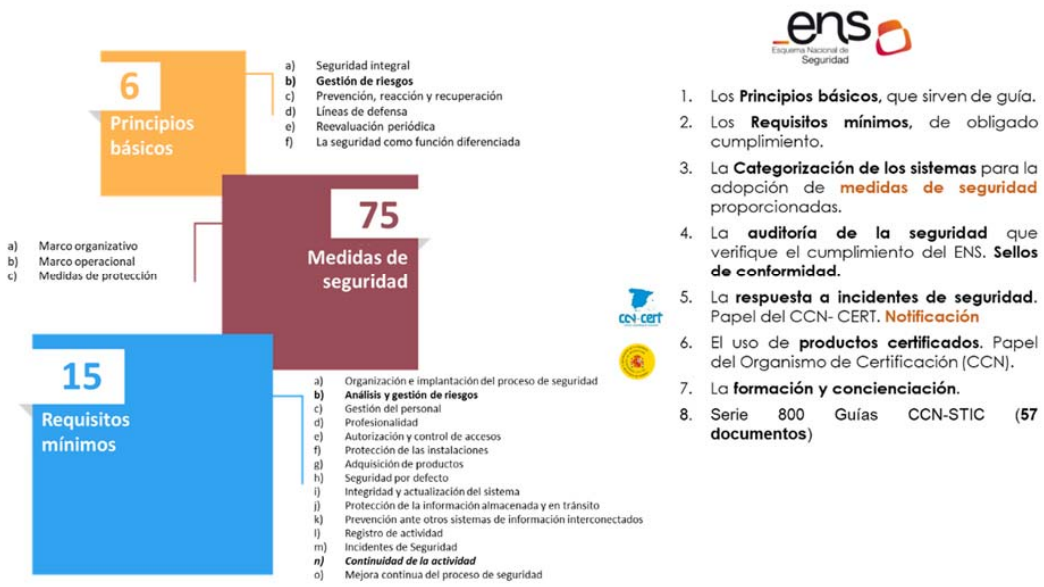


Figura 2. Aspectos más destacados del ENS.

En cuanto a las normas internacionales, la Regulación de Protección de Datos de la UE basa la implementación de medidas de ciberseguridad en la gestión de riesgos y establece la obligación de notificar ciberincidentes (brechas de seguridad), mientras que la Directiva NIS afianza los conceptos para los sistemas TIC que soportan los servicios esenciales de una sociedad, como podrían ser el sistema bancario, el sector de aguas, el sector energético, el sector transporte o el sector de la salud.

Finalmente, en esta década el concepto que está en todas las agendas de Gobiernos y empresas es el de transformación digital (TD), que se ha acelerado con la pandemia de la COVID-19 y la implantación del teletrabajo por las restricciones de movilidad. Esta TD sin ciberseguridad sería como un salto al vacío. Por ello, se requiere una actitud más proactiva ante las ciberamenazas que se materializan en los conceptos de defensa activa y ciberinteligencia, cada vez más útil, y que permite a los defensores el conocimiento

[7] Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional.

profundo de las tácticas, técnicas y procedimientos (TTP) de los atacantes para poder realizar una detección y respuesta eficaz.

Así, los conceptos que se impondrán entre 2020 y 2030 son los de *zero trust* (medidas de ciberseguridad en las interconexiones de los diferentes sistemas, aunque pertenezcan a la misma empresa u organización), el de seguridad por defecto en los sistemas (articulando esquemas de certificación para el internet de las cosas, los servicios en nube, las tarjetas inteligentes o los sistemas que soportan servicios esenciales) y auditoría y vigilancia, resaltando la necesidad de que sean continuas en el tiempo. Además, se debe evolucionar hacia un intercambio de incidentes, donde todos los equipos formen parte de un sistema y dejando atrás el concepto de «notificación». Gracias al modelo de diamante (figura 3) se pueden determinar las TTP de un atacante. En su eje horizontal se describen las características técnicas del ataque y en el vertical las motivaciones del atacante. Del mismo modo, los equipos de respuesta a incidentes, CERT[8] o CSIRT[9], deben enviar toda la información de valor sobre las ciberamenazas y su comunidad (público al que dan servicio) debe responder intercambiando todos los ciberincidentes que sufra.

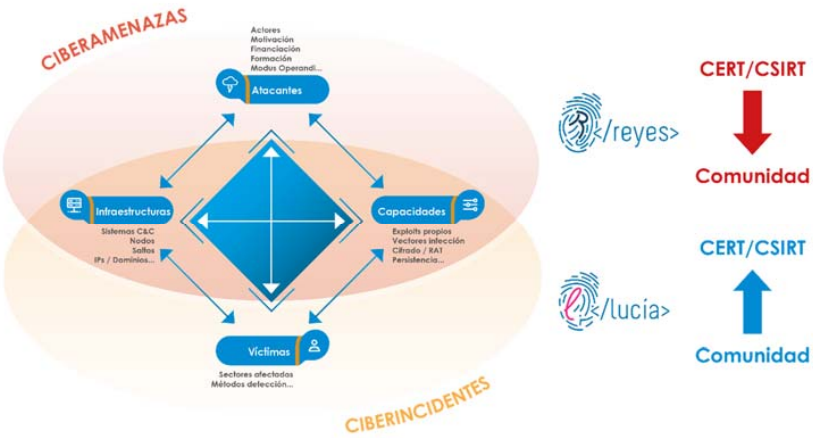


Figura 3. Modelo de diamante.

[8] Guía CCN-STIC 401, del Centro Criptológico Nacional. CERT. Computer Emergency Response Team. Organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.

[9] CSIRT Computer Security Incident Response Team. An organization «that coordinates and supports the response to security incidents that involve sites within a defined constituency.» [R2350] (Ver: CERT, FIRST, *security incident*) [RFC4949:2007].

Finalmente, los servicios en la nube y los accesos remotos (teletrabajo) son conceptos que han venido para quedarse en el nuevo entorno tecnológico donde el límite de nuestro sistema de información es más difuso y está compartido con nuestros proveedores. La interconexión con otros organismos para la prestación de servicios es casi obligatoria y la necesidad de monitorización y vigilancia se antoja fundamental para evitar su interrupción ante los ataques.

## Evolución normativa

Hasta principios de este siglo, excepto la Ley Orgánica de Protección de Datos de Carácter Personal (1999)[10], el ordenamiento jurídico español no contaba con normas que regularan la ciberseguridad.

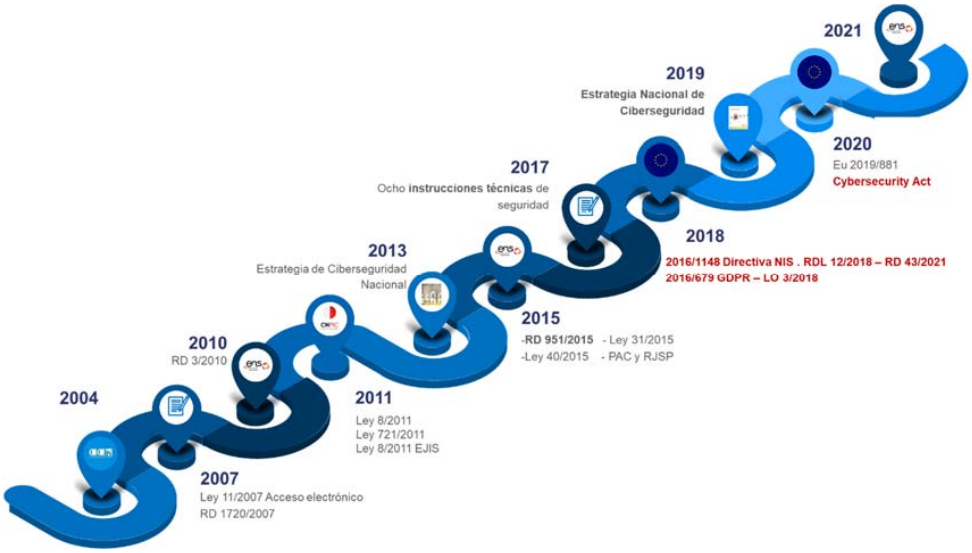


Figura 4 Evolución de la normativa de Ciberseguridad en España.

