La ciberseguridad

José Manuel Huidobro

Informe 2022

Publicación patrocinada por

CEDRO

ACTA representa en CEDRO los intereses de los autores científico-técnicos y académicos. Ser socio de ACTA es gratuito.

Solicite su adhesión en acta@acta.es

La ciberseguridad

CONTENIDO

INTRODUCCIÓN

Hoy en día es imposible no oír hablar de la ciberseguridad en Internet y de todas las formas en las que personas no autorizadas pueden acceder a nuestros datos bancarios, nuestros archivos personales o secuestrarnos un ordenador. La ciberseguridad en las empresas es igual de importante o incluso más que en el ámbito privado y es absolutamente necesario que los activos digitales críticos estén protegidos frente a las amenazas internas y externas.

Por regla general, las empresas e instituciones más grandes tienen más probabilidades de sufrir ciberataques y que sean de mayor gravedad. Sin embargo, ninguna empresa ni negocio que tenga presencia online y que emplee dispositivos tecnológicos está libre de estos ataques.

Se entiende por ciberseguridad aquellas estrategias y acciones que lleva a cabo una empresa o un particular para proteger y defender sus activos digitales de posibles ataques cibernéticos, como robo de información, acceso a nuestros sistemas y control de los dispositivos.

El pasado 30 de marzo se publicó en el BOE el Real Decreto-ley 7/2022, de 29 de marzo, que establece requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología 5G.

El texto completo se encuentra y puede descargarse en la página web del BOE: https://www.boe.es/boe/dias/2022/03/30/pdfs/BOE-A-2022-4973.pdf

Son objetivos del Real Decreto-ley:

- Impulsar una seguridad integral del ecosistema generado por la tecnología 5G.
- Reforzar la seguridad en la instalación y operación de las redes de comunicaciones electrónicas 5G y en la prestación de los servicios de comunicaciones móviles e inalámbricas que se apoyen en las redes 5G.
- Promover un mercado de suministradores en las redes y servicios de comunicaciones electrónicas 5G bastante diversificado a fin de garantizar la seguridad basada en razones técnicas, estratégicas y operativas y evitar, por dichas razones, la presencia de suministradores con una calificación de alto riesgo o de riesgo medio en determinados elementos de red o ámbitos. .
- Reforzar la protección de la seguridad nacional.
- Fortalecer la industria y fomentar las actividades de I+D+i nacionales en ciberseguridad relacionadas con la tecnología 5G.

Pero la seguridad no solo afecta a las redes móviles 5G, sino que va mucho más allá. En un sentido amplio protege sistemas, redes y programas de ataques digitales. Por lo general, los ciberataques apuntan a acceder, modificar o destruir la información confidencial, extorsionar a los usuarios o interrumpir la continuidad del negocio. Actualmente, la implementación de medidas de seguridad digital se debe a que, gracias a la proliferación y extensión de Internet y las redes móviles, hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos.

En el actual mundo conectado y global, todos se benefician de los programas de ciberdefensa avanzados. A nivel individual, un ataque a la ciberseguridad puede dar como resultado desde un robo de identidad hasta intentos de extorsión y la pérdida de datos importantes, como fotos familiares o los ficheros de nuestras obras en caso de los autores científico-técnicos y académicos. A nivel empresarial las consecuencias pueden ser muy graves, pues todos confiamos en las infraestructuras críticas, como las centrales eléctricas, los hospitales y las empresas de servicios financieros y proteger estas es esencial para el funcionamiento normal de la sociedad.

QUÉ ES LA CIBERSEGURIDAD

La ciberseguridad es la práctica de defender los ordenadores, servidores, dispositivos móviles, sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y se puede dividir en algunas categorías comunes.

- **La seguridad de red** es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.

- **La seguridad de las aplicaciones** se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

- **La seguridad de la información** protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en su tránsito a través de la red.

- **La seguridad operativa** incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- **La recuperación ante desastres y la continuidad del negocio** definen la forma en que una empresa/institución/organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.

- **La capacitación del usuario final** aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñar a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades de almacenamiento no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

Figura 1. La ciberseguridad y las redes.

EL ESTADO DE LA CIBERSEGURIDAD EN ESPAÑA

Según datos del Instituto Nacional de Ciberseguridad (INCIBE), entidad referente para el fortalecimiento de la ciberseguridad y el impulso del talento en torno a este sector, y ONTSI, a través de un informe elaborado para ObservaCiber, la brecha de talento en el área de ciberseguridad en España es superior a los 26.000 profesionales. Por su parte, LinkedIn ha detectado que la demanda de habilidades de ciberseguridad en Europa ha crecido un 22% en el último año.

Según Harvard-Deusto, en su documento "Ciberseguridad: Inteligencia artificial para garantizar la mejor defensa"

> "Hoy en día, la ciberseguridad ha pasado a ser una de las cuestiones corporativas más críticas, porque los incidentes que se generen en este nuevo mundo interconectado pueden afectar gravemente no solo al día a día de las compañías (riesgos operacionales), sino también a su reputación e imagen, a su visibilidad corporativa, y poner incluso en peligro su continuidad (riesgos estratégicos). Porque una ciberseguridad deficiente puede tener un impacto financiero muy negativo. De acuerdo con el informe Inteligencia artificial en el mercado de la ciberseguridad: pronóstico global hasta 2026, publicado por MarketsandMarkets, el sector de inteligencia artificial en ciberseguridad alcanzará los 38.200 millones de dólares en 2026, lo que representa un crecimiento medio anual del 23,3%. Los principales impulsores de este crecimiento serían la aparición de nuevas tecnologías disruptoras, el aumento de los casos de ciberamenazas, una mayor preocupación en torno a la protección de datos y unas redes Wi-Fi más vulnerables".

La creciente importancia que la digitalización ha alcanzado en el ámbito empresarial ha impactado directamente en las necesidades de ciberseguridad de las organizaciones, con independencia de su tipología. En este contexto, el 94% de las empresas ha sufrido al menos un incidente grave de ciberseguridad a lo largo de 2021, según se desprende del estudio Deloitte "El estado de la ciberseguridad en España", del que se hablará más tarde, en el que se ofrece una panorámica de la ciberseguridad en las organizaciones de nuestro país a través de las respuestas de los responsables de seguridad de la información de más de 100 empresas.

Por otra parte, muchos de los ciberataques, relacionados con el phishing, se producen como consecuencia de mensajes (SPAM) que todos recibimos a diario.

Según un reciente artículo publicado en la revista online zonamovilidad, acerca del SPAM: https://www.zonamovilidad.es/ataques-phishing-encuentran-nuevas-vias-ataque-obligando-personas-no-bajar-guardia

> "España lleva siete trimestres consecutivos posicionada como el primer país víctima de spam. Esto engloba todo el año 2020 y 2021".

Un estudio realizado por Kaspersky señala que España ha recibido el 9,55% del total mundial de este tipo de ataques a lo largo de los meses de julio, agosto y septiembre. Esta cifra refleja que el número de ataques ha incrementado medio punto porcentual respecto al segundo trimestre de 2021. Después de España se sitúa Rusia, con el 6,52% del total; Italia, con el 5,47%; Brasil, con el 5,37%; y México, con el 4,69% del total de los ataques mundiales.

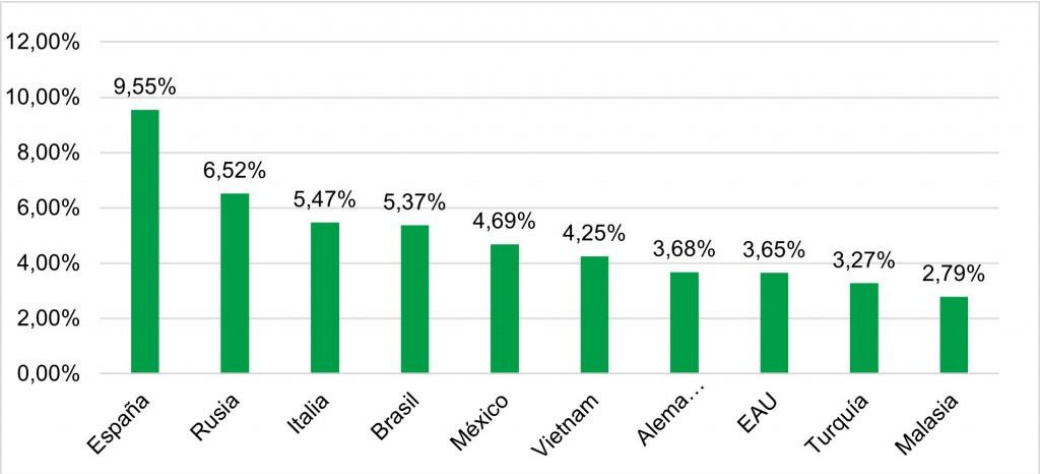


Figura 2. España es el país que más correos maliciosos recibe.

Por otro lado, si se hace un análisis sobre los países desde donde se envían más spam, Rusia se posiciona en la primera posición con un 24,9% del total, aunque este porcentaje es inferior al que se registró en el segundo trimestre de 2020. Por consiguiente, en el segundo puesto de la clasificación se encuentra Alemania con un 14,19% del total, China con un 10,31%, Estados Unidos con un 9,15% y Países Bajos con un 4,96%. Además, España ocupa la octava posición de esta clasificación con el 2,70% (hace años era muy superior) del spam saliente a nivel internacional.

Sin embargo, el porcentaje medio de spam en el tráfico general de email registrado durante este trimestre ha se reduce en un 1,09% en comparación con el periodo anterior, estableciéndose en el 45,47%. Agosto ha sido el mes que mayor porcentaje ha tenido, con un 45,84%.

Organismos de ciberseguridad en España

En los últimos años se han ido creando organismos que tienen por objetivo velar por la seguridad en el ciberespacio. Los principales existentes en España en materia de ciberseguridad, son:

Web: https://ciberseguridad.com/normativa/espana/organismos/

CNI. Centro Nacional de Inteligencia

El Centro Nacional de Inteligencia es el servicio de inteligencia de España, creado en 2002 como sucesor del antiguo Centro Superior de Información de la Defensa.

El CNI, adscrito al Ministerio de Defensa, tiene presencia en España y también fuera de nuestras fronteras, en aquellos Estados en los que nuestro país tiene intereses políticos, económicos o vinculados a la seguridad.

Las actividades del CNI, su organización y estructura interna, los medios y procedimientos, su personal, sus instalaciones, bases y centros de datos, las fuentes de información, así como las informaciones o datos que puedan conducir al conocimiento de las anteriores materias, constituyen información clasificada con el grado de secreto.

Figura 3. Logo del CNI.

La misión general asignada al CNI es la de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones. Esta misión se concreta en diversas funciones (art. 4 de la Ley 11/2002) que definen sus cometidos y ámbitos de actuación y que, anualmente, se detallan y desarrollan en la Directiva de Inteligencia.

Por otro lado los gobiernos utilizan en ocasiones a los Servicios de Inteligencia como un canal discreto de enlace y comunicación entre Estados cuando la vía diplomática habitual no existe o por la razón que sea no conviene utilizarla. Sitio web: https://www.cni.es/

INCIBE

El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Economía y Empresa de España, Secretaría de Estado de Progreso Digital, y es la institución de referencia en lo que respecta al desarrollo de la ciberseguridad y de la confianza digital para el público en general, para RedIRIS (la red académica y de investigación española), y para las empresas, especialmente los sectores de importancia estratégica.

Figura 4. INCIBE.

Como centro de excelencia, INCIBE es un servicio que ofrece el Gobierno español para trabajar por el desarrollo de la ciberseguridad como instrumento de transformación social y para el desarrollo de nuevos campos de innovación. Para ello, con sus actividades centradas en la investigación, la prestación de servicios y la cooperación con los actores relevantes, INCIBE lidera una serie de iniciativas dirigidas a la ciberseguridad tanto a nivel nacional como internacional.

En España el INCIBE trabaja en diversos aspectos de Ciberseguridad, y ofrece un servicio nacional, gratuito y confidencial que pone a disposición de los usuarios de Internet y la tecnología con el objetivo de ayudarles a resolver los problemas de ciberseguridad que puedan surgir en su día a día. Está dirigido a los ciudadanos (usuarios de Internet en general); empresas y profesionales que utilizan Internet y las nuevas tecnologías en el desempeño de su actividad y deben proteger sus activos y su negocio; y menores y su entorno (padres, educadores y profesionales que trabajen en el ámbito del menor o la protección online ligada a este público). Sitio web: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad

En el marco del Plan de Confianza en el Ámbito Digital (derivado de la Agenda Digital para España), INCIBE en colaboración con el ecosistema investigador en ciberseguridad español, ha liderado la creación de una Red de centros de excelencia I+D+i en ciberseguridad con el objetivo de aglutinar los esfuerzos de este ecosistema existentes en la actualidad y dirigir su actividad de forma coordinada a través de un futuro plan director alineado con la estrategia europea y las necesidades reales de la industria y los usuarios finales.