La Ley 11/2002, de 6 de mayo reguladora del Centro Nacional de Inteligencia (CNI), viene a corregir esta situación y en ella ya se establece como una de sus funciones la de «coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la

[10] Ley Orgánica 18/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en su redacción dada por la Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional, por la que se declaran nulos determinados preceptos —BOE núm. 4 de 4-1-2001— y por la Ley 62/2003, de 30 de diciembre).

información en ese ámbito…». Una función que, precisamente, da origen al Centro Criptológico Nacional, regulado dos años después a través del Real Decreto 421/2004, de 12 de marzo.

Posteriormente, la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, ya expone que el principal reto que tiene la implantación de las TIC en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización.

Un año antes, el Plan Avanza 2006-2010[11] ya menciona el desarrollo de una red de centros de seguridad cuyo principal objetivo sea crear una infraestructura básica de centros de alerta y respuesta ante incidentes de seguridad que atienda a las demandas específicas de los diferentes segmentos de la sociedad. En este mismo texto se adelanta la creación de un CERT para la Administración/Gubernamental.

La aprobación del ENS en 2010 (con dos actualizaciones en 2015 y una próxima en ciernes [figura 5]) establece una aproximación a la ciberseguridad guiada por las mejores prácticas internacionales y utilizando las guías CCN-STIC, del Centro Criptológico Nacional, para concretar los principios y las medidas de aplicación difusa.

En 2011, la Ley de Infraestructuras Críticas[12] puso el foco en los sectores estratégicos, aunque muy centrada en ataques terroristas y focalizada en los activos físicos. En 2016, la UE enriquece el concepto de infraestructura crítica con el de servicio esencial, centrándolo en evitar ciberataques a los sistemas TIC que lo soportan (directiva NIS). España traspuso esta directiva con el Real Decreto Ley 12/2018, que ha servido para ordenar el modelo de gobernanza de la ciberseguridad española esbozado en la Estrategia de Ciberseguridad Nacional de 2013 y consolidado en 2019[13].

Así pues, con la regulación de la protección de datos (publicada como reglamento pero enriquecida con la Ley Orgánica 3/2018) y la Ley de Ciberseguridad de 2020 (Cybersecurity Act), la Unión Europea está terminando de definir su aproximación a la ciberseguridad, que completará con la actualización de la directiva NIS (conocida como

[11] Plan Avanza 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas. Disponible en: https://avancedigital.mineco.gob.es/programas-avance-digital/Paginas/plan-avanza.aspx.
[12] Ley 8/20211, de 28 de abril, «por la que se establecen medidas para la protección de las infraestructuras críticas».
[13] Orden PCI/487/2019, de 26 de abril, «por la que se publica la Estrategia Nacional de Ciberseguridad 2019», aprobada por el Consejo de Seguridad Nacional (12 de abril de 2019).

NIS 2.0), refinando los criterios para la notificación de incidentes transfronterizos, homogeneizando la designación de los operadores y estableciendo métricas para medir el nivel de ciberseguridad de estos operadores.

Se espera que durante los próximos años toda esta normativa alcance mayor grado de madurez y se vayan generando esquemas de certificación de las diferentes tecnologías, se impulse una red de Centros de Operaciones de Ciberseguridad (SOC) en la UE, se fortalezca el papel de las agencias de ciberseguridad y se puedan coordinar las capacidades nacionales. También se observan pasos decididos en la respuesta diplomática conjunta en lo que se conoce como *cyberdiplomacy toolbox*[14].

Por último, cabe decir que España puede aportar una aproximación muy práctica en gestión de riesgos, intercambio automatizado de incidentes y definición de métricas para establecer la posición de ciberseguridad de una organización. El nuevo ENS (figura 5) que se está desarrollando añade un nuevo principio básico (siete en total): vigilancia continua y reevaluación periódica. En él se resalta el concepto dinámico de la ciberseguridad con una medición permanente de la superficie de exposición y se complementa con el de prevención, detección, respuesta y conservación.

Además, cambia el concepto de «seguridad por defecto» al de mínimo privilegio y presta especial atención a aspectos tales como la protección de la cadena de suministro, la interconexión de sistemas, los servicios en la nube o la protección de la navegación web.

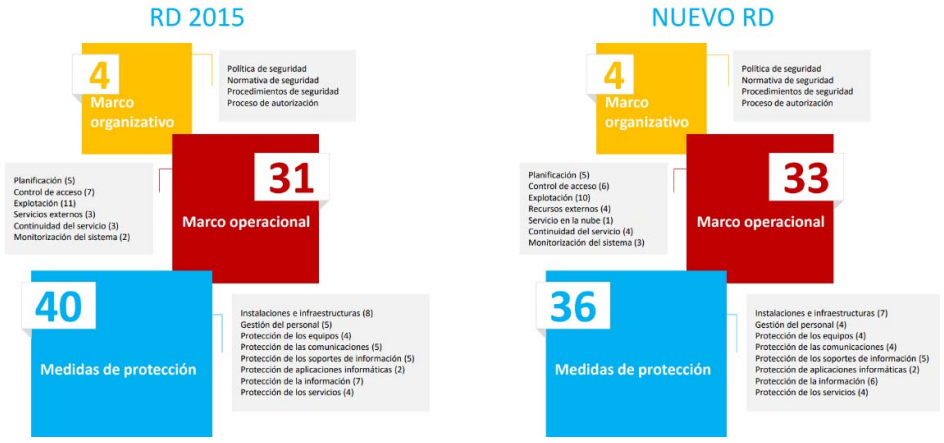


Figura 5. Cambios más relevantes del ENS.

[14] El Consejo de Europa acordó en 2017 elaborar un marco para una respuesta diplomática conjunta de la UE, dispuesta a responder con diversas medidas, incluidas las sanciones a los ciberataques. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

**Evolución de las ciberamenazas**

Los conceptos y la normativa se han ido configurando para responder a unas ciberamenazas cada vez más orientadas a destruir, alterar y sustraer la información y a quebrantar o interrumpir la disponibilidad de los servicios.

Para tener una aproximación práctica a este fenómeno, el CCN-CERT establece una priorización por agentes de la amenaza, según sus motivaciones:

- Ciberespionaje. Ciberataques realizados para obtener secretos de Estado, propiedad industrial, propiedad intelectual, información comercial sensible o datos de carácter personal. Es, junto con el cibercrimen, los ataques que causan una mayor preocupación al CCN (figura 6), siendo con diferencia la amenaza más compleja y con mayor capacidad técnica. Su detección se debe basar en técnicas que analicen comportamientos anómalos y que requieren herramientas tecnológicamente muy avanzadas y un personal muy experto en la detección y respuesta a este tipo de ataques.
- Ciberdelito/cibercrimen. Actividad que emplea las redes y sistemas como medio, objetivo o lugar del delito. Se les aplican todas las figuras delictivas del crimen tradicional pero adaptadas al ciberespacio. Normalmente su motivación es el rendimiento económico y sus objetivos son más indiscriminados: víctimas que dispongan de la vulnerabilidad adecuada y con la capacidad financiera para atender a sus demandas. Durante 2021 han destacado sobremanera los grupos de *ransomware*[15] que se describirán en un capítulo específico.
- Ciberactivismo. Activismo digital antisocial. Persiguen el control de redes o sistemas (sitios web) para promover su causa o defender su posicionamiento político o social. En 2021 han reducido considerablemente su actividad y la capacidad de coordinación que disponían en 2015 se ha mermado considerablemente.
- Ciberterrorismo. Actividades dirigidas a causar pánico o catástrofes en las redes y sistemas o utilizando estas como medio.
- Uso de internet por los terroristas. Actividad de los grupos terroristas que utilizan internet como soporte de comunicaciones y coordinación, para obtención de

[15] El *ransomware* es un código dañino para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado.

información de posibles objetivos en tareas de propaganda, radicalización o financiación de sus actividades. Su volumen ha crecido considerablemente, aunque dista mucho del empleo de internet para causar terror atacando a infraestructuras críticas en las que se siguen sin detectar casos relevantes. Por lo tanto, en el concepto puro del término ciberterrorismo los casos detectados son mínimos y sin impactos.

- Ciberconflicto/ciberguerra/guerra operación dirigida por un Estado para desestabilizar otros Estados y polarizar a la población civil. Incluye una gran variedad de herramientas como diplomacia y acciones de inteligencia tradicional, actos subversivos y de sabotaje, influencia política y económica, instrumentalización del crimen organizado, operaciones psicológicas, propaganda y desinformación y ciberataques. Han tenido un crecimiento constante y se considera que son, en muchos casos, el paso posterior a una actividad de ciberespionaje. Una vez colonizada la red víctima, con las mismas herramientas con las que roban información podrían realizar acciones de cibersabotaje contra infraestructuras críticas y otros servicios esenciales de un país.

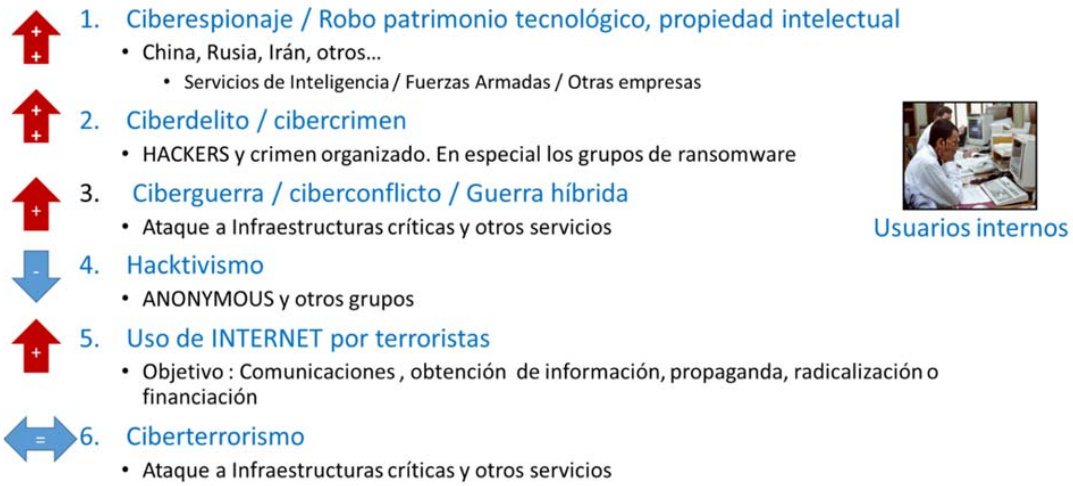


Figura 6 Importancia de las amenazas según el CCN-CERT.

***Las vulnerabilidades en la tecnología***

Las vulnerabilidades[16] son consustanciales al software. Todos los años se publican alrededor de 5000 en las diferentes tecnologías (el CCN-CERT publica en su portal diariamente las de los principales fabricantes y emite avisos y alertas a su comunidad cuando constata alguna de especial gravedad[17], Figura 7).

Las consecuencias de este fallo en el *software* pueden ser muy variadas. Desde la posibilidad de ejecutar remotamente código por el atacante, lo que permitiría un control externo del sistema afectado, hasta que el sistema deje de funcionar correctamente. Algunos fabricantes (Microsoft, Oracle, Cisco, Adobe, Android o Apple, por ejemplo) publican periódicamente actualizaciones de seguridad conocidas como parches para resolver las deficiencias detectadas.

[16] Vulnerabilidad. Debilidad de seguridad de un sistema que le hace susceptible de poder ser dañado al ser aprovechada por una amenaza. *Guía CCN-STIC-400*.
[17] Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades.html.


## Vulnerabilidad en Microsoft

Fecha de publicación: **01/07/2021**
Nivel de peligrosidad: **CRÍTICO**

El Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN-CERT, alerta de la publicación de actualizaciones de seguridad de **Microsoft** correspondientes al mes de junio.

Con el lanzamiento del boletín de seguridad de Microsoft correspondiente al mes de junio se solucionaron **50 vulnerabilidades**; 10 de las cuales fueron calificadas como críticas; y 40 fueron catalogadas como altas, según el criterio de la compañía.

Sin embargo, **una de esas vulnerabilidades**, inicialmente catalogada como alta, ha sido **reclasificada a un nivel crítico**. Este error, en un principio fue clasificado como una vulnerabilidad que permitía solamente una escalada de privilegios dentro del sistema, no obstante, en esta nueva reclasificación, se le ha otorgado un nivel crítico debido a que permite la ejecución de código de forma remota (RCE).

El CVE asignado es el CVE-2021-1675, y se ha publicado esta nueva clasificación en la página oficial de Microsoft después de que el equipo de ciberseguridad de la empresa China QiAnXin Technology explotara esta vulnerabilidad llegando a ejecutar código arbitrario de forma remota. En concreto, la vulnerabilidad reside en el servicio Print Spooler (spoolsv.exe) encargado de administrar el proceso de impresión, **afectando a todas las versiones del sistema operativo Windows.** Destacar que desde la empresa China se ha evitado revelar los detalles técnicos sobre el ataque.

Asimismo, en adición a lo anterior, tres analistas de la firma de seguridad china Sangfor, publicaron un exploit para aprovechar esta vulnerabilidad después de que los investigadores de QiAnXin compartieran el video de la prueba de concepto (PoC) realizada en sus investigaciones. Unas pocas horas más tarde, los expertos retiraron el exploit.

**Recomendaciones:**

Se recomienda encarecidamente a los usuarios y administradores de sistemas que apliquen los parches de seguridad en cuanto se encuentren disponibles, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos. Por el momento, Microsoft no ha revelado medidas de mitigación alternativas a la actualización de los sistemas a fin de parchear la vulnerabilidad descrita.

Sin embargo, como solución alternativa si no es posible aplicar los parches de seguridad correspondientes, se recomienda deshabilitar el servicio Print Spooler:

- How to Disable/Enable Print Spooling Service.

**Referencias:**

- Windows Print Spooler Remote Code Execution Vulnerability.
- PoC exploit for CVE-2021-1675 RCE started circulating online.
- Privilege escalation in Microsoft Windows Print Spooler.

Atentamente,

Equipo CCN-CERT

Figura 7. Ejemplo de alerta emitida por el CCN-CERT a su comunidad.

Por otro lado, las vulnerabilidades denominadas día cero o *zero day* tienen un tratamiento especial por ser aquellas que son desconocidas por el fabricante y por lo tanto no existe actualización de seguridad para la misma. Existe un mercado negro muy lucrativo de compraventa de estas vulnerabilidades por Gobiernos, empresas y *hackers* en la *dark web*[18].

Finalmente existe otro tipo de vulnerabilidad conocida como día uno donde el fabricante ha publicado la actualización de seguridad, pero los responsables TIC de la organización todavía no la han desplegado en sus sistemas y por lo tanto estos son todavía vulnerables.

La existencia de estas vulnerabilidades en la tecnología requiere, como ya se ha señalado, una auditoría continua y la automatización de las actualizaciones de seguridad de las distintas tecnologías. Todo ello junto con la vigilancia continua que intenta detectar cualquier actividad del atacante dentro de los sistemas.

### *La explosión del* ransomware*. La otra pandemia*

El *ransomware* es un código dañino con capacidad de cifrar los ficheros o dispositivos de la red de una organización. En 2014 ya se utilizaba para extorsionar a usuarios particulares a los que se pedía un rescate en bitcoines[19] (en aquel momento el valor de una unidad equivalía a quinientos euros).

Este tipo de ataque ha ido evolucionando y ha pasado de tener como víctimas a usuarios particulares a atacar a organizaciones públicas y privadas de gran tamaño con la consiguiente petición de rescates cada vez más abultados. A este nuevo tipo de ataque se le conoce como *human operated ransomware* (HOR), donde los atacantes consiguen penetrar en la red manejando *malware* junto con herramientas ofensivas con la finalidad de establecer persistencia, realizar movimiento lateral, extraer información y finalmente cifrar la información.

Durante 2021, los precios de esta extorsión se han incrementado considerablemente (figura 8). La media de los rescates pagados por empresas pequeñas asciende a unos

[18] Porción de internet intencionadamente oculta a los motores de búsqueda, con direcciones IP enmascaradas y accesibles solo con un navegador web especial (Xakata.com)
[19] Bitcóin es una criptomoneda/moneda virtual, sistema de pago y mercancía. Fue concebida en 200 por una entidad conocida bajo el seudónimo de Satoshi Nakamoto. Es la más popular. Su valor máximo en 2020 fue de 20 000 euros. En 2021, el valor máximo alcanzado ha sido de 60 000 euros.

8000 dólares, mientras que el rescate para las grandes empresas se acerca a los 180 000 dólares.