La Red de Excelencia se ha constituido formalmente como entidad jurídica el día 1 de julio de 2016, con el nombre de Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), inscrita en el Registro Nacional de Asociaciones del Ministerio del Interior. RENIC es una asociación sectorial que engloba centros de investigación, universidades y otros agentes del ecosistema investigador de ciberseguridad en España.

Figura 5. RENIC.

En España INCIBE gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020.

INCIBE
El Instituto Nacional de Ciberseguridad (INCIBE), a través de INCIBE-CERT (su Centro de Respuesta a Incidentes de Seguridad), gestionó 133.155 incidentes de ciberseguridad durante el año 2020, de los cuales 106.466 hacen referencia a ciudadanos y empresas, 1.190 a operadores estratégicos y 25.499 a la Red Académica y de Investigación española (RedIRIS). De esos incidentes, el 35,2% correspondía a malware y el 32% a cualquier tipo de fraude, seguido de sistemas vulnerables, con un 17,4%. Con el objetivo de incrementar la confianza digital de los ciudadanos y las empresas de España, INCIBE ofrece entre sus servicios la creación de contenidos de concienciación. Entre ellos destacan los avisos de seguridad, con la publicación en 2020 de 495, en los que facilitaba información de actualidad y utilidad para sus públicos objetivo. Cabe destacar que en los últimos años ha aumentado el nivel de prevención y anticipación de la sociedad a los problemas en temas de ciberseguridad.

CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio fue creado en 2006 como CERT del Gobierno de España. Sitio web: https://www.ccn-cert.cni.es/

El CCN-CERT es responsable de los ciberataques a sistemas y sistemas clasificados de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país (aquellas que son imprescindibles para la seguridad nacional y para el conjunto de la economía española).

Figura 6. Logo del CCN_CERT.

CETSE

El CETSE Constituye la sede de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS), como órgano de implementación de las funciones específicas de esta Subdirección y de las políticas de I+D+i del órgano Directivo, conforme a lo establecido en el Real Decreto 734/2020 de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

El CETSE, inaugurado el 20 de abril de 2016, se encuentra ubicado en la localidad de El Pardo (Madrid) y, además de la SGSICS, alberga al Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC). https://cetse.ses.mir.es/publico/cetse

CNPIC

El Centro Nacional de Protección de las Infraestructuras Críticas se ha creado dentro de la Secretaría de Estado de Seguridad para instrumentar las tareas encomendadas a ese Órgano Superior en la materia. Este Centro custodiará y actualizará el Plan de Seguridad de Infraestructuras Críticas y el Catalogo Nacional de Infraestructuras Críticas.

Figura 7. Logo del CNPIC.

Órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior.

Consejo Nacional de Ciberseguridad. DSN

Es un órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno. El Consejo Nacional de Ciberseguridad se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013.

El Consejo Nacional de Ciberseguridad reforzará las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores públicos y privados, y facilitará la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

Figura 8. Composición del Consejo de Ciberseguridad.

La composición del este Consejo reflejará el espectro de los ámbitos de los departamentos, organismos y agencias de las Administraciones Públicas con competencias en materia de ciberseguridad, para coordinar aquellas actuaciones que se deban abordar de forma conjunta con el fin de elevar los niveles de seguridad. En el Consejo podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria. En el cumplimiento de sus funciones el Consejo Nacional de Ciberseguridad será apoyado por el Departamento de Seguridad Nacional en su condición de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional.

Sitio web: https://www.dsn.gob.es/es/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad

Guardia Civil

Dentro de la Guardia Civil, a mediados de 2019, se creó la Unidad de Coordinación de Ciberseguridad. Es un órgano que, dentro de la Dirección General de la Guardia Civil, coordina y optimiza el potencial disponible para hacer frente a las amenazas procedentes de medios cibernéticos o transmitidas a través de ellos, y que se constituya como punto de referencia en aspectos relacionados con la ciberseguridad.

La unidad se crea bajo dependencia directa del Director Adjunto Operativo (DAO), el número dos de la Guardia Civil, por debajo del director general, del que dependen el Mando de Operaciones, la Secretaría de Cooperación Internacional, la Intervención Central de Armas y Explosivos, el Servicio de Asuntos Internos y la Unidad Especial de Intervención.

El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet o de las Tecnologías para su comisión. Su origen se remonta al año 1996, cuando se constituyó el Grupo de Delitos Informáticos (GDI) para atender a las pocas denuncias que había entonces por los llamados delitos informáticos.

Este grupo de trabajo integrado dentro de la Guardia Civil tiene como misión llevar a cabo todas aquellas investigaciones relacionadas con la delincuencia informática que le encomienden las Autoridades judiciales o que conozca por comunicaciones y denuncias de los ciudadanos. Su web: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

Figura 9. Grupo de Delitos Informáticos de la GC.

Policía Nacional

Según la Policía, el 15% de los delitos en España se cometen en la esfera de la ciberdelincuencia, que va en aumento, Dentro de la Policía Nacional, existe la Brigada Central de Investigación Tecnológica (BCIT) con la función de responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería, etc. Su Web: https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php

La Brigada Central de Investigación Tecnológica está encuadrada en la Unidad de Investigación Tecnológica (C.G.P.J), que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución del ciberdelito de ámbito nacional y transnacional. Actuará como Centro de Prevención y Respuesta E- Crime de la Policía Nacional.

Su misión consiste en obtener las pruebas, perseguir a los delincuentes y poner a unas y otros a disposición judicial. Sus herramientas son la formación continua de los investigadores, la colaboración de las más punteras instituciones públicas y privadas, la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana.

EMAD

El Estado Mayor de la Defensa, con rango de Secretaría de Estado, es el órgano que se ocupa de preparar la fuerza, promulgar la doctrina militar nacional y establecer la Fuerza Conjunta. Su organización actual está regulada por el Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas y por la Orden DEF 710/2020, de 28 de julio, que desarrolla la organización básica del Estado Mayor de la Defensa. Su web: https://www.defensa.gob.es/fuerzasarmadas/emad/

El Estado Mayor de la Defensa (EMAD), con sede en Madrid, es un órgano del Ministerio de Defensa de España que opera como auxiliar del Jefe del Estado Mayor de la Defensa (JEMAD) dentro de la estructura orgánica de las Fuerzas Armadas de España y en posición jerárquica militar de dependencia de aquel.

Bajo su dependencia está el Centro de Inteligencia de las Fuerzas Armadas (CIFAS) y multitud de órgano de asistencia, asesoramiento y auxilio, tales como Gabinetes, un equipo legal y diferentes unidades y jefaturas para el desarrollo de las competencias del JEMAD.

AEPD

La Agencia Española de Protección de Datos (AEPD) es la Autoridad Nacional de Protección de Datos de España. Es un organismo público independiente encargado de hacer cumplir el RGPD en España. Su sede social se encuentra en Madrid.

Es la autoridad de derecho público que vela por el cumplimiento de las disposiciones legales en materia de protección de datos de carácter personal, gozando como tal de absoluta independencia de la Administración Pública. Su web: https://www.aepd.es

A continuación se exponen unas recomendaciones que publicó CEDRO en su portal (24/07/2018) sobre la protección de datos. Se trata de un decálogo para aquellos autores o escritores que recogen datos de carácter personal para el desarrollo de su actividad. Incluye unas indicaciones para cumplir con el nuevo Reglamento General de Protección de Datos (RGPD). https://www.cedro.org/blog/articulo/blog.cedro.org/2018/07/24/10-consejos-sobre-proteccion-datos

10 CONSEJOS SOBRE PROTECCIÓN DE DATOS
1. Consentimiento inequívoco El consentimiento para el tratamiento de datos personales debe darse de forma afirmativa y explícita por parte del interesado. No es válido el consentimiento tácito o por omisión. **2. Base legitimadora** Todo tratamiento de datos debe apoyarse en una base que lo legitime. Por ejemplo, el consentimiento explícito del interesado o una relación contractual con él. **3. Responsable del tratamiento** En toda actividad que se gestionen datos personales tiene que haber un responsable de la protección de los mismos que garantice el cumplimiento de lo dispuesto en el RGPD. En algunos casos, también es necesario el nombramiento de un delegado que apoye las funciones del responsable.

4. Mantener informado al interesado

El responsable de protección de datos tiene que informar al contacto sobre las condiciones del tratamiento de sus datos y sus derechos. Todo ello, de una forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

5. Derechos

–Derecho de acceso para conocer de qué datos disponen y su uso.

–Derecho de rectificación, si la información es inexacta o incompleta.

–Derecho de oposición a que se traten sus datos.

–Derecho de supresión o derecho al olvido: eliminación de sus datos.

–Derecho a la limitación del tratamiento de los datos.

–Derecho a la portabilidad: capacidad para solicitar que sus datos se traspasen directamente de una organización a otra.

–Derecho a no ser objeto de decisiones individuales automatizadas.

6. Principio de responsabilidad proactiva

El responsable de la protección de datos también deberá realizar un análisis del riesgo del tratamiento de estos que va a llevar a cabo. En función de los resultados, tiene que decidir qué medidas de seguridad se deberán aplicar para cumplir con la normativa.

7. Registro de actividades

Hay que disponer de un registro interno de las actividades del tratamiento de datos, excepto en las organizaciones que tengan menos de 250 trabajadores y no traten datos sensibles o que entrañen un riesgo para los afectados.

8. Protección de datos concebida desde el diseño y por defecto

Es necesario tomar medidas desde el inicio del diseño del tratamiento de datos para cumplir con la normativa y, por defecto, solo se debe gestionar la información personal estrictamente necesaria.

9. Notificación de una vulneración

Se deberá notificar a la Agencia Española de Protección de Datos, en un plazo de 72 horas, cuando se produzca una violación de seguridad (destrucción, pérdida o alteración accidental o ilícita) de datos personales. En el caso de que esta violación sea de alto riesgo, se deberá informar también al interesado.

10. Evaluación de impacto

En aquellos tratamientos de datos que conlleven un alto riesgo, por ejemplo, la manipulación de información sensible a gran escala, se tendrá que realizar una evaluación de impacto.

BCSC (País Vasco)

Basque Cybersecurity Centre (BCSC), es la organización designada por el Gobierno Vasco para promover la ciberseguridad en Euskadi. Su misión es promover y desarrollar una cultura de ciberseguridad entre la sociedad vasca, dinamizar la actividad económica relacionada con la aplicación de la ciberseguridad y fortalecer el sector profesional.

Figura 10. Infografía. Fuente: BCSC.

El Basque Cybersecurity Centre asume dos grandes cometidos: convertir a Euskadi en un referente europeo en la aplicación de las nuevas tecnologías de la información y las comunicaciones, por una parte, y por otra, contribuir a dotar a las infraestructuras críticas y a las empresas vascas de una cobertura efectiva y fiable de prevención y reacción ante posibles amenazas y/o ataques. Su web: https://www.basquecybersecurity.eus/es/

Agencia de Ciberseguridad de Cataluña

La Agencia de Ciberseguretat de Catalunya es el organismo encargado de garantizar la protección, prevención y gobernanza en materia de ciberseguridad de la Generalitat de Cataluña y de su Gobierno. Su web: https://ciberseguretat.gencat.cat/es/inici/

Es la encargada de establecer el servicio público de ciberseguridad y trabaja para garantizar y aumentar el nivel de seguridad de las redes y los sistemas de información en Cataluña, así como la confianza digital de los ciudadanos. Además de la gobernanza de la ciberseguridad, en el ámbito de la Generalitat de Catalunya, la Agencia de Ciberseguridad de Cataluña Ciberseguridad lleva a cabo actividades de protección frente a ciberamenazas e incidentes de seguridad, prevención en el ámbito de la ciberseguridad desde el punto de vista organizativo, tecnológico y regulatorio, y la resiliencia de los activos e infraestructuras TIC como mecanismo para garantizar la robustez frente a los ciberataques.

CSIRT (Galicia)

El Centro de respuesta a incidentes de seguridad de la información de Galicia, CSIRT.gal, es un equipo de personal técnico especializado, dedicado a desarrollar medidas preventivas y reactivas con el objetivo de mitigar el impacto de los incidentes de seguridad en los sistemas de información de la Xunta de Galicia que son administrados por la Amtega.

El objetivo principal de CSIRT.gal es potenciar la seguridad y calidad de los servicios públicos prestados a través de los sistemas de información de la Xunta de Galicia, proporcionando capacidad de detección y respuesta eficaz y coordinada ante incidentes de ciberseguridad. Su web: https://amtega.xunta.gal/es/csirt

CENID (Alicante)

El Centro de Inteligencia Digital (CENID) es una iniciativa de la Diputación de Alicante, la Universidad de Alicante (UA) y la Universidad Miguel Hernández (UMH), para crear el principal referente de la provincia de Alicante en cuanto a desarrollo, investigación, divulgación y aplicación de estrategias y tecnologías habilitadoras digitales, todo ello al amparo de la experiencia y el conocimiento del personal investigador y científico de ambos centros universitarios.