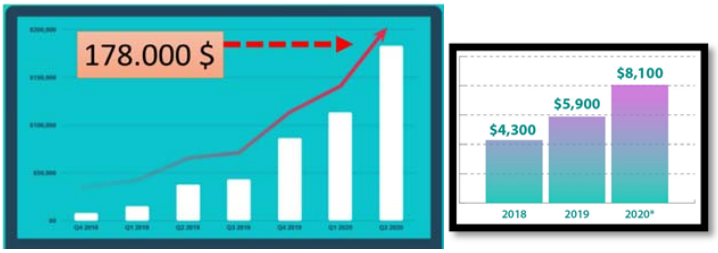


Figura 8. Evolución del precio pedido por el rescate del *ransomware*.

Una situación agravada por la pandemia y las exigencias del teletrabajo que obligó a las organizaciones a habilitar tecnologías que permitían a sus usuarios acceder remotamente desde sus casas a los diferentes recursos, aplicaciones y bases de datos de la red corporativa. Esta migración no se hizo de la manera más segura por razones de urgencia[20].

En 2021, el *ransomware* ha aumentado de forma espectacular porque los grupos de cibercrimen han sido capaces de asociarse y automatizar los ataques a las diferentes organizaciones [en España destacan los recibidos por el Servicio Público de Empleo Estatal (SEPE) o los ministerios de Economía y de Trabajo y Economía Social]. Hasta ahora el ataque más empleado era el *phishing*[21].

Los atacantes para entrar en los sistemas de las organizaciones suelen utilizar: credenciales débiles en los sistemas de acceso remoto, compra de credenciales legítimas en el mercado negro o explotación de vulnerabilidades en los dispositivos de protección de perímetro de la organización. Quizá la segunda opción es la más utilizada. Así, las TTP más comunes de los atacantes durante este año 2021 han sido las siguientes:

[20] *Medidas de Seguridad para acceso remoto del CCN*. Disponible en: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/191-abstract-politica-de-acceso-remoto-seguro/file

[21] *Phishing*: método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.

1. Compra de credenciales de acceso remoto a la organización en el mercado negro.
2. Entrada en la red por un acceso remoto a la misma y elevación de privilegios a administrador en un servidor.
3. Instalación de herramientas de control remoto, como Cobalt Strike y movimiento lateral para controlar toda la red.
4. Robo de información de la organización (datos personales o propiedad industrial) que permita la extorsión y fuerce el pago del rescate.
5. Cifrado de datos de la organización y solicitud de rescate.

Estas TTP se han automatizado por parte de los cibercriminales y han alcanzado una eficiencia espectacular. Se han detectado ataques que en solo dos horas han entrado a la red y han sido capaces de detonar el *ransomware*, eliminar las copias de seguridad de la víctima, ocasionar un daño irreversible y provocar el pago del rescate o la caída de todo el negocio durante varias semanas.

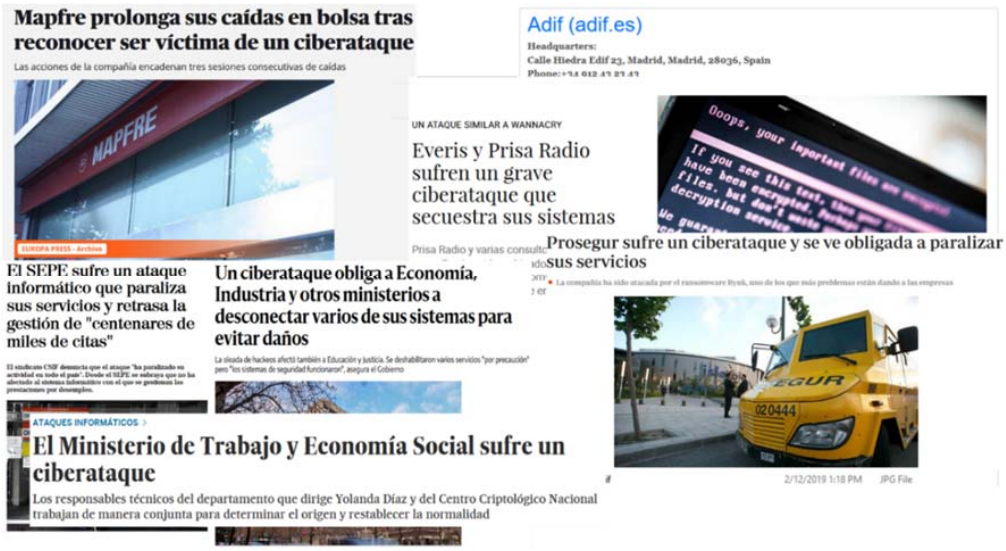


Figura 9. Repercusión en prensa de los principales ataques de *ransomware* en España.

De este modo, el CCN-CERT ha tenido que desplegar en lo que llevamos de año equipos de respuesta rápida en más de quince organizaciones para ayudar a recuperarse del impacto de estos ataques. Dicho impacto suele ser el cifrado total o parcial de la red, la perdida de información (publicada posteriormente si no se satisface el rescate) y la caída de todos los servicios de la organización, como la atención a los desempleados en el caso del SEPE. Cuando se cifra la red de la organización la recuperación puede llevar

varias semanas con el consiguiente daño causado a los ciudadanos y a la imagen de la organización[22].

***El ciberespionaje de los grupos relacionados con Estados. La amenaza permanente***

Durante 2021, los casos de ciberespionaje patrocinados por Estados se han seguido incrementando. Su objetivo es obtener secretos de Estado, propiedad industrial o intelectual, información comercial sensible o datos de carácter personal. Al ser un actor sistemático, con objetivos permanentes y con protección estatal es con diferencia el actor más peligroso que podemos encontrar.

Son grupos técnicamente avanzados que se mueven por objetivos con las siguientes características:

- Están motivados y disponen de la paciencia necesaria para esperar a que se presente la vulnerabilidad de la red.
- Disponen de gran cantidad de recursos económicos para articular infraestructuras que garanticen su anonimato y desvinculación, así como la adquisición de las vulnerabilidades día cero que sean necesarias.
- Disponen de gran cantidad de recursos humanos con especialización en cada una de las tecnologías claves de las redes corporativas.

Su objetivo es permanecer en la red víctima el máximo tiempo posible pudiendo permanecer en redes durante años. La información que extraen está muy depurada, pues su conocimiento de la red objetivo es muy profundo, superando incluso al de los administradores de la misma red.

En el año 2010 destacaban los grupos con procedencia de Rusia por ejecutar ataques muy sigilosos y con unas herramientas propietarias muy avanzadas. En cambio, los actores chinos que no eran tan sigilosos se centraban en redes de empresas y usaban herramientas más ruidosas (figura 11). Sin embargo, en la actualidad, el nivel de

[22] De esta experiencia, el CCN-CERT ha desarrollado el documento de *Buenas prácticas 21* sobre gestión de incidentes de *ransomware*. Disponible en: https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp.html

complejidad y sigilo de estos últimos se ha incrementado mucho y la dificultad de detección es ya similar.

Por otro lado, existen actores de menor complejidad como los de Corea del Norte o Irán que utilizan los ciberataques para financiarse y para seguimiento de sus comunidades.

No obstante, a causa de la facilidad de ocultación y de engaño con ataques de falsa bandera (simulando a otro país) no se puede descartar ciberataques desde ningún origen.

Últimamente, se está detectando una tendencia de uso de *ransomware* por actores de ciberespionaje para ocultar trazas de ataque o para distraer la atención de los responsables de ciberseguridad. Por supuesto, también utilizan TTP del cibercrimen para confundirse con estos.


Figura 10. Planos de los aviones F-35 estadounidense y J31 chino.

***El ciberespionaje sobre plataformas móviles. El ataque más rentable***

Las plataformas móviles se han convertido en un vector de ataque utilizado por los diferentes actores por la extraordinaria rentabilidad que supone poder acceder a toda la información disponible en el dispositivo de una autoridad como contactos, correos electrónicos, ubicación o conversaciones de cualquier sistema de mensajería tipo WhatsApp, Telegram o Signal. También con ataques a redes sociales como Twitter o Instagram mediante el secuestro de los perfiles de los usuarios.