Ofrece opinión y líneas de actuación, consultoría y asesoramiento digital en el acompañamiento a ayuntamientos, instituciones, administración, organismos, empresas, pymes, autónomos y profesionales en la transformación digital y en la implantación de la inteligencia artificial. Su web: https://cenid.es/

Oficina de seguridad del internauta (OSI)

La Oficina de Seguridad del Internauta (OSI), dependiente del INCIBE, proporciona la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

Su objetivo es reforzar la confianza en el ámbito digital a través de la formación en materia de ciberseguridad. Su web: https://www.osi.es

Internet segura for Kids

Estos días en casa todos hacemos más uso de Internet y de las nuevas tecnologías, también los más pequeños. Internet Segura for Kids (IS4K) es el Centro de Seguridad en Internet para menores de edad en España y tiene por objetivo la promoción del uso seguro y responsable de Internet y las nuevas tecnologías entre los niños y adolescentes.

Es un lugar de referencia para aprender a hacer un buen uso de Internet y transmitir ese aprendizaje a los más pequeños. Ya sea desde una perspectiva familiar o escolar, nuestro papel a la hora de enseñar a los menores cómo utilizar las nuevas tecnologías y afrontar sus riesgos es fundamental. Su web: https://www.is4k.es/

Figura 11. Algunos consejos para niños.

Centro Nacional de Excelencia en Ciberseguridad

El Centro Nacional de Excelencia en Ciberseguridad (CNEC) es un centro dependiente del ICFS de la UAM (en colaboración con la EPS) dedicado a la formación, entrenamiento, investigación y desarrollo tecnológico de excelencia en materia de ciberseguridad y ciberinteligencia para el incremento de la eficacia de la lucha contra la criminalidad

Una de las máximas prioridades del Centro es la creación y desarrollo de tecnología que permita una lucha más eficaz contra la creciente cibercriminalidad. Su web: https://www.icfs-uam.es/home-v10-magazine/cnec/

Centro de Seguridad TIC de la Comunidad Valenciana

Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico. Actualmente CSIRT-CV está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Consellería de Hacienda y Modelo Económico. Su web: https://www.csirtcv.gva.es/

CSIRT-CV ofrece servicios dentro de la Comunitat Valenciana, con vocación de servicio público, sin ánimo de lucro, por lo que sus servicios se ofrecen gratuitamente.

Su principal objetivo es contribuir a la mejora de la seguridad de los sistemas de información dentro de su ámbito, así como promover una cultura de seguridad y buenas prácticas en el uso de las nuevas tecnologías de forma que se minimicen los incidentes de seguridad y permita afrontar de forma activa las nuevas amenazas que pudieran surgir.

Centro de Ciberseguridad de Andalucía

El Centro de Ciberseguridad de Andalucía dependerá de la Agencia Digital de Andalucía (ADA), coordinará y pondrá en marcha la Estrategia Andaluza de Ciberseguridad 2022-2025. Sitio web: https://www.juntadeandalucia.es/organismos/ada.html

ADA, con sede en Málaga, es un ente instrumental que debe trazar la estrategia de por dónde debe ir el futuro de la digitalización, con el principal reto de eliminar la brecha digital. También deberá servir para avanzar en la administración electrónica de la Junta. Se trata de integrar todos los servicios tecnológicos de la Junta y unificar bajo un único paraguas a todos los funcionarios que diseminados en los muy diversos departamentos que posee trabajan en con lo digital como principal cometido.

La ADA es el medio más eficaz para eliminar la brecha digital, apostar por la administración digital y agilizar los procesos en las relaciones con los ciudadanos en las instituciones.

Este centro mejorará la resiliencia del tejido empresarial a través de un catálogo de servicios específicos que se diseñarán junto con el propio sector, y reforzará las capacidades de prevención, detección y respuesta a incidentes de seguridad en la Administración andaluza a través de la puesta en marcha de un conjunto de servicios avanzados de ciberseguridad.

INFORME DELOITTE 2022

En este año 2022 la empresa de consultoría Deloitte ha publicado su informe "El estado de la ciberseguridad en España. Post pandemia: un camino inexplorado", en el que destaca que el 94% de las empresas españolas ha sufrido, al menos, un incidente grave de ciberseguridad en 2021. Accesible en: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

La creciente importancia que la digitalización ha alcanzado en el ámbito empresarial ha impactado directamente en las necesidades de ciberseguridad de las organizaciones, con independencia de su tipología. En este contexto, el 94% de las empresas ha sufrido al menos un incidente grave de ciberseguridad a lo largo de 2021, según se desprende de nuestro estudio en el que se ofrece una panorámica de la ciberseguridad en las organizaciones de nuestro país a través de las respuestas de los responsables de seguridad de la información de más de 100 empresas.

En el informe, las principales conclusiones se exponen a continuación:

Incidentes de seguridad

En el último año se ha experimentado un más que notable aumento del número de ciberataques y sofisticación de las amenazas conocidas. En este sentido, casi el 69% de las empresas afirma que ha sufrido entre 1 y 2 ciberincidentes de gravedad durante este último año, agravándose la situación para el 25% de las empresas que afirma haber sufrido más de 2 ciberataques en 2021.

Además, según la comparativa del año 2020 con respecto a este último año, se observa cómo el número de empresas que ha recibido 1 o 2 ataques se ha reducido. En cambio, las empresas que han sufrido al menos un ciberincidente han aumentado casi un 7%. Es un dato significativo y que tiene su explicación en el hecho de que tras las medidas de teletrabajo masivo fruto de la pandemia, los ciberatacantes intensificaron sus ofensivas, siendo al mismo tiempo la superficie de ataque expuesta en la red mayor para estos.

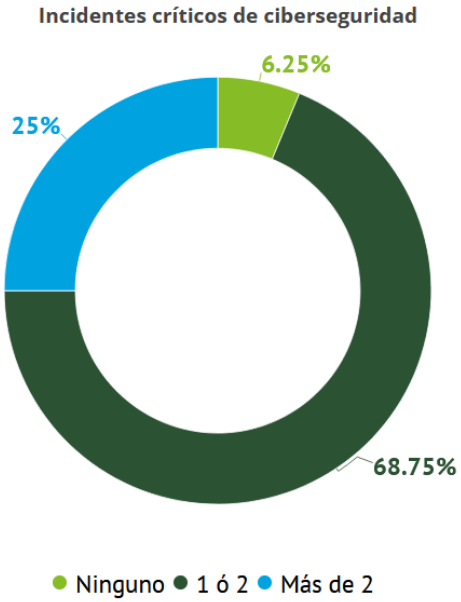


Figura 12. Incidentes de seguridad. Fuente: Deloitte.

La media de incidentes entre 2020 y 2021 ha aumentado considerablemente, de 1,69 incidentes de media en 2020, a 2,13 incidentes este último año; es decir, un 26% más de ciberincidentes.

Incidentes por sector

Hay varios sectores que se encuentran por encima de los dos incidentes de media al año. Entre estos, se encuentran el sector de Seguros, TMT (Telecomunicaciones, Medios de comunicación y Tecnología), Fabricación, Banca y Administración Pública. Cabe destacar que ciertos sectores como el de la banca y seguros se encuentran fuertemente regulados y cuentan con nivel de madurez en ciberseguridad razonablemente elevado, motivo por el cual el número de incidentes que sufren se debe más a que son un objetivo prioritario para los cibercriminales, más que al hecho de una falta de ciberresiliencia por su parte.

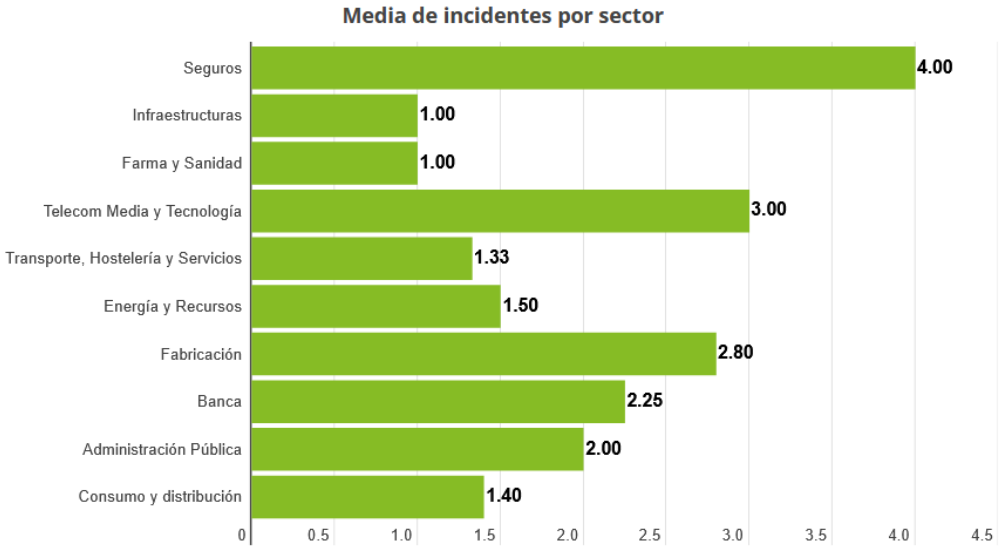


Figura 13. Media de incidentes por sector. Fuente: Deloitte

Además. el metaverso y la Web3, incluidos los NFT, los contratos inteligentes, las DAO y las criptomonedas, seguirán evolucionando de maneras nuevas y emocionantes, lo que planteará problemas novedosos y fascinantes de privacidad, seguridad, responsabilidad e propiedad intelectual, entre otros.

Amenazas más habituales

Las máximas preocupaciones entre los CISO a nivel general son el malware, el phishing y el ransomware. Cada vez son más los ataques de ransomware que sufren las empresas y la sofisticación de estos como, por ejemplo, el ransomware de triple extorsión.

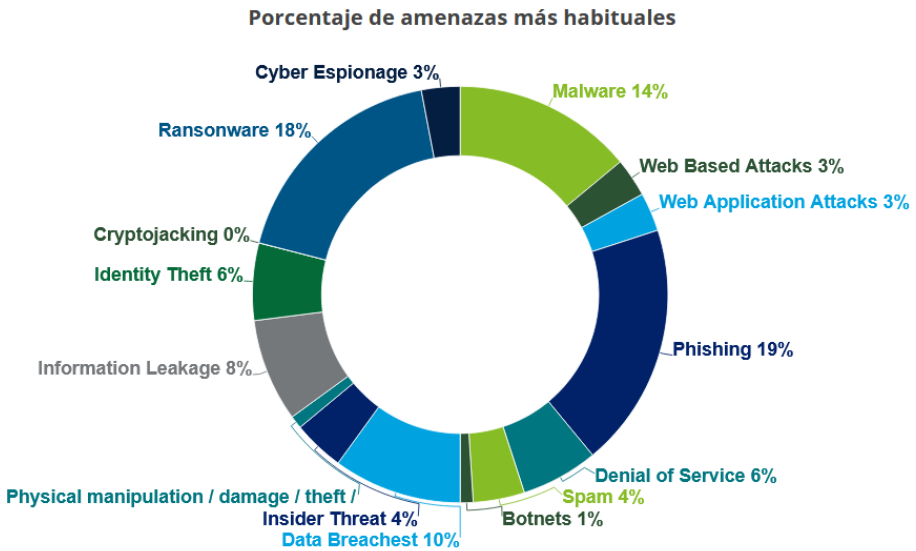


Figura 14. Amenazas más habituales. Fuente: Deloitte

El caso del phishing también es bastante preocupante, por este motivo, el entrenamiento de los empleados en la identificación y reporte del phishing es crucial. Muchas de las amenazas pueden combinarse en un mismo ataque, donde destaca el phishing, que es el vector de entrada por el que se decantan mayoritariamente los atacantes.

GOBERNANZA DE LA CIBERSEGURIDAD. 2022

Recientemente, el CCN-CERT, del Centro Criptológico Nacional (CCN), ha publicado en su portal el informe "Aproximación al marco de gobernanza de la ciberseguridad". En este documento se abordan las ciberamenazas, salvaguardas, el marco de gobernanza de la ciberseguridad, su estructura organizativa y cómo abordar la gestión de crisis.

El informe puede descargarse, en formato PDF, en el siguiente enlace: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6431-aproximacio-n-al-marco-de-gobernanza-de-la-ciberseguridad/file.html

A lo largo de 47 páginas, se detallan los elementos clave para establecer el marco de gobernanza de la ciberseguridad. Cabe recordar que la gestión de la ciberseguridad requiere de un marco de gobernanza en el que se designen a los organismos o unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización.

Figura 15. Informe Marco de Gobernanza de Internet.

En él se propone un modelo básico de referencia para la gobernanza según las siguientes premisas:

a) identifica una estructura organizativa de las unidades que prestan los diferentes servicios de ciberseguridad;

b) integra los procesos de gestión para la gobernanza de la ciberseguridad, con especial énfasis en los servicios de prevención proactiva y

c) identifica los servicios proveídos por la cadena de suministro TIC, así como los requisitos de cumplimiento exigibles a los suministradores.