Además, la implantación de la nueva tecnología de comunicación 5G incrementa las posibilidades de comunicación y de actuación en remoto, pero introduce nuevas vulnerabilidades sobre las tecnologías ya existentes.

El CCN-CERT publica un informe específico relacionado con las vulnerabilidades y los ataques más frecuentes en estas tecnologías[23]. En él se analizan los dos sistemas operativos dominantes: Android (85 % del mercado) y Apple (15 %).

Determinar la seguridad de estas tecnologías es difícil, puesto que, en el caso de Android, la seguridad depende de cómo implemente y configure el fabricante el sistema operativo y cómo incorpore las últimas versiones de este en su plataforma. Para Apple, el entorno es más homogéneo y el seguimiento de las actualizaciones más fácil.

Por otro lado, el código de Android está disponible para su análisis y el de iPhone no (seguridad por oscuridad). Si lo valoramos desde el mercado negro la vulnerabilidad día cero de Android tiene mayor coste que la de iPhone, por lo que se deduce que estos últimos podrían ser más fáciles de atacar además de tener menor número de clientes.

En este contexto, durante este año 2021 han aparecido en prensa los ataques realizados por diversos Estados a líderes, periodistas u opositores utilizando la herramienta Pegasus de la empresa NSO. Esta herramienta proporciona la capacidad de infectar un teléfono móvil sin interacción del usuario y permitiendo el acceso a toda la información del dispositivo. Se calcula que más de 50 000 teléfonos han sido atacados con esta herramienta[24].

***La desinformación. Una amenaza emergente***

La excepcionalidad que ha caracterizado a 2020, tanto por el gran consumo de información digital debido al confinamiento, como por el carácter emocional de la situación, ha supuesto una ventana abierta a la desinformación y las noticias falsas, que se han propagado rápidamente entre los ciudadanos.

La información no contrastada, las advertencias mal interpretadas y las teorías de la conspiración han generado confusión entre la población, facilitando en muchos casos el éxito de los ciberataques[25]. Asimismo, se notificaron casos de desinformación vinculada al comercio ilegal de productos médicos no legítimos[26].

[23] *CCN-CERT IA-18/21*. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6113-ccn-cert-ia-18-21-informe-anual-2020-dispositivos-moviles-1/file.html.
[24] Informe de Citizanlab de diciembre de 2020.
[25] Ver https://www.muyseguridad.net/2021/01/02/desinformacion-ciberseguridad/.
[26] Ver https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

La UE ha tomado cartas en el asunto de las noticias falsas, como parte de su política de combatir y aumentar la resiliencia a los ataques de desinformación (se recomienda la lectura del documento de *Buenas prácticas* del CCN-CERT sobre esta problemática[27]). En diciembre de 2020, el Consejo Europeo hizo una llamada a los Estados miembros para mejorar la respuesta a las amenazas híbridas. En la misma línea, el Consejo Europeo animó a las plataformas digitales a contribuir a la lucha contra las *fake news* y otros tipos de desinformación vinculada a las vacunas de la COVID-19[28].

### *El fraude del CEO. La pandemia lo ha rentabilizado*

Otro mecanismo de estafa que ha visto incrementado su uso ha sido el conocido como fraude del CEO, un tipo de táctica BEC (*business email compromise*). En este ataque, el delincuente se gana la credibilidad ante sus víctimas suplantando la identidad del propietario o director de la empresa, o bien de un responsable, para defraudar a la empresa y a sus empleados, clientes, proveedores, etcétera.

En la mayoría de los casos, estos ataques se dirigen hacia personal relacionado con la contabilidad y las finanzas, ya que el foco suele estar en la realización de transferencias bancarias fraudulentas, el secuestro de conversaciones con proveedores o la modificación de datos de facturas para redirigir los pagos a un proveedor, de manera que el montante económico termine en manos de los atacantes.

Para socavar las finanzas de las empresas, los atacantes falsifican cuentas y sitios web corporativos (normalmente mediante ligeras modificaciones del nombre), envían correos de *phishing* dirigido (*spear phishing*) o introducen *malware* específico para analizar previamente los correos y no levantar sospechas, o bien para acceder a datos confidenciales de las potenciales víctimas.

En el último trimestre del año se ha detectado un incremento en los ataques a administraciones públicas españolas y a sus proveedores. En estos incidentes, además de utilizar las técnicas anteriores, los atacantes se han servido de datos obtenidos en los portales de contratación pública para dar más credibilidad a sus estafas y conseguir

[27] *BP/13 Desinformación en el ciberespacio*. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3552-ccn-cert-bp-13-desinformacion-en-el-ciberespacio-1/file.html.
[28] Ver https://www.consilium.europa.eu/en/policies/coronavirus/fighting-disinformation/.

engañar a sus víctimas. El teletrabajo ocasionado por la COVID-19 ha facilitado este tipo de ataques.

***Las brechas de datos. El compromiso de las credenciales***

En cuanto a incidentes relacionados con brechas de seguridad que afectan a datos personales se producen casi a diario, aunque en muchos casos no salen a la luz. En la mayoría de los casos, la motivación es económica. Cuando los ciberdelincuentes, a través de *malware*, *phishing*, técnicas de ingeniería social o cualquier otro método, consiguen acceder a los datos, piden un rescate a cambio de que estos no sean publicados o destruidos, lo cual representaría un gran daño para una compañía en caso de que no tuviese copias de seguridad. Según un estudio de la compañía CrowdStrike, más de una cuarta parte de las organizaciones afectadas pagan el rescate.

En 2020 se han producido casi a diario brechas de seguridad que han comprometido datos personales en empresas tan importantes como Microsoft, Aptoide, Decathlon España, Twitter, Canon, Intel o Volkswagen Group.

Esta cantidad de datos expuestos ha originado un mercado negro muy activo relacionado con la venta de credenciales. Para mitigar este riesgo, se ha popularizado un servicio de búsqueda de credenciales comprometidas en los diversos incidentes.

**IoT *y* botnets**

El internet de las cosas (IoT, por sus siglas en inglés) está cada vez más presente en nuestro día a día. Con la llegada del 5G se está haciendo un uso cada vez más generalizado de dispositivos interconectados como altavoces, asistentes de voz, enchufes o bombillas. En la actualidad, se estima que en torno al 33 % de los dispositivos englobados en esta categoría ya han sufrido algún tipo de incidente de seguridad, frente al 19 % del año anterior[29]. Este crecimiento sin precedentes se debe principalmente a estos factores:

- Crecimiento exponencial de dispositivos IoT.

[29] Ver https://pages.nokia.com/T005JU-Threat-Intelligence-Report-2020.html.

- Implementación insegura de dispositivos IoT a los que es fácil acceder directamente desde internet.
- Falta de actualizaciones de seguridad para estos dispositivos, lo cual los deja expuestos a *exploits* comunes de muchos actores de amenazas.
- Falta de un enfoque de seguridad de dispositivos IoT por parte de los propietarios de dichos activos.
- Dispositivos con contraseñas predeterminadas, conocidas públicamente, que en la mayoría de los casos no se reemplazan.

Estas vulnerabilidades hacen que el atacante pueda infectar grandes cantidades de ellos (cientos de miles o millones) y lo utilice para realizar cualquier tipo de ataque de denegación de servicio. A estas redes de ataque se les conoce como *botnets*.

Estas *botnets* se utilizan para otros fines como la distribución de *malware* o para dispositivos Android (móviles, TV inteligentes, etc.) que están expuestos con una mala configuración de este y que permiten su control remoto.

**Tendencias de las ciberamenazas**

Durante estos últimos veinte años, las tendencias de las ciberamenazas han evolucionado constantemente, como se han ido describiendo en los sucesivos informes del CCN-CERT[30].

[30] *Informe de ciberamenazas y tendencias 13/20*. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html.

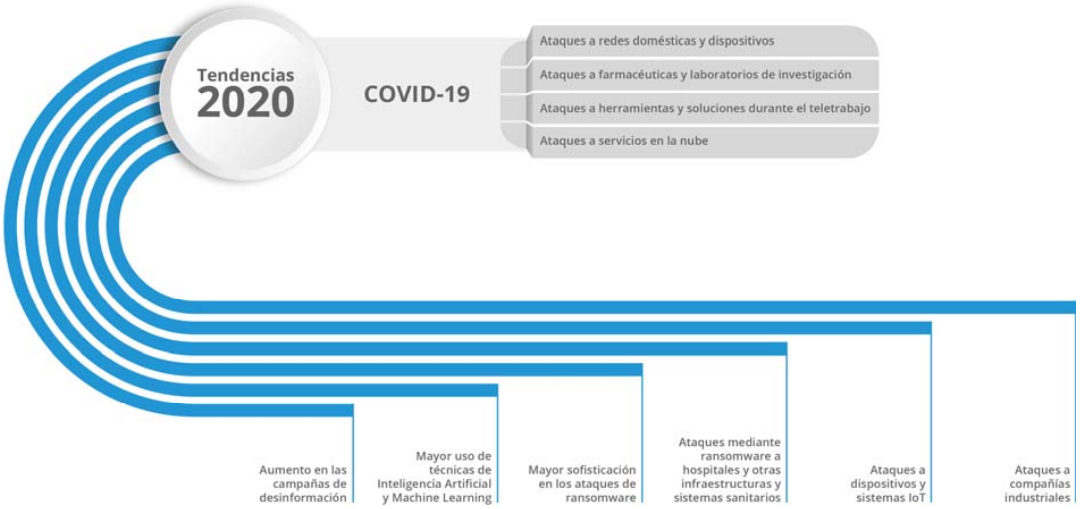


Figura 11. Tendencias de las ciberamenazas durante el año 2020.

El año 2020 estuvo marcado por la pandemia y las medidas de confinamiento adoptadas. Estas propiciaron un enorme despliegue de entornos tecnológicos de teletrabajo para salvaguardar la continuidad de actividades y negocios. La forma tan apresurada de su despliegue provocó que no se evaluaran los riesgos asociados, ni las soluciones, ni los protocolos de actuación, incorporando numerosas deficiencias de seguridad que los ciberatacantes han sabido aprovechar.

El aumento de soluciones en la nube, conexiones VPN para conectar de forma cifrada a la red de la organización, servicios de escritorio remoto virtual, uso de herramientas colaborativas, aplicaciones de videoconferencia, etcétera, ha generado un incremento de los ataques a estas tecnologías para acceder a las redes corporativas de organismos públicos y empresas.

Se están incrementando las vulnerabilidades detectadas sobre estas tecnologías porque diferentes actores se han centrado en la seguridad de estos dispositivos (véanse las vulnerabilidades detectadas en la tecnología Zoom o los ataques a servicios en nube) por su rentabilidad en el acceso a las redes corporativas. Lamentablemente estas tecnologías muchas veces no han sufrido los procesos de certificación que deberían ser exigibles a tecnologías tan críticas para la seguridad de las organizaciones.

Preocupan especialmente los actores de ciberespionaje por sus posibilidades en la detección de vulnerabilidades y de acceso a esta nueva arquitectura de redes que aumenta de manera tan drástica la superficie de exposición.

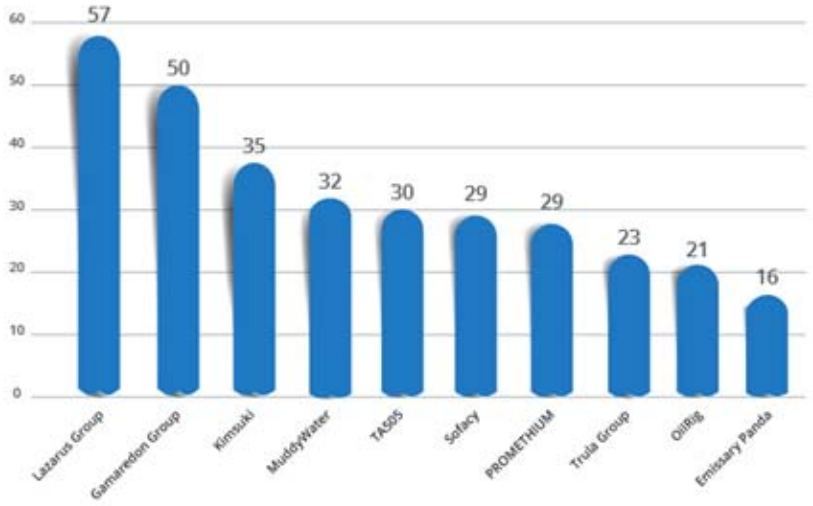


Figura 12. Ataques detectados por el CCN-CERT. Fuente: REYES, solución desarrollada por el CCN-CERT para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas. Disponible en: https://www.ccn-cert.cni.es/soluciones-seguridad/reyes.html.

Otro foco importante en el que se centrarán los atacantes es en las redes de control industrial (operacionales), que son las que controlan los procesos productivos. Son redes difíciles de actualizar y sin las medidas de ciberseguridad necesarias (copias de seguridad, herramientas de detección de *malware* o de gestión de incidentes). La interconexión entre estas redes y las redes corporativas es cada vez mayor y la pandemia de la COVID-19 ha generalizado el acceso remoto de los técnicos de mantenimiento. Se empieza a detectar *ransomware* con capacidad de cifrado sobre estas redes.

Respecto a sistemas IoT/control industrial se espera un crecimiento de los ataques en especial en el ámbito doméstico. Se debe tener en cuenta la variedad de dispositivos que muchas veces se utilizan como sistemas de climatización, seguridad física o de salud (análisis clínico, diagnostico por la imagen, soporte en quirófanos, distribución de gases medicinales…). Para no interrumpir la operación, las víctimas accederán al pago de rescates como ha ocurrido con la empresa de distribución de hidrocarburos Colonial (figura 14).


- Inicio del incidente: **07.05.2021**
- Fin del incidente: **14.05.2021**
- **Impacto:**
  - Interrupción de operación en oleoducto de 8.000 km. 45% combustible de la Costa Este
  - Temor a desabastecimiento en 50M personas
  - Pago rescate: 5.000.000 $
- **Grupo de Ataque:**
  - DARKSIDE

Figura 13. Datos sobre el ataque a la empresa de hidrocarburos Colonial.

Sobre los ataques de *ransomware* destaca el incremento de su sofisticación, automatización y la copia de las TTP de los ataques más complejos (*advanced persistent threats*, APT). Así, tras un reconocimiento inicial, se compromete a la víctima a través de sistemas vulnerables expuestos a internet y, una vez el atacante controla la infraestructura, persiste en ella y se mueve lateralmente adquiriendo y exfiltrando información. Se ha popularizado el empleo de la doble extorsión en las que además del secuestro de datos se amenaza con el filtrado de estos[31].

También se espera un incremento en las campañas de desinformación por su gran capacidad de desestabilización. El uso masivo de redes sociales o la enorme cantidad de información disponible acaba creando un efecto denominado infoxicación, multiplicando la efectividad de dichas operaciones. Cabe destacar el uso de tecnologías *deep fake* para ejecutar ataques de *phishing* mucho más sofisticados, simulando la voz de directivos o su forma de redactar.

Respecto a la inteligencia artificial (IA), su uso será determinante para optimizar los ciberataques. Un atacante puede lanzar *malware* que recoja información y determinar por qué un ataque no ha tenido éxito. Posteriormente podría utilizar esta información para lanzar un segundo ataque mejor adaptado. Esta tecnología, a pesar de ser avanzada, está disponible para los atacantes, tanto en herramientas comerciales como de *open source*.

[31] Ver https://www.welivesecurity.com/la-es/2020/12/04/tendencias-ciberseguridad-2021-que-esperar-proximo-ano/.

Por la parte defensiva, se utilizará la IA para gestionar toda la información de ciberseguridad de las redes y proporcionar una detección y respuesta eficiente. Esta nueva aproximación permitirá a los sistemas de seguridad aprender de los ciberataques detectados y generar nuevas TTP que ajusten los sistemas. Será de especial interés el uso de tecnologías como UEBA (*user entity behavior analytics*), en el que se monitoriza el comportamiento de los usuarios y los equipos dentro de una infraestructura.

No obstante, la IA todavía se encuentra lejos de sustituir al experto en ciberseguridad. Pero será de interés observar quién se adaptará mejor a esta tecnología, los atacantes o los defensores.

Del mismo modo, la presencia en la nube de una amplia mayoría de las empresas, especialmente tras este último año, va a suponer que muchas de ellas tengan que ampliar o mejorar las medidas adoptadas en materia de seguridad.

El aumento acusado del uso de las redes sociales, tanto en el ámbito privado como en el profesional, lleva a pensar que este puede convertirse en un vector de ataque creciente durante este año.