En el marco de gobernanza, el comité de seguridad TIC se constituye como órgano especializado y permanente y está integrado por personas con responsabilidad en la toma de decisiones. Dentro de la estructura de seguridad, se constituirá una unidad denominada Oficina de gobernanza y cumplimiento normativo de la seguridad TIC, cuyas competencias incluirán la coordinación de los diferentes actores de seguridad de los órganos concernidos y el Centro de Operaciones de Seguridad. También puede ser conveniente la constitución de un Órgano de Auditoría Técnica (OAT) independiente, para la realización de auditorías de conformidad de los sistemas.

Por último, el capítulo 6 ofrece un análisis detallado de la gestión de ciberincidentes, con la creación del comité de crisis, su activación, funciones, composición, dinámica de las reuniones, así como un apartado dedicado a las buenas prácticas en la gestión de crisis

INFORME ESCUDOS 2021

No solo las grandes empresas y los usuarios particulares se ven afectados por los ciberataques, sino que también las pyme, de las que hay casi tres millones en España, son víctimas de los ciberdelincuentes.

Según concluye el informe Escudos 2021, promovido por la agencia española Exsel (https://exseluwa.com), promotora del Escudo Ciber, más de 300.000 pymes (un 10% del total) han sufrido ataques informáticos en 2021, la mayoría por fallos humanos, un 70% más que en todo 2020 y más del doble que antes de la pandemia, siendo la principal vulnerabilidad la relacionada con ingeniería social (fallos humanos inducidos por los ciberdelincuentes).

Una de cada cinco pequeñas y medianas empresas españolas ha sufrido algún ciberataque en el último año, siendo los ataques más habituales los fraudes en Internet, que se han convertido ya en el segundo delito más común en España, adelantando a robos con fuerza en domicilios, y suponen el 90% de los ataques que reciben en las empresas.

La ingeniería social, responsable directa o indirectamente del 95% de los ciberataques, ha repuntado tanto en volumen de ataques el último año (que se ha multiplicado por 8), como en efectividad (incrementado en más de un 40%), derivado de las circunstancias especiales del confinamiento (miedo, falsa confianza) y su impacto en la extensión del teletrabajo, unido al aprovechamiento de la coyuntura por los cibercriminales (noticias falsas, comunicaciones oficiales o invitaciones falsas a reuniones virtuales, por ejemplo, a través de Zoom o Teams).

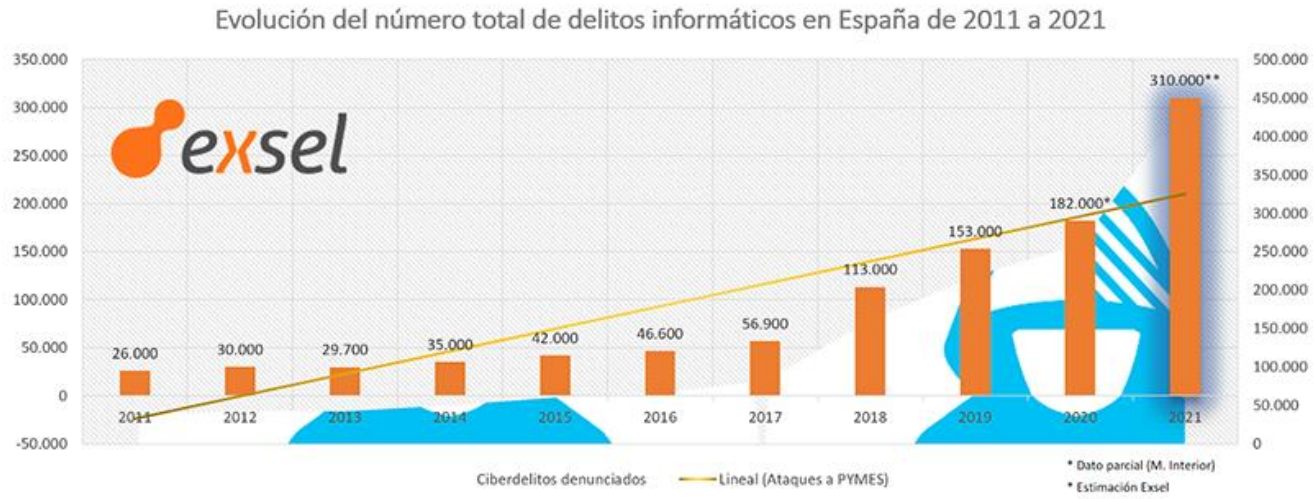


Figura 16. Evolución de delitos informáticos.

La pandemia del Covid disparó en un 2.000% el número de ciberamenazas –entre ellas un incremento del 95,2% en los incidentes de ramsomware–, ya que la extensión precipitada y falta de formación a empleados y medidas suficientes en ciberseguridad del teletrabajo ha proporcionado nuevas oportunidades que los atacantes comenzaron a aprovechar rápidamente y seguirán haciéndolo durante el mayor tiempo posible, por lo que es muy importante extremas las medidas de precaución, invirtiendo en equipos y software de confianza y actualizado.

Estos riesgos (Ciber Riesgos), al igual que otros, pueden ser objeto de asegurarse frente a ellos, algo que suele ser desconocido por la mayoría de usuarios, existiendo empresas para ello.

ÍNDICE GLOBAL DE CYBERSEGURIDAD 2020

El IGC (Índice Global de Ciberseguridad) es un índice compuesto para medir el compromiso de los Estados Miembros de la UIT con la ciberseguridad. Según el IGC-2020 publicado por la UIT (Unión Internacional de Telecomunicaciones), España figura en 4º puesto a nivel mundial en el IGC, situándose sólo por detrás de EE.UU., Reino Unido, Arabia Saudí y Estonia, y empatada con Corea del Sur y Singapur.

A nivel de Europa, España se sitúa en tercer lugar, sólo superada por Reino Unido y Estonia; segundo lugar, por tanto, en la Unión Europea.

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15
Netherlands**	97.05	16
Norway**	96.89	17
Mauritius	96.89	17
Brazil	96.6	18
Belgium	96.25	19
Italy	96.13	20
Oman	96.04	21
Finland	95.78	22
Egypt	95.48	23

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43
Thailand	86.5	44
Tunisia	86.23	45
Ireland	85.86	46
Nigeria	84.76	47
New Zealand**	84.04	48
Malta	83.65	49
Morocco	82.41	50
Kenya	81.7	51
Mexico	81.68	52
Bangladesh	81.27	53

Figura 17. Índice Global de Ciberseguridad.

El GCI maneja cinco pilares respaldados por la Agenda Global de Ciberseguridad (*Global Cybersecurity Agenda* - GCA):

- Legal: existencia de un marco legal relativo a la ciberseguridad y el ciberdelito.
- Técnico: existencia de un marco de medidas técnicas para afrontar el desarrollo de la ciberseguridad a nivel nacional.
- Organizativo: existencia de un marco organizativo para afrontar la ciberseguridad a nivel nacional. Incluye estructuras de organización y gobernanza para la ciberseguridad.
- Creación de capacidades: existencia de programas de investigación y desarrollo, educación y capacitación, profesionales certificados y de entidades del sector público que los fomentan.
- Cooperación: existencia de asociaciones, marcos de cooperación y redes de intercambio de información.

CIBERAMENAZAS EN EL MUNDO

Recientemente, 4 de abril de 2022, la empresa Avast ha presentado su Informe Global de Riesgos para PC. Accesible en línea: https://press.avast.com/es-es/2021-avast-global-pc-risk-report

Analiza las amenazas online que los usuarios domésticos y empresariales de Windows encontraron en durante el año pasado. De media, los usuarios domésticos de todo el mundo tuvieron un 29,25% de posibilidades de encontrarse con una amenaza, y en España este porcentaje se quedó en el 28,9%. Además, los usuarios empresariales españoles ocuparon el puesto 43 de los 77 países incluidos en el estudio. De media, los usuarios empresariales de todo el mundo tuvieron un 15,1% de posibilidades de encontrarse con una amenaza, y en España, la media fue de 21,9%.

Una de las conclusiones del informe es que los países con mayor ratio de riesgo son los que se encuentran en situaciones sociopolíticas más inestables (Oriente Medio, Asia, África y Europa del Este). El motivo de este mayor ratio de riesgo podría deberse al hecho de que estos usuarios tienen un acceso limitado a los contenidos, lo que les obliga a recurrir a canales no seguros para acceder a contenidos bloqueados. Además, la infraestructura digital de estos países tiende a tener niveles más bajos de seguridad. Otro hecho que puede explicar los resultados de los ratios es que estas regiones se caracterizan por un menor nivel de educación en cuanto a las mejores prácticas de ciberseguridad entre los usuarios de ordenadores. En cuanto a los principales tipos de malware a los que se enfrentaron los consumidores globalmente en 2021 son: troyanos (30,7%), infectadores de archivos (24,1%), adware (12,7%), gusanos (7,8%) droppers (6,9%), password (4,0%), minería de monedas (2,4%), RATs (2,3%), spyware (2,3%) y bots (1,7%).

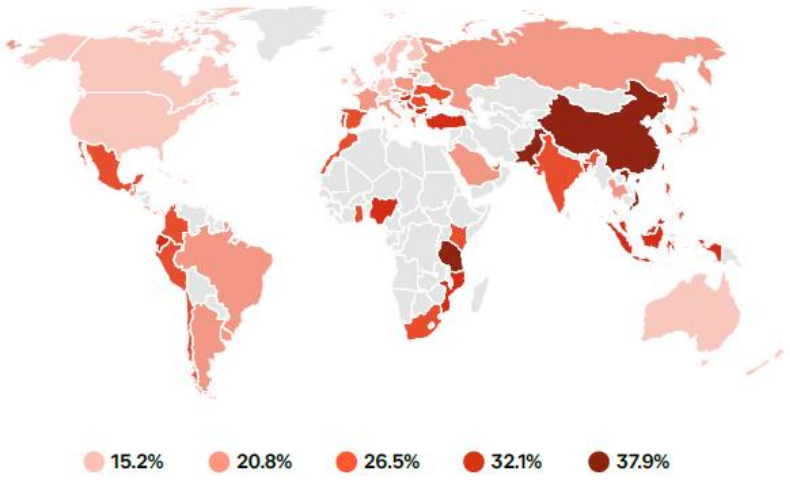


Figura 18. Ratio de riesgo para usuarios de negocios.

Aunque los ataques de ransomware persistieron en 2021, el ransomware no pertenece a las principales amenazas digitales a las que se enfrentan los usuarios domésticos. El ransomware es solo la punta del iceberg de las amenazas generales a las que se enfrentan, tanto los usuarios domésticos como las empresas en todo el mundo. Sin embargo, si el ransomware ataca, puede causar un daño significativo, por lo que se discute y se teme tanto, a pesar de su relativamente baja participación general entre las amenazas."

Las amenazas digitales ponen en juego la productividad, los beneficios y la reputación de las empresas. Un ataque puede costar a una empresa la rentabilidad, la productividad o la totalidad del negocio, dependiendo de la gravedad. Hemos observado un descenso en los ataques de ransomware a finales del año 2021 como resultado de la cooperación coordinada de naciones, agencias gubernamentales y proveedores de seguridad para hacer frente a las bandas de ransomware. Por desgracia, la guerra en Ucrania podría extenderse al mundo cibernético, como hemos visto en el pasado, y las empresas de todo el mundo podrían verse afectadas".

Los países donde los usuarios empresariales tienen más riesgo de encontrarse con amenazas siguen el siguiente orden: Vietnam (37,8%), China (35,6%), Tanzania (35,3%), Pakistán (35,6%), Croacia (32,5%), Bulgaria (31,6), Mozambique (30,5%), Indonesia (30,3%), Bangladesh (30.1%) y Taiwán (29,8%). Por otro lado, los diez países con menor riesgo de sufrir amenazas son: Suecia (9,5%), Noruega (10,8%), Luxemburgo (11,2%), Irlanda (11,5%), Reino Unido (11,7%), Alemania (11,8%), Puerto Rico (11,8%), Países Bajos (11,8%), Suiza (12,0%) y Estados Unidos (12,6%).

COUNTRIES MOST AT RISK

The ten countries in which businesses are most at risk of encountering a threat are:

1.	Vietnam	37.80%
2.	China	35.65%
3.	Tanzania	35.29%
4.	Pakistan	35.61%
5.	Croatia	32.55%
6.	Bulgaria	31.64%
7.	Mozambique	30.54%
8.	Indonesia	30.29%
9.	Bangladesh	30.07%
10.	Taiwan	29.78%

COUNTRIES LEAST AT RISK

The ten countries with the lowest risk ratio are:

1.	Sweden	9.52%
2.	Norway	10.86%
3.	Luxembourg	11.24%
4.	Ireland	11.52%
5.	United Kingdom	11.71%
6.	Germany	11.83%
7.	Puerto Rico	11.86%
8.	Netherlands	11.86%
9.	Switzerland	12.00%
10.	United States	12.60%

Figura 19. Ranking de países con riego más elevado y mínimo.

Los usuarios particulares se enfrentan a muchas amenazas a diario y es fácil que se descuiden en cualquier momento y sean víctimas de una estafa o daños en su sistema informático si no disponen de un buen sistema de protección, como es Norton 360, utilizado por el autor de este texto durante más de 10 años. Finalmente, los empresarios corren menos riesgo que los usuarios domésticos de encontrarse con amenazas, ya que, normalmente tienen capas de protección establecidas, y sus redes y dispositivos suelen estar gestionados por profesionales de la seguridad informática, lo que evita que se encuentren con amenazas de entrada.

PRINCIPALES CIBERAMENAZAS DE 2022

Según Avansis, una empresa especialista en servicios IT, ciberseguridad, innovación y outsourcing para empresas, 2020 y 2021 fueron años muy negros para la ciberseguridad. Estos dos años se ha presenciado un aumento importante de ciberataques a nivel mundial. Este aumento de ataques está directamente relacionado con la pandemia del Vovid-19 y por esta razón las empresas, las organizaciones y los países se están rearmando día a día para poder protegerse de las diferentes ciberamenazas que puedan aparecer en cualquier momento.

Las principales ciberamenazas a las que se pueden enfrentar los usuarios, las organizaciones, los países o las empresas son principalmente 6:

1. Guerra Fría 2.0

La guerra híbrida se ha transformado en una guerra cibernética. En los últimos tiempos, los ciberataques han sido orquestados desde algunos gobiernos para atacar políticamente a gobiernos del otro bloque. Rusia, Irán, Estados Unidos o Israel han sido acusados durante estos dos últimos años de llevar a cabo multitud de ataques de todo tipo hacia plataformas gubernamentales, por lo que se les define como una de las grandes ciberamenazas del 2022.

2. Brechas de seguridad

Las brechas de seguridad pueden suponer un gran problema para las empresas y organizaciones, así como para los usuarios. Los ciberdelincuentes se aprovechan de cualquier brecha o debilidad para atacar. Las compañías tendrán que repensar su estrategia en ciberseguridad y asegurar bien sus defensas. El daño que pueden causar estos ciberataques puede ser importante y complicado de solucionar.

3. Fake News

El incremento de las noticias falsas es más que evidente en los últimos tiempos. Las redes sociales se han convertido en su medio favorito para darse a conocer y así, crear ciberamenazas. Las fake news pueden causar un daño enorme a empresas, ciudadanos y países. En época de pandemia han experimentado un crecimiento preocupante que ya se está traduciendo en una proliferación de bulos y noticias falsas.

4. Ataques a criptomonedas y NFT

El auge de las criptomonedas en los últimos años se ha extendido rápidamente y esta circunstancia ha aumentado el número de casos de criptomonedas robadas o estafas. Al convertirse en un producto tan popular ha llamado la atención de los ciberdelincuentes.

El auge de los tokens no fungibles (NFT) también ha provocado algunos incidentes de seguridad graves. Para participar en un mercado de NFT, hay que tener una billetera de criptomonedas activa y esto expone a los titulares de NFT a nuevos riesgos, ya que los atacantes pueden encontrar formas de ingresar a su billetera criptográfica a través de su cuenta de mercado.

5. Teletrabajo

El teletrabajo ha supuesto un aumento importante de ciberataques a los sistemas de los trabajadores que ponen en peligro datos de las empresas. Estos ataques se producen en los dispositivos móviles de empresa o en los equipos de trabajo, con el principal objetivo de robar datos privilegiados de la empresa, acceder a sus cuentas y vender estas credenciales privilegiadas.

La mayoría de las empresas actualmente utilizan una VPN (*Virtual Private Network*) e infraestructura de escritorio virtual (VDI) para conectar a los trabajadores remotos. No obstante, estas soluciones pueden tener problemas de seguridad. Así, la mayoría de las VPN están configuradas para proporcionar acceso de todo o nada y aunque los administradores pueden restringir aplicaciones o activos confidenciales para ciertos usuarios es una tarea compleja de hacer.

6. Herramientas de defensa para ejecutar ataques

Esta es considerada una de las peores ciberamenazas, puesto que las herramientas de defensa están pensadas para proteger a las empresas, pero los ciberdelincuentes han dado con la manera de atacar estos sistemas. Su forma de actuar se basa en personalizar herramientas claves de estas aplicaciones a su gusto y ejecutarlas con ataques de ransomware.

LA EXTENSIÓN DE LAS CIBERAMENAZAS

Las ciberamenazas mundiales siguen desarrollándose a un ritmo rápido, con una cantidad cada vez mayor de filtraciones de datos cada año. Los servicios médicos, los minoristas y las entidades públicas fueron los que sufrieron más filtraciones, y los delincuentes maliciosos fueron los responsables de la mayoría de los incidentes. Algunos de estos sectores son más atractivos para los cibercriminales, ya que recopilan datos financieros y médicos, aunque todas las empresas que utilizan las redes pueden ser atacadas para robarles datos de clientes, hacer espionaje corporativo o lanzar ataques a sus clientes. La tendencia es que los ataques a grandes empresas disminuyen para dejar paso a un mayor número de ataques a pymes y ciudadanos.

Figura 20. Robo de datos.

Ciertos sectores vitales, como el transporte, la energía, la sanidad y las finanzas, dependen cada vez más de las tecnologías digitales para sus actividades esenciales. La digitalización, que brinda enormes oportunidades y ofrece soluciones para muchos de los retos a los que se enfrenta Europa, como se ha demostrado en particular durante la crisis de la COVID-19, también expone a la economía y a la sociedad a ciberamenazas.

TIPOLOGÍA

• **Ataques menos dirigidos y más masivos**: se lanzan a discreción sobre muchas víctimas potenciales y son poco complejos técnicamente. Un ejemplo: la distribución de correos con spam entre pymes para infectar cualquier dispositivo mal protegido o el llamado fraude del CEO, los atacantes se hacen pasar por el CEO de una empresas y escriben al departamento financiero solicitando una transferencia para realizar una compra. Son muy numerosas las pequeñas empresas que han perdido dinero con estos tipos de ataques.

• **Ataques profesionalizados**: tienen un componente muy especializado y con un objetivo muy definido. Los ataques más casuales, simplemente movidos por la curiosidad técnica de los hackers ya no se dan, siempre te atacan para conseguir algo, ya sea con un objetivo económico, o simplemente porque pueden utilizar nuestro email para usarlo en nuevos ataques.

• **Ataques que requieren de intervención humana**: se aprovechan de la falta de concienciación de usuarios y empleados (especialmente dañinos para pymes, que suelen contar con protocolos de protección menos avanzados y un bajo nivel de sensibilización entre su personal); alguien que haga clic en un enlace malicioso, pinche un adjunto que no debe abrir, de una información por teléfono que no debe dar.

Los ciberdelincuentes se enfocan en obtener la información de identificación personal de los clientes: nombres, direcciones, números de identificación nacional (por ejemplo, números de seguridad social en los EE. UU., códigos fiscales en España) e información de tarjetas de crédito para posteriormente vender estos registros en mercados digitales clandestinos. Esto a menudo generan la pérdida de la confianza del cliente, multas regulatorias e incluso acciones legales.

Los ciberataques y la ciberdelincuencia están aumentando en toda Europa, y cada vez son más sofisticados. Esta tendencia seguirá agravándose en el futuro, ya que se espera que 22 300 millones de dispositivos en todo el mundo estén conectados a la internet en 2024. Con una respuesta firme en materia de ciberseguridad que permita crear un ciberespacio abierto y seguro se podrá generar entre los ciudadanos una mayor confianza en las herramientas y servicios digitales.

Con la extensión de las ciberamenazas en constante aumento, la Corporación Internacional de Datos predice que el gasto mundial en soluciones de ciberseguridad alcanzará la impresionante cifra de 133 700 millones de dólares para el año 2022. Los gobiernos de todo el mundo han respondido a las crecientes ciberamenazas con orientaciones para ayudar a las organizaciones a aplicar prácticas eficaces de ciberseguridad.

En Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) ha creado un marco de ciberseguridad. Para contrarrestar la proliferación de código malicioso y ayudar en la detección temprana, en el marco se recomienda el monitoreo continuo y en tiempo real de todos los recursos electrónicos.

Quien apueste únicamente por medidas preventivas como cortafuegos o escáneres antivirus, se lo pone demasiado fácil a los hackers. Para protegerse de forma eficaz frente a los ciberataques, las empresas deben tener en cuenta la prevención, detección y reacción por igual.

Figura 21. Las cinco principales amenazas cibernéticas (2019).

TIPOS DE CIBERAMENAZAS

La seguridad cien por cien no existe, pero si aplicamos el sentido común y algunas reglas básicas su impacto se puede ver muy reducido.

Las amenazas a las que se enfrenta la ciberseguridad son cuatro:

- ✓ El delito cibernético incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.
- ✓ El ciberespionaje también muy extendido. Los ciberataques a menudo involucran la recopilación de información con fines políticos.
- ✓ El ciberterrorismo tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor.
- ✓ La ciberguerra o guerra tecnológica hace referencia al uso de ataques digitales por parte de un país para dañar los sistemas informáticos más esenciales de otro país. Para esto se pueden usar virus informáticos o realizar ataques de piratería informática.

Pero ¿cómo consiguen los agentes malintencionados el control de los sistemas informáticos? Estos son algunos de los métodos comunes utilizados para amenazar la ciberseguridad:

Malware

"Malware" se refiere al software malicioso, diseñado para obtener acceso no autorizado o causar daños en un ordenador.

Ya que es una de las ciberamenazas más comunes, el malware es software que un cibercriminal o un hacker ha creado para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia propagado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima, el malware puede ser utilizado por los ciberdelincuentes para ganar dinero o para realizar ciberataques con fines políticos.

Hay diferentes tipos de malware, entre los que se incluyen los siguientes:

- ✓ Virus: un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso. Afortunadamente existen muchos antivirus muy eficaces, gratuitos y de pago.

- ✓ Troyanos: un tipo de malware que se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos en sus ordenadores o teléfonos móviles, donde causan daños o recopilan datos.

- ✓ Spyware: un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.

- ✓ Ransomware: malware sofisticado y selectivo que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos, a menos que se pague un rescate. El pago del rescate no garantiza que se recuperen los archivos o se restaure el sistema.

    - Ciberdelincuencia como servicio (CaaS)
      Hoy en día, los ciberdelincuentes comercializan el ransomware de manera similar al software normal, creando así un nuevo modelo de negocio. A cambio del pago de una tarifa de licencia, los delincuentes pueden comprar malware que incluso incluye

servicios de soporte técnico. Las empresas deben responder de forma proactiva y aumentar sus inversiones en formación y concienciación de los empleados y en la seguridad de su infraestructura técnica.

- ✓ Adware: software de publicidad que puede utilizarse para difundir malware.

- ✓ Botnets: redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario. Convierten tu ordenador en un "zombi".

- ✓ Rootkit: un paquete de software malicioso que está diseñado para permanecer oculto en un ordenador mientras proporciona acceso y control remotos. Los ciberdelincuentes los utilizan para manipular el equipo sin el conocimiento o consentimiento del usuario.

Pegasus (spyware)

Un tipo de spyware que está teniendo una gran repercusión estos días es el debido a "Pegasus", un programa utilizado para acceder a teléfonos móviles y controlar sus funciones y contenido. Ha protagonizado las noticias de prensa, pues ha sido empleado para espiar a políticos del Gobierno Central y de alguna autonomía, como la catalana. Aun así, Pegasus no es el primer software utilizado para espiar a políticos, periodistas, etc. sino que ha habido y hay otros, no es exclusivo.

Hay varias maneras de detectar el software espía Pegasus en un teléfono móvil, ya sea Android o iOS, y muy sencillas de ejecutar, por ejemplo, utilizando el antivirus Look Out, que podemos encontrar en la App Store y en Google Play. Y también MVT, que de comentará después.

> *El 2 de mayo el Gobierno anunció que los teléfonos móviles de Pedro Sánchez y de Margarita Robles fueron infectados con el software Pegasus. El ministro de la Presidencia, Relaciones con las Cortes y Memoria Democrática, Félix Bolaños, aseguró en rueda de prensa que ambos habían sido sometidos a escuchas "ilícitas y externas.*
>
> *El Centro Nacional de Inteligencia (CNI), el servicio de inteligencia español, ha confirmado que espió a 18 políticos catalanes independentistas después de recibir la autorización de un juez. Sin embargo, todavía hay dudas sobre quién autorizó el espionaje al resto de políticos y qué organismos del Estado están involucrados.*

Pegasus es un software desarrollado por la compañía israelí NSO Group, una empresa israelí creada por tres antiguos agentes del ejército de Israel especializados en ciberarmamento y ataques informáticos, que permite hacerse con el control remoto de un dispositivo móvil sin que el usuario sea consciente de ello. Se utiliza por parte de los servicios de inteligencia de los gobiernos –como en España por el CNI (Centro Nacional de Inteligencia)– no siendo accesible al público general. Sitio web: https://www.nsogroup.com/

Pegasus utiliza doce técnicas para explotar diferentes vulnerabilidades: infecta el móvil, escala privilegios, descubre lo que hay en el móvil, accede a las credenciales que el teléfono tiene guardadas y toma el control para escuchar, leer, robar, abrir micrófonos, abrir cámaras y enviar la información robada a quien la compra o realiza chantajes.