A medida que se popularizan los pagos móviles entre los usuarios, habrá un aumento en sus vulnerabilidades basadas en la recepción de un correo electrónico de *phishing*, un mensaje directo o un mensaje *smishing*[32], indicado al usuario que puede recibir un pago, un reembolso de la transacción o un premio en efectivo haciendo clic en una URL engañosa, siendo estafado para que envíe un pago desde su cuenta.

Los ataques de *phishing* ya sean correos electrónicos para toda la empresa, dirigido a un empleado (BEC) o, la más reciente, el ataque de *vishing* (*phishing* de voz), seguirán cada vez más presentes en 2021.

En este escenario, se espera que los costes asociados a los incidentes de ciberseguridad se incrementen en torno a un 15 % en 2021 y mantengan la tendencia ascendente, llegando a superar los 80 000 millones de euros a nivel global en 2025[33].

[32] Envío de un SMS simulando ser una entidad legítima.
[33] Ver https://cybersecurityventures.com/cybercrime-will-cost-the-world-16-4-billion-a-day-in-2021/.

**Tendencias de la ciberseguridad en los próximos años**

Para conformar una visión estratégica de la ciberseguridad y conocer las líneas que marcarán su desarrollo futuro, es necesario realizar una aproximación al sector sabiendo su impacto directo en la seguridad nacional, en la competitividad de las empresas y en la prosperidad de la sociedad en su conjunto. Diez son los aspectos claves que pueden dirigir el futuro en un sentido u otro (decálogo expuesto por el CCN en su informe *Aproximación española a la ciberseguridad*[34])

1. Estrategia Nacional de Ciberseguridad, donde se establece la visión, el alcance, los objetivos y las prioridades. En nuestro país, hasta la fecha se han publicado dos documentos, en 2013 y 2019 (véase nota 12).


Figura 14. Estrategias de ciberseguridad publicadas hasta la fecha en España.

2. Instauración de una estructura de gobierno clara que identifique e involucre a las partes interesadas: gobernanza.
3. Hacer un balance de las políticas, regulaciones y capacidades existentes: desarrollo reglamentario posibilista. Apoyo en un marco jurídico operativo y eficaz.
4. Incremento de la capacidad de prevención, detección y respuesta ante ciberamenazas, creando CSIRT de referencia y por sectores.

[34] *Aproximación española a la ciberseguridad*, CNI. Disponible en: https://www.ccn.cni.es/index.php/es/menu-ccn-es/aproximacion-espanola-a-la-ciberseguridad.

5. Desarrollo e implementación de sistemas de alerta temprana. Capacidad de detección y establecimiento de mecanismos de notificación de incidentes.
6. Incremento de la vigilancia, con un servicio de evaluación continua y cibervigilancia basado en centros de operaciones de ciberseguridad (SOC) que permitan conocer en cada momento la superficie de exposición ante una posible amenaza y así asignar los recursos de manera óptima y priorizada.
7. Fomento, desarrollo y mantenimiento de perfiles profesionales cualificados en todos los niveles (dirección, gestión, implantación y usuarios) para protegerse de las ciberamenazas. La búsqueda de talento se ha convertido en un elemento crítico.
8. Impulso de acciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial. Institucionalizar la cooperación entre los organismos públicos y la empresa privada como clave para construir comunidad.
9. Implementación de mecanismos confiables de intercambio de información entre organismos, públicos y privados, tanto de análisis de ciberamenazas como de notificación de ciberincidentes, para generar confianza.
10. Comunicación y sensibilización en ciberseguridad de toda la ciudadanía.

Los tres primeros aspectos conforman, sin duda, las bases de la ciberseguridad y su gobernanza. Así, la primera estrategia estableció el Consejo Nacional de Ciberseguridad (CNCS), mientras que en la de 2019 se creó el Foro Nacional de Ciberseguridad para incrementar la colaboración público-privada y se activó una comisión permanente para facilitar la coordinación y la respuesta ante incidentes. No obstante, la aplicación de ciberseguridad sigue sometida a los criterios de los diferentes departamentos ministeriales sin establecer unas prioridades centralizadas ni disponer de un presupuesto propio.

Sería necesario evolucionar el modelo de ciberseguridad definido para asemejarnos a países como el Reino Unido, Alemania o Francia, que han desarrollado centros nacionales de ciberseguridad que permiten una aplicación de la ciberseguridad mucho más eficiente.

Por otro lado, asociado a los fondos de recuperación se observa que se van a iniciar proyectos para complementar las siguientes líneas de acción establecidas en la ENCS:

- LA 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio.
- LA 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España.
- LA 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.
- LA 4. Impulsar la ciberseguridad de ciudadanos y empresas.
- LA 5. Potenciar la industria española de ciberseguridad y la generación y retención de talento, para el fortalecimiento de la autonomía digital.
- LA 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.
- LA 7. Desarrollar una cultura de ciberseguridad.

***Actores relevantes en ciberseguridad***

Para articular la respuesta efectiva a los ciberataques, la Unión Europea en la ya mencionada directiva NIS ha apostado por fortalecer las capacidades nacionales a través de los denominados CERT o CSIRT de referencia que faciliten una respuesta coordinada y eficiente a los ciberataques. Estos equipos pueden buscar ataques basados en indicadores de compromiso (IOC) en reglas definidas, con análisis del tráfico exterior y con un carácter muy general, abstrayéndose de las particularidades de cada organismo.

En España existen más de cincuenta CERT/CSIRT[35]. De ellos, y según el RDL 12/2018 que traspone la Directiva NIS, tres son CSIRT de referencia:

- CCN-CERT del Centro Nacional de Inteligencia (Ministerio de Defensa) o CERT gubernamental nacional que tiene responsabilidad para actuar ante ciberataques sufridos por los sistemas clasificados, sector público y empresas y organizaciones de sectores estratégicos para el país, en coordinación con el CNPIC[36].
- INCIBE-CERT del Ministerio de Asuntos Económicos y Transformación Digital para dar servicio al sector privado.

[35] Buena parte de ellos están integrados en el CSIRT.es (https://csirt.es/).
[36] Centro Nacional de Protección de Infraestructuras y Ciberseguridad.

- ESP DEF-CERT, del Mando Conjunto del Ciberespacio (Ministerio de Defensa) para dar servicio al propio ministerio y a empresas de interés en la defensa nacional.

Los tres CERT mencionados son instrumentos útiles para la coordinación nacional e internacional y un último recurso ante emergencias o crisis dando apoyo a las organizaciones con personal experto y herramientas específicas, pero no pueden resolver la gestión diaria de la ciberseguridad en las organizaciones.

Sin embargo, un SOC[37] tiene un ámbito de actuación más táctico, pues abarca la prevención, protección, detección, respuesta y la recuperación de los sistemas tras un ciberataque. El SOC recibe información del CERT, la complementa con la parte interna y detecta nuevas relaciones.

Por ello, los SOC se deben organizar como servicios de ciberseguridad horizontal para un conjunto de organizaciones a fin de concentrar los recursos económicos y el talento necesario. Un ejemplo de esto será el futuro Centro de Operaciones de Ciberseguridad de la AGE (COCS-AGE) que dará servicio a más de cien organismos entre ministerios, instituciones y agencias del Gobierno de España.

Por ello, desde los CSIRT de referencia se está impulsando la creación de una Red Nacional de SOC[38] (figura 18) basados en los siguientes principios de funcionamiento: cumplimiento, operación, superficie de exposición, detección y respuesta.

[37] CCN-STIC 401. SOC. *Security operation center*. Un centro de operaciones de seguridad (COS) es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en internet. Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos. Disponible en: https://www.ccn-cert.cni.es/guias/glosario-de-terminos-ccn-stic-401.html.

[38] Los diferentes SOC que articulan esta red nacional están definidos en el documento *Desarrollando la Red de SOC Nacionales. Aproximación del CCN-CERT*.


Figura 15. Red Nacional de SOC.

Todos estos SOC se coordinarán con los CSIRT de referencia a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, que está desarrollándose en estos momentos, y que viene definida en el artículo 11 del RD 43/2021[39] (figura 19).