Según la compañía: "Nuestra tecnología se utiliza todos los días para acabar con redes de pedofilia, cárteles de la droga, mafias de explotación sexual, bandas de delincuentes internacionales. Salva vidas, encuentra a niños desaparecidos y protege el espacio aéreo de las ciudades del ataque de drones enemigos. Solo se vende a funcionarios gubernamentales amparados por la ley con el único propósito de prevenir el crimen y el terrorismo".

Figura 22. Funcionamiento de Pegasus. Fuente: Citizen Labs. OCCRP.

Fue creado para infectar teléfonos Android, iOS, Blackberry o Symbian y convertirlos en un dispositivo de vigilancia en remoto. Una vez dentro, el spyware puede tener acceso a la cámara, el micrófono (sin necesidad de que esté en uso), la localización del GPS, las contraseñas y las aplicaciones de mensajería.

Puede grabar conversaciones telefónicas, capturar pantallas y descargar contenido sin que el usuario sea consciente de ello. La principal virtud de este programa de vigilancia es que puede utilizar tecnología de "cero clic", es decir, no necesita que la víctima realice ninguna acción consciente o inconsciente para dejarse infectar.

Pegasus, aprovechando alguna vulnerabilidad del sistema, puede infectar a un dispositivo móvil de variadas maneras. Por un lado, existe una versión más clásica que requiere la acción del usuario accediendo a un enlace que le ha podido llegar por SMS, WhatsApp, email, un mensaje que vea en redes sociales; o descargando archivos, como podría ser el caso del presidente del Gobierno; sin embargo, la forma de hackeo más empleada no requiere ni siquiera la acción del usuario. También se puede cargar manualmente.

Malware de cero clic

Tradicionalmente, el software espía requiere convencer al usuario objetivo de que haga clic en un enlace o archivo comprometido para que se instale en su teléfono, tableta u ordenador. Sin embargo, con un ataque de clic cero, el software puede instalarse en un dispositivo sin que la víctima tenga que hacer clic en ningún enlace. Como resultado, el malware de cero clic o sin clics es mucho más peligroso.

Por lo general, la infección remota de un dispositivo móvil objetivo requiere un cierto grado de ingeniería social, mediante la cual el usuario hace clic en un enlace malicioso o instala

una aplicación maliciosa para ofrecerle un punto de entrada al atacante. Este no es el caso en los ataques de cero clic, los cuales evitan por completo la necesidad de aplicar ingeniería social.

Una vulnerabilidad de cero clic puede afectar a varios dispositivos, tanto Apple como Android. El hecho de que las aplicaciones de mensajería permitan identificar a las personas mediante sus números de teléfono, los cuales pueden localizarse fácilmente, implica que pueden ser un objetivo claro tanto para entidades políticas como para operaciones comerciales de piratería.

Cómo protegerse de los exploits de cero clic

Como los ataques de cero clic no se basan en la interacción de la víctima, es evidente que no se puede hacer mucho para protegerse. Aunque esto suene desalentador, es importante recordar que, generalmente, estos ataques suelen estar dirigidos a víctimas específicas con fines de espionaje o, quizá, para obtener ganancias económicas. Ante esto se pueden poner en marcha medidas de sentido común, como las siguientes:

- ✓ Mantener actualizado el sistema operativo, el firmware y las aplicaciones en todos los dispositivos cuando se reciban las solicitudes correspondientes.
- ✓ Usar una autenticación segura para acceder a las cuentas, especialmente en redes críticas. Usar contraseñas sólidas; es decir, contraseñas largas y únicas.
- ✓ Descargar solo aplicaciones de tiendas oficiales.
- ✓ Desinstalar las aplicaciones que ya no se utilicen.
- ✓ No hacer «jailbreaking» o «rooting» en muestro teléfono, ya que esto elimina la protección proporcionada por Apple y Google.
- ✓ Utilizar la protección por contraseña de nuestro dispositivo.
- ✓ Hacer una copia de seguridad frecuente de los sistemas, así se podrán restaurar en caso de ransomware, y contar con una copia de seguridad actual, en un servidor local o en la nube de todos los datos acelera el proceso de recuperación.
- ✓ Activar bloqueadores de ventanas emergentes o evitar que estas aparezcan modificando la configuración del navegador. Los estafadores suelen usar ventanas emergentes para propagar malware.

Usar un antivirus integral también ayudará a mantenernos a salvo en Internet. Los más conocidos ofrecen una protección contra hackers, virus y malware, además de protección para pagos y herramientas de privacidad que nos protegerán desde todos los ángulos.

Qué es el Mobile Verification Toolkit

Mobile Verification Toolkit (MVT) es el nombre de un software desarrollado y publicado por el Laboratorio de Seguridad de Amnistía Internacional en julio de 2021. Permite hacer un análisis forense consentido de dispositivos Android e iOS, con el fin de identificar rastros de Pegasus. Sitio web: https://cdisonancia.gitlab.io/mvt-esp/

Amnistía Internacional ha desarrollado un software de detección de virus diseñado para analizar todos los archivos a partir de una copia de seguridad y seguir cualquier rastro de Pegasus que haya en nuestro dispositivo. Este análisis se envía automáticamente a Amnistía Internacional, desde donde nos informarán si se ha encontrado a Pegasus en el móvil.

Figura 23. Mobile Verification toolkit.

Esta herramienta forense para móviles, que analiza una copia realizada del móvil sospechoso, se ha publicado con licencia de código abierto y tanto la arquitectura, como el funcionamiento, la metodología y los indicadores técnicos están detallados. El fin es ayudar a los investigadores de seguridad de la información y a la sociedad civil a detectar y responder a estas graves amenazas. Web: https://docs.mvt.re

Después de conectar el Smartphone a un ordenador, el programa MVT guardará una copia de seguridad del terminal en el ordenador y escaneará todos los datos. Tras realizar este procedimiento, la aplicación avisará al usuario de si la información del terminal analizado se ha visto comprometida en algún momento por Pegasus.

Phishing

La suplantación de identidad (phishing) es la práctica de enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. El objetivo es robar datos sensibles, como números de tarjetas de crédito, información de inicio de sesión y otra información personal. Es el tipo más común de ciberataque. Puede protegerse mediante la educación o una solución tecnológica que filtre los correos electrónicos maliciosos.

Una variante es el **Smishing**: (SMS+ Phishing) Ataque de Phishing realizado a través de un SMS. Por lo general, el contenido del mensaje invita a pulsar en un link que lleva a una web maliciosa, en el que intentarán engañar con que la víctima introduzca información sensible o de que descargue una aplicación que en realidad es un malware. Estos SMS generalmente se hacen pasar por servicios habitualmente usados en la población, comúnmente bancos o servicios de reparto. Los usuarios ya tienen cierto nivel de concienciación con las estafas a través de email, pero no tanto con los SMS, es por eso que hay una falsa percepción de seguridad con la mensajería móvil y nos lleva a que este ataque sea más efectivo.

Figura 24. Phishing. Fuente: Fundación UNAM.

Autenticación multifactor

Los ciberdelincuentes intentan vulnerar nuestras cuentas y realizan diversos tipos de ataques con el objetivo de obtener un beneficio y robarnos nuestros datos. Uno de los procedimientos que pueden emplear es un ataque de phishing para robarnos nuestras credenciales. Si queremos añadir una seguridad extra a nuestras cuentas y protegerlas, podemos dotarlas de una segunda línea de defensa; así, en el caso de que obtengan nuestra contraseña no van a poder acceder a nuestra cuenta porque les falta un segundo paso de comprobación.

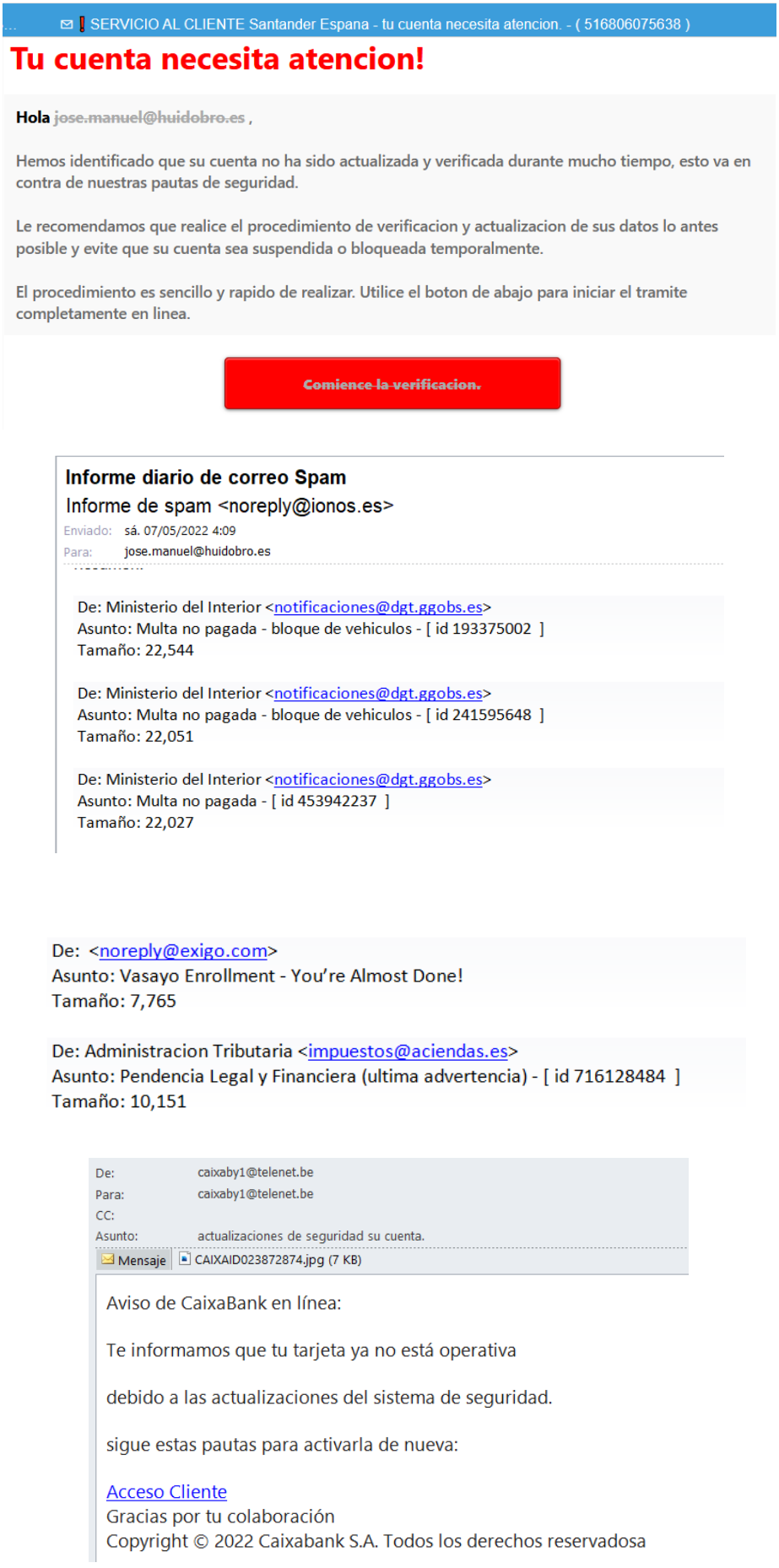
Figura 25. Autenticación multifactor.

Normalmente, ese segundo paso va a ser introducir un código que genera una aplicación o que recibimos en un SMS. También en algunas plataformas se permite vincular ese segundo paso a un dispositivo. En cuanto a una aplicación con autenticación multifactor que podemos utilizar para proteger nuestras cuentas es Google Authenticator.

Clickjacking es una técnica que permite a un atacante engañar a un usuario para que haga clic en elementos aparentemente inofensivos de una página web con fines fraudulentos: descargar malware, redirigirlos a sitios web maliciosos o revelar información sensible.

Los ciberdelincuentes intentan vulnerar nuestras cuentas y realizan diversos tipos de ataques con el objetivo de obtener un beneficio y robarnos nuestros datos. Uno de los procedimientos que pueden emplear es un ataque de phishing para robarnos nuestras credenciales. Aunque los mensajes que suelen enviar son muy burdos y con errores gramaticales o de redacción, al llegar a miles (millones) de usuarios y ser muy repetitivos, es fácil que alguno, por descuido o desconocimiento pique, acceda al enlace y de sus datos personales.

Pero si queremos añadir una seguridad extra a nuestras cuentas y protegerlas, podemos dotarlas de una segunda línea de defensa. Así, en el caso de que obtengan nuestra contraseña no van a poder acceder a nuestra cuenta porque les falta un segundo paso de comprobación.