***Herramientas necesarias para la prevención, detección y respuesta***

Para un funcionamiento eficaz, estos CERT y SOC deben disponer de herramientas en los siguientes campos:

- Prevención:
  - Medir la superficie de exposición implementando el concepto de auditoría continua.
  - Formación del personal especializado y de los usuarios de la organización.
  - Medir la posición de seguridad de la organización
  - Medir las configuraciones de seguridad aplicadas a las diferentes tecnologías.
  - Análisis y gestión de riesgos.
  - Vigilancia digital para detectar amenazas a la organización.
- Detección y respuesta:
  - Detección basada en patrones y anomalías.

[39] 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».

- Herramientas de *endpoint* (ver nota 21) que permitan la reacción rápida ante ataques (en especial de *ransomware*).
- Análisis forense de dispositivos.
- Análisis masivo de los registros proporcionados por las herramientas de seguridad.
- Intercambio de ciberincidentes a nivel interno y externo de la organización.
- Intercambio de ciberinteligencia y difusión de indicadores de compromiso y listas negras.
- Análisis estático y dinámico del código dañino.
- Automatización de la respuesta ante determinados escenarios de ataque.

**Conclusiones**

Este análisis ha puesto de manifiesto que la ciberseguridad sigue siendo uno de los pilares fundamentales para cualquier empresa, organismo o institución. Es un sector en constante crecimiento, con agentes de amenaza cada vez más preparados, capaces de orquestar ataques de un alto nivel de complejidad e impacto.

La pandemia de la COVID-19 no ha hecho sino acelerar la transformación digital que debe ir acompañada de las medidas de ciberseguridad necesarias, especialmente en momentos en los que somos más vulnerables. Por ello, hoy en día resulta crítico aprender las mejores formas de protegernos, tanto en el ámbito privado como en el empresarial.

Los ataques dirigidos a grandes corporaciones, a secciones gubernamentales, empresas públicas, proveedores, etcétera, han puesto de manifiesto la necesidad de una cooperación más estrecha entre los sectores público y privado, con el fin de atajar eficazmente el peligro que la COVID-19 supone para nuestra salud, también desde la perspectiva de la ciberseguridad.

Con una tendencia cada vez más al alza del cibercrimen y con un mundo tan cambiante, no cabe duda de que se avecinan grandes retos para los profesionales de la ciberseguridad que tienen que desplegar herramientas y organizar servicios de ciberseguridad horizontales de alta disponibilidad para responder a estas nuevas amenazas.

Si queremos una transformación digital plena y segura, esta debe ir acompañada de un componente de ciberseguridad que garantice que nuestra información y procesos críticos tienen la mejor protección posible y que seremos capaces de responder ante cualquier eventualidad.

### *Anexo I. Aproximación española a la ciberseguridad*

Tal y como se ha mencionado en capítulos anteriores, la ciberseguridad ha pasado a considerarse un asunto intrínseco a la seguridad nacional. El Centro Criptológico Nacional ha realizado una aproximación al desarrollo, implantación y mejora de un esquema general de ciberseguridad nacional, con el que se permita facilitar esta tarea. Partiendo del desarrollo realizado en España en los últimos veinte años, y con el caso concreto del CCN-CERT, se busca aportar un modelo de desarrollo para afrontar, a nivel nacional, los diferentes desafíos que emanan de la protección de la red de un país y, por extensión, de su Administración, empresas y ciudadanos (ver nota 36).

Los diez puntos fundamentales de este modelo se recogen en el capítulo 5 de este artículo y se resumen en la siguiente figura:


Figura 16. Pasos a dar para una implementación de ciberseguridad satisfactoria.

***Anexo II. Sobre el CCN-CERT***

El CCN-CERT es el CERT gubernamental/nacional que tiene por misión contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al sector público a afrontar de forma activa las nuevas ciberamenazas.

Tiene responsabilidad de actuar ante ciberataques sufridos por:

- Sistemas clasificados.
- Sistemas del sector público.
- Empresas y organizaciones de sectores estratégicos para el país en coordinación con el CNPIC.

Sus funciones y competencias se establecen en las leyes y reales decretos que se muestran en la siguiente figura (figura 17).

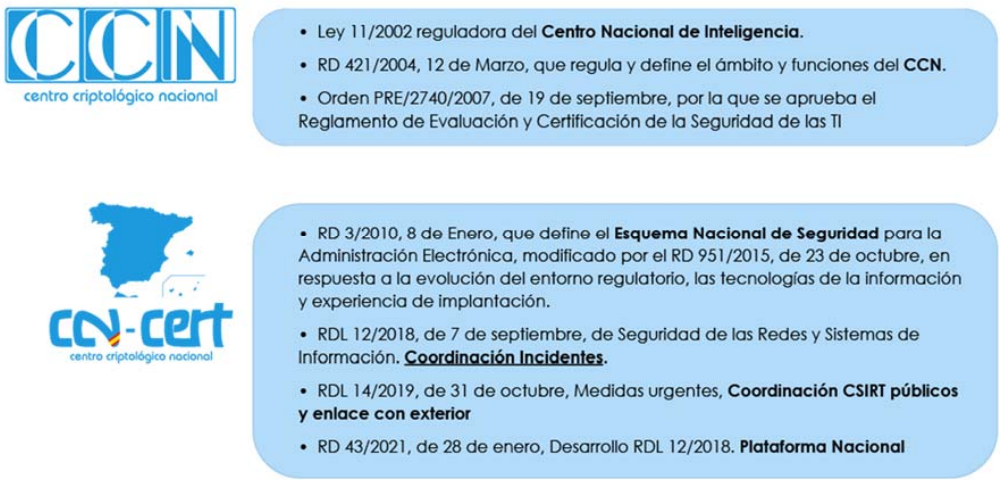


Figura 17. Normativa que fija las funciones y competencias del CCN y CCN-CERT.

Esta normativa se concreta en una serie de servicios de prevención, detección y respuesta destinados a reducir la superficie de exposición, mantener una vigilancia continua y alcanzar una respuesta eficiente e integrada (figura 18).


Figura 18. Servicios del CCN-CERT.

Asimismo, gracias a su experiencia de más de treinta años en ciberseguridad desarrolla soluciones con tecnología nacional que pone a disposición del sector público (figura 18.

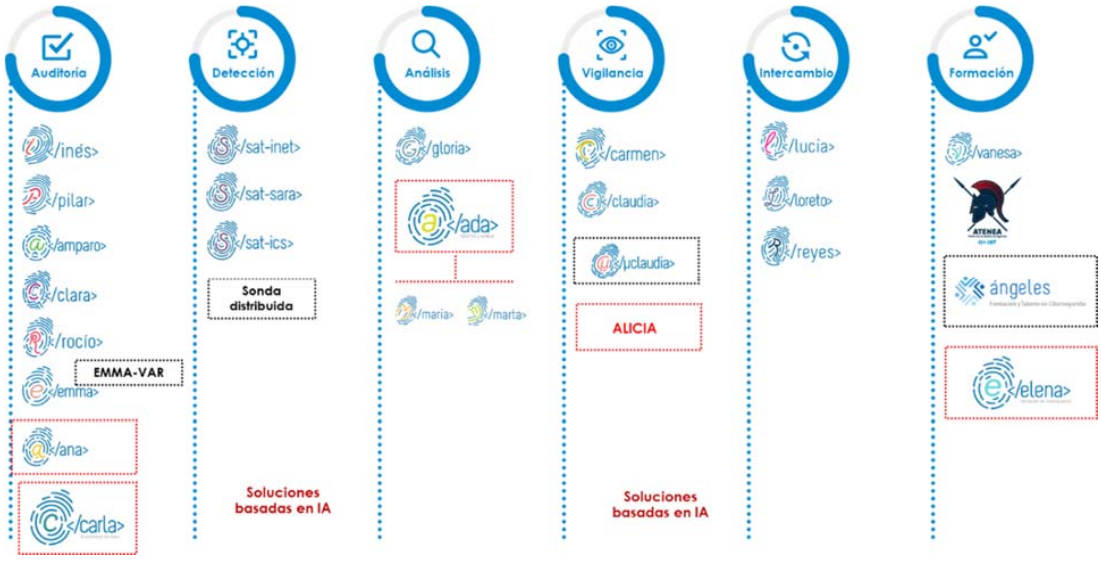


Figura 19. Soluciones desarrolladas por el CCN-CERT.

*Javier Candau**
Jefe del Departamento de Ciberseguridad
Centro Criptológico Nacional