SERVICIO AL CLIENTE Santander Espana - tu cuenta necesita atencion. - (516806075638)

Tu cuenta necesita atencion!

Hola jose.manuel@huidobro.es ,

Hemos identificado que su cuenta no ha sido actualizada y verificada durante mucho tiempo, esto va en contra de nuestras pautas de seguridad.

Le recomendamos que realice el procedimiento de verificacion y actualizacion de sus datos lo antes posible y evite que su cuenta sea suspendida o bloqueada temporalmente.

El procedimiento es sencillo y rapido de realizar. Utilice el boton de abajo para iniciar el tramite completamente en linea.

Comience la verificacion.

Informe diario de correo Spam

Informe de spam <noreply@ionos.es>

Enviado: sá. 07/05/2022 4:09

Para: jose.manuel@huidobro.es

De: Ministerio del Interior <notificaciones@dgt.ggobs.es>
Asunto: Multa no pagada - bloque de vehiculos - [id 193375002]
Tamaño: 22,544

De: Ministerio del Interior <notificaciones@dgt.ggobs.es>
Asunto: Multa no pagada - bloque de vehiculos - [id 241595648]
Tamaño: 22,051

De: Ministerio del Interior <notificaciones@dgt.ggobs.es>
Asunto: Multa no pagada - [id 453942237]
Tamaño: 22,027

De: <noreply@exigo.com>
Asunto: Vasayo Enrollment - You're Almost Done!
Tamaño: 7,765

De: Administracion Tributaria <impuestos@aciendas.es>
Asunto: Pendencia Legal y Financiera (ultima advertencia) - [id 716128484]
Tamaño: 10,151

De: caixaby1@telenet.be
Para: caixaby1@telenet.be
CC:
Asunto: actualizaciones de seguridad su cuenta.

Mensaje | CAIXAID023872874.jpg (7 KB)

Aviso de CaixaBank en línea:

Te informamos que tu tarjeta ya no está operativa

debido a las actualizaciones del sistema de seguridad.

sigue estas pautas para activarla de nueva:

Acceso Cliente
Gracias por tu colaboración
Copyright © 2022 Caixabank S.A. Todos los derechos reservadosa

Figura 26. Ejemplos de correos para robar credenciales.

Ingeniería social

La ingeniería social basa su comportamiento en una premisa básica: es más fácil manejar a las personas que a las máquinas. Para llevar a cabo este tipo de ataque se utilizan técnicas de manipulación psicológica con el objetivo de conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente.

Figura 27. Ciclo de la Ingeniería social. Fuente INCIBE.

La ingeniería social es una táctica que usan para influirnos o engañarnos a fin de que revelemos información confidencial en contra de nuestros intereses. Pueden solicitarnos un pago monetario u obtener acceso a datos confidenciales. Puede combinarse con cualquiera de las amenazas listadas anteriormente para predisponernos a hacer clic en un enlace, descargar malware o confiar en una fuente maliciosa. Esto suele funcionar muy bien utilizando las redes sociales (RRSS).

Según INCIBE, a pesar de ser múltiples y varias las técnicas utilizadas por los ciberdelincuentes para manipular a sus víctimas, suelen seguir una serie de principios básicos:

Técnicas utilizan los ciberdelincuentes en los ataques de ingeniería social

- **Respeto a la autoridad**. Por norma general, los trabajadores y ciudadanos en general, respetamos la autoridad de nuestros superiores, bien sea dentro de la organización o en la vida cotidiana. Este tipo de ataques se basa en ese respeto que tenemos a nuestros responsables y a autoridades como las Fuerzas y Cuerpos de Seguridad del Estado.
- **Voluntad de ayudar**. Sobre todo en los entornos laborales, los trabajadores, generalmente, cuentan con esta voluntad de ayudar a los compañeros en todo lo posible. Por este motivo, los ciberdelincuentes pueden hacerse pasar por un falso empleado de la empresa. Otra variante utilizada, es hacerse pasar por un técnico de informática para instalar herramientas de acceso remoto no autorizado.
- **Temor a perder un servicio**. Esta técnica es habitualmente utilizada en campañas de *phishing*. Bajo el pretexto de existir repetidos accesos no autorizados, cambio en las políticas o cualquier otro engaño, los ciberdelincuentes fuerzan a la víctima acceder a una web fraudulenta donde roban información confidencial.
- **Respeto social**. En algunos casos, los ciberdelincuentes basan su estrategia en el miedo que tienen los usuarios a no ser socialmente aceptados o a perder su reputación. Esto es habitual en los correos de sextorsión, donde los ciberdelincuentes amenazan con difundir un supuesto video privado que en realidad no existe.
- **Gratis**. Este tipo de engaño se basa en ofrecer un producto o servicio gratis a cambio de información privada. Este tipo de fraude suele llevarse a cabo por medio de páginas web emergentes que suelen aparecer cuando se navega por sitios poco legítimos. También es común en mensajes de redes sociales o aplicaciones de mensajería.

Los ataques de ingeniería social usan como canal principal para su propagación el correo electrónico gracias a su uso masivo tanto por empresas, como por particulares. Pero no es la única vía de la que hacen uso los ciberdelincuentes, ya que pueden utilizar otros canales de comunicación como llamadas telefónicas, aplicaciones de mensajería, redes sociales, USB, etc.

Ataque de tipo "Man-in-the-Middle"

Un ataque "MitM" es un tipo de ciberamenaza en la que un cibercriminal intercepta la comunicación entre dos individuos para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

Amenazas persistentes avanzadas (APT)

Una amenaza persistente avanzada (APT) es un término que se usa para describir una campaña de ataque en la que un intruso, o equipo de intrusos, establece una presencia ilícita y cautelosa a largo plazo en una red o sistema para extraer datos altamente confidenciales, mientras evita la activación de respuestas defensivas. Debido a su complejidad las APT están bien financiadas y apuntan a las organizaciones o países por motivos políticos o comerciales.

Generalmente relacionadas con el espionaje con base en la red, el propósito de las APT es implementar malware personalizado en uno o varios sistemas de destino y pasar desapercibidas. Con múltiples fases de operación y varios tipos personalizados de malware que afecten a distintos dispositivos y realizan funciones específicas, un atacante individual generalmente carece del conjunto de habilidades, recursos o la perseverancia necesarios para llevar a cabo una APT.

Ataque de denegación de servicio

Un ataque de denegación de servicio (DoS y DDoS) son un tipo de ataque a la redes, cuando los cibercriminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema sea inutilizable e impide que una organización, como un banco o un aeropuerto, realice funciones vitales. Un ataque DoS distribuido (DDoS) es similar a un ataque DoS, pero proviene de múltiples fuentes coordinadas.

Los ataques de DoS se consideran un riesgo importante porque pueden interrumpir fácilmente la comunicación y causar una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de llevar a cabo, incluso por un atacante inexperto.

Amenazas internas

Los empleados actuales o anteriores, socios comerciales, contratistas o cualquier persona que haya tenido acceso a sistemas o redes en el pasado se pueden considerar una amenaza interna si abusan de sus permisos de acceso. Las amenazas internas pueden ser invisibles para las soluciones de seguridad tradicionales como firewalls y sistemas de detección de intrusos, que se enfocan en amenazas externas. La principal amenaza interna en las organizaciones son los empleados que cometen negligencias de forma involuntaria.

Vulnerabilidad del teletrabajo

Muchas empresas no estaban preparadas para el escenario actual y han tenido que adaptarse rápidamente a realizar sus trabajos desde casa sin ser conscientes de todas las implicaciones que tiene y sin un plan de acción para garantizar la ciberseguridad en el teletrabajo, algo que puede ponerlas en una situación vulnerable frente a los ataques de los ciberdelincuentes, puesto que en el momento en el que se produce una comunicación entre un domicilio y la oficina, comienzan a compartirse datos entre ambos lugares que pueden ser interceptados por terceros.

Los autores de las ciberamenazas explotan las vulnerabilidades de los sistemas, redes y aplicaciones empleados por las empresas, las administraciones públicas y los centros de enseñanza para apoyar al personal que trabaja actualmente a distancia. Los delincuentes buscan nuevas oportunidades de intrusión para robar datos, obtener ganancias o provocar disfunciones.

Envenenamiento SEO

El envenenamiento SEO podemos decir que es uno de los problemas de seguridad que puede afectar a una página web. Un objetivo principal para cualquier usuario particular o empresa que cuente

con un sitio web es posicionarlo correctamente en los buscadores. Esto es lo que se conoce como SEO. Es todo lo que conlleva que este mismo artículo llegue a tener relevancia para los buscadores. Ahora bien, esto también puede ser utilizado por los piratas informáticos para aumentar el tráfico a determinados sitios bajo su control, que en realidad son maliciosos.

Algo básico va a ser siempre verificar que el sitio web al que estamos accediendo sea oficial y debemos comprobar la URL, la información que muestran y el aspecto general. De esta forma evitaremos dar nuestros datos o descargar algún archivo en un sitio que en realidad es falso y ha sido creado únicamente para atacar, pero ha aparecido en una buena posición en el buscador.

ESPIONAJE POR CÁMARA WEB

A veces se nos olvida que la webcam de nuestro ordenador o de nuestro Smartphone es un puerto de entrada para los piratas informáticos, por este motivo hay que estar atentos a ciertos síntomas que están relacionados con una cámara secuestrada. También, esto todo esto afecta a las cámaras de videovigilancia del hogar, en caso de que dispongamos de una o varias de ellas asociadas a un sistema de alarma

Por ejemplo, algunas de las características de una cámara sencilla de video para el hogar, de interior o exterior y que podemos adquirir por un precio inferior a unos 50 euros, son: Cámara IP Wi-Fi 360º de Vigilancia Interior Inteligente, alta resolución 720p HD. Sensor de Movimiento, Visión Nocturna, Audio Bidireccional. Wi-Fi 2,4 GHz. Control remoto por app. Se pueden guardar y visualizar las fotos y grabaciones de video en la aplicación del dispositivo, en una tarjeta MicroSD de hasta 64 GB, o bien en la nube, pero esto último suele requerir una suscripción y abonar una cantidad mensual por ello, pero así se garantiza que en caso de ser sustraída o rota, la información se puede siempre recuperar. Gracias a la integración de varios factores como la tecnología de aprendizaje profundo, la optimización enfocada de los algoritmos y el software de red, la cámara puede determinar con precisión si es necesario enviar una notificación a nuestro teléfono para alertarnos de cualquier anomalía cuando detecta movimientos sospechosos.

Figura 28. Cámara IP para videovigilancia.

Su instalación suele ser muy sencilla. Para que se pueda conectar perfectamente y ver las imágenes de la mejor manera, estas cámaras poseen una conectividad Wi-Fi para conectarse a nuestro Smartphone o tableta de una manera muy fácil. Con esta conexión con el dispositivo móvil se pueden tener diversas mejoras como poder ver las imágenes allá donde estemos y que podamos controlar la cámara con Alexa o Google HomeKit para tener la mejor capacidad de conexión.

Figura 29. Control de cámaras desde el smarphone.

Informar de la presencia de cámaras de videovigilancia
Si la cámara o cámaras se instalan de cara al exterior de la vivienda, es siempre obligatorio informar de su presencia. También es imprescindible si, por ejemplo, la instalación de cámaras se produce en una Comunidad de Propietarios. En éste último caso, además, hay dos trámites necesarios que hay que realizar; por una parte, el fichero de datos de la Comunidad debe ser dado de alta en la AEP (Agencia Española de Protección de Datos) y, por otro, en este organismo debe también estar registrado al menos un fichero de datos personales. A todo ello hay que añadir que la Ley Orgánica de Protección de Datos impide que las instalaciones de videovigilancia de las comunidades se dirijan a la vía pública.

Diferentes modelos de cámaras de videovigilancia

Podemos elegir entre diferentes tipos de cámaras, y en muchas ocasiones las podremos instalar nosotros mismos, bien de forma independiente o asociadas a otros dispositivos de seguridad caseros. Es mucho más fácil y económico que contratar empresas de seguridad, ya que no siempre se puede decidir sobre la privacidad y omitir la grabación y transmisión de video sin previo aviso:

- Cámaras analógicas: Son las de mayor calidad, aunque con menos sistemas. Las mejores son las híbridas.
- Cámaras IP: Proporciona una excelente calidad de imagen, así como enviar videos a la aplicación de teléfonos móviles para ver la grabación en tiempo real.
- Cámara HD-TVI: La mejor calidad, también utiliza el mismo cableado.
- Cámara WI-FI: Buena precisión y evita cablear cables.
- Cámara oculta: Oculta en lugares pequeños y de tamaño reducido. Su propósito es que la persona que está siendo grabada no lo sepa.
- Cámara de simulación: Falsas cámaras que parecen reales.

Además, existen modelos que funcionan tanto con batería como conectadas directamente a la red eléctrica. Así que escogeremos una opción que se ajuste a la perfección a lo que buscamos.

Algunos de los motivos que pueden indicarnos si estamos siendo espiados, son:

- **La luz que indica que la cámara está activa se enciende:** aunque algunos atacantes pueden hacer que no se encienda la luz de la cámara, no siempre es así. Si se enciende cuando no la estás usando, es posible que el dispositivo haya sido secuestrado.
- **Presencia de archivos extraños en la computadora:** si un ciberdelincuente ha realizado un registro de su cámara web es posible que aún haya archivos guardados en su computadora. Buscar cualquier cosa inusual, especialmente en los documentos o carpetas de video que forman parte del disco duro.
- **Presencia de aplicaciones inusuales en el ordenador:** una de las formas más comunes en que utilizan los cibercriminales para grabar desde tu cámara web es mediante un RAT. Escanear el equipo con una solución antimalware y revisar las posibles alertas sobre algún software que no debería estar en la PC o dispositivo.
- **La configuración del PC cambió:** otra cosa que los programas maliciosos como los RAT suelen hacer para allanar su camino es interferir con el software de seguridad que está instalado en una máquina o en el sistema operativo. Comprobar si se han deshabilitado algunas funciones de seguridad.

¿Alguna vez nos han arreglado el PC de forma remota? A mí, sí. Llamamos al servicio de atención al cliente, seguimos unas sencillas indicaciones y el interlocutor que está al otro lado de la línea —y, a menudo, en el otro extremo del mundo— accede a nuestro equipo para arreglarlo o para instalar una nueva versión de algún programa o antivirus.

El software de administración remota es bastante común, pero no siempre se usa con fines nobles. Cuando está programado para invadir equipos, se denomina «troyano de acceso remoto» (RAT, por su sigla en inglés). Programas de malware como SubSeven, Back Orifice, Poison-Ivy, ProRat (y la lista continúa) son las armas definitivas de pirateo.

Una vez que el troyano está en el PC, el ciberacosador puede ver lo que haces en Internet, leer mensajes, capturar tu pantalla y las pulsaciones de teclado, así como hacerse con el control total del equipo, cámara incluida.

En los albores de la informática, uno de los mayores miedos de los usuarios era que se les espiase. A través de programas que registraban todo lo que hacían, las páginas visitadas, los términos de busca, los correos enviados... y, sobre todo, que vieran a través de la webcam

CIBERDELINCUENCIA Y REDES SOCIALES

En la actualidad, uno de los medios que suelen emplear los delincuentes para sus ataques son las redes sociales (RRSS), por la facilidad que supone y el gran alcance que tienen.

Así, según un reciente artículo aparecido (20-Abril-2022) en el diario CincoDías:

https://cincodias.elpais.com/cincodias/2022/04/19/companias/1650374141_599961.html

> *Empresas de reconocido prestigio, aquellas marcas con las que más se suele interactuar en internet, bancos, compañías de suministros o administraciones públicas (ojo que ya ha arrancado la campaña de Hacienda). Los ciberdelincuentes suelen atreverse con todo y con todos, tal y como acaba de poner de manifiesto un estudio.*

La división de Inteligencia de Amenazas de Check Point Software Technologies ha analizado cuáles son las compañías que más tratan de suplantar estos delincuentes para acceder a información personal o credenciales de pago.

La red social LinkedIn encabeza por primera vez en la historia esta clasificación, al haber acaparado más de la mitad (52%) de los intentos de phishing durante el primer trimestre del año, lo que representa un espectacular aumento del 44% respecto al periodo anterior, cuando esta red social ocupaba la quinta posición en el ranking y apenas representaba el 8% de esta clase de ciberataques.

Figura 30. Índice de marcas suplantadas.

> *De esta forma LinkedIn supera a la empresa de transportes DHL como la más afectada, que ahora pasa a ocupar la segunda posición y representa el 14% de todos los intentos de phishing durante los tres primeros meses del año. Tal y como explican desde Check Point, todo apunta a que las redes sociales se han convertido en el primer objetivo de los hackers, mientras que en el pasado empresas de transporte y gigantes tecnológicos como Google, Microsoft o Apple se disputaban este triste honor.*

Además, en el Informe de seguridad cibernética de 2022 (Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed) se muestran las tendencias clave de seguridad cibernética de 2021, incluido un aumento de ataques a la cadena de suministro y una mayor interrupción de la vida cotidiana. La Educación y la Investigación se revelaron como el sector más objetivo.

Desde el ataque 'SolarWinds' a principios de año, que presentó un nivel completamente nuevo de sofisticación y propagación, hasta diciembre y la afluencia de explotaciones de vulnerabilidad 'Apache Log4j', el Informe de seguridad cibernética 2022 revela el ataque clave vectores y técnicas presenciadas por Check Point Research (CPR) durante 2021.

Los aspectos más destacados del informe de seguridad cibernética de Check Point 2022 incluyen:

- Los ciberataques contra redes corporativas aumentaron un 50% en 2021 respecto a 2020.
- Educación e investigación fue el sector más atacado, con organizaciones que enfrentaron un promedio de 1.605 ataques semanales.

- Los proveedores de software experimentaron el mayor crecimiento año tras año, con un aumento del 146%.

El informe es accesible en: https://pages.checkpoint.com/cyber-security-report-2022.html?utm_source=cp-home&utm_medium=cp-website&utm_campaign=pm_wr_21q1_ww_security_report

CIBERTERRORISMO

En los años 80, Barry Collin, un investigador senior del *Institute for Security and Intelligence* en California acuñó el término *cyberterrorism* para referirse a "la convergencia del ciberespacio con el terrorismo". El ciberterrorismo es una forma de terrorismo en la que los grupos agresores emplean medios digitales para atacar ordenadores, sistemas de servicio público e información privada con el objetivo de intimidar o coaccionar a un Gobierno o población. Sus fines pueden ser políticos, sociales o religiosos.

Un ejemplo de ciberterrorismo es la intrusión en un sistema informático de un hospital para dañar su infraestructura crítica y con ello afectar a los pacientes. Suena un poco exagerado, pero puede asemejarse a lo que pasó con el ransomware Exptr o WannaCry.

Comprender los peligros del ciberterrorismo es importante, porque todos los que usamos internet somos estamos expuestos a ello. Inclusive, todos los profesionales en TI deben ser conscientes de las posibles áreas de vulnerabilidad, con el fin de proteger mejor sus sistemas informáticos y posiblemente ayudar a poner fin a esta actividad.

Debido a que el ciberterrorismo es un problema que crece cada día, muchas naciones han solicitado que sus plataformas de detección de ciberseguridad se modernicen. Como requiere de un alto entrenamiento y gran dedicación, pero es difícil de rastrear y el daño al "enemigo" puede ser desde considerable hasta muy grave, los países deben establecer una continua cooperación en materia de seguridad, manejo de crisis y tecnología avanzada en la lucha contra el terrorismo.

Por ejemplo, en Estados Unidos desde 1996 se creó la Comisión de Protección de Infraestructura Crítica. Las autoridades encontraron que la combinación de electricidad, comunicaciones y computadoras es necesaria para la supervivencia del país, por los cual no pueden ser amenazados por la guerra cibernética. Lo que se recomienda en estos casos es que los sistemas críticos sean aislados de la conexión externa, o protegidos por firewalls adecuados. En España, desde el 2007, tenemos el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

A pesar de toda la ciberseguridad que pueda tener una empresa o gobierno, hasta la fecha no hay formas infalibles de proteger un sistema, pero una buena plataforma de protección es más complicado que sea vulnerada. Otro de los métodos más común de protección es el cifrado.

Los nuevos ataques de DDoS, ransomware o malware pueden ser una pequeña prueba de lo que se podría realizar con un gran ciberataque mundial que pueda ser considerado ciberterrorismo, por lo cual hay que estar muy atentos, y considerar una buena estrategia de seguridad. Los mayores ataques de ciberterrorismo se producen mediante la denegación de servicio, para extorsionar a las empresas y a los gobiernos, y el robo de cuentas.

Inyección de código SQL

Una inyección de código SQL (por sus siglas en inglés *Structured Query Language*) es un tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso

en una base de datos mediante una instrucción SQL maliciosa, lo que les brinda acceso a la información confidencial contenida en la misma.

MEDIDAS PARA AFRONTAR LOS CIBERCRÍMENES

Y para mitigar el riesgo, las empresas deben tomar medidas. Aquí se muestran algunos consejos para comenzar a tomar en serio la ciberseguridad en un negocio:

- Toda empresa con presencia debe invertir en medidas avanzadas de **seguridad cibernética**. Incluyendo firewalls, conexiones cifradas, protección contra fugas de datos y protección contra ransomware.
- Deben configurarse **filtros de spam** para evitar que se envíen correos electrónicos de phishing a sus empleados, evitar la suplantación de correo electrónico y escanear correos electrónicos entrantes / salientes.
- El **software antivirus** también debe usarse y actualizarse regularmente para ayudar a proteger los puntos finales.
- Las **copias de seguridad** son muy importantes. Los datos de empleados y de la empresa deben ser respaldados regularmente para reducir el riesgo de perder todo si el sistema falla o si un hacker lo toma como rehén.
- Los archivos confidenciales de la compañía deben respaldarse en una **instalación de almacenamiento remota** y desconectada (como copias de seguridad sin conexión).
- Tener un **plan de respuesta a incidentes** con el que identificar la última copia de seguridad, los protocolos de comunicación con la policía, procedimientos de aislamiento para dispositivos.
- Adoptar la cultura empresarial, la transformación digital y la **alfabetización cibernética**.

Figura 31. Ciberataque.

Protección frente a los ciberataques

¿Cómo podemos las personas y las empresas protegernos contra las ciberamenazas? A continuación se indican algunos consejos de ciberseguridad:

1. Actualizar el software y el sistema operativo. Esto significa que aprovechará las últimas revisiones de seguridad.

2. Utilizar software antivirus. Las soluciones de seguridad detectarán y eliminarán las amenazas. Mantener el software actualizado para obtener el mejor nivel de protección.
3. Utilizar contraseñas seguras. Asegurarnos de que las contraseñas no sean fáciles de adivinar, utilizando números, letras mayúsculas y minúsculas y caracteres especiales. Modificar las contraseñas que vengan por defecto en el dispositivo.
4. No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos. Podrían estar infectados con malware.
5. No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos. Es una forma común de propagación de malware.
6. Evitar el uso de redes Wi-Fi no seguras en lugares públicos. Las redes no seguras nos dejan vulnerable a ataques del tipo MitM (o MitMobile). Lo mejor sería utilizar una VPN (*Virtual Private Network*) para proteger la conexión a Internet.
7. Informarse en sitios web oficiales o de confianza sobre el *modus operandi* de los ciberdelincuentes y hacer un uso responsable de los dispositivos y la navegación.
8. extremar todas las precauciones ante cualquier tipo de comunicación recibida en los dispositivos personales o de trabajo.

Todo software es vulnerable por naturaleza, no importa el esfuerzo que se ponga en obtener un desarrollo 100% seguro: siempre existe un resquicio por el que un atacante puede colarse hasta obtener el control del software y del dispositivo que lo ejecuta. Estas vulnerabilidades van parcheándose; ya sea porque las descubren sus desarrolladores como la comunidad que hace uso del software. Precisamente, es lo que ocurre con sistemas operativos como iOS o Android: son muy seguros, pero a menudo dejan puertas abiertas (*back doors*) que tardan un tiempo en cerrarse.

Afortunadamente, en la actualidad, la IA (Inteligencia Artificial) está cambiando el juego para la ciberseguridad, con el análisis de grandes cantidades de datos de riesgo para poder acelerar los tiempos de respuesta y aumentar las operaciones de seguridad con recursos insuficientes.

Prueba de vulnerabilidad. Cobalt Strike

Cuando se tiene un sistema que pueda ser atacado, es conveniente probar antes su resistencia, mediante una simulación de ataque controlado, y así poder descubrir y solucionar sus debilidades y fallos. Una de las herramientas, entre otras, como Metasploit y PupyRat, que se utiliza para ello es Cobalt Strike. Una herramienta de seguridad legítima y bastante eficaz que utilizan los encargados de las pruebas de penetración para emular la actividad de los ciberdelincuentes en una red y detectar vulnerabilidades de acceso al sistema. El problema es que no solo la utilizan los propietarios legítimos, sino los ciberdelincuentes. Históricamente, el uso de Cobalt Strike con fines maliciosos se asocia principalmente a grupos de amenazas con muchos recursos, incluidos importantes grupos ciberdelictivos dedicados a las amenazas persistentes avanzadas (APT).

Desde 2012, Cobalt Strike Beacon se ha utilizado como una forma proactiva de probar las defensas de la red contra herramientas, tácticas y procedimientos (TTP) avanzados de actores de amenazas. El objetivo es imitar a los actores de amenazas más maliciosos y sus técnicas para probar su postura de seguridad y practicar los procedimientos de respuesta. Desafortunadamente, como la mayoría de las cosas en seguridad, las herramientas y el conocimiento destinados a ayudar a los equipos de seguridad también pueden ser utilizados de forma maliciosa por los delincuentes.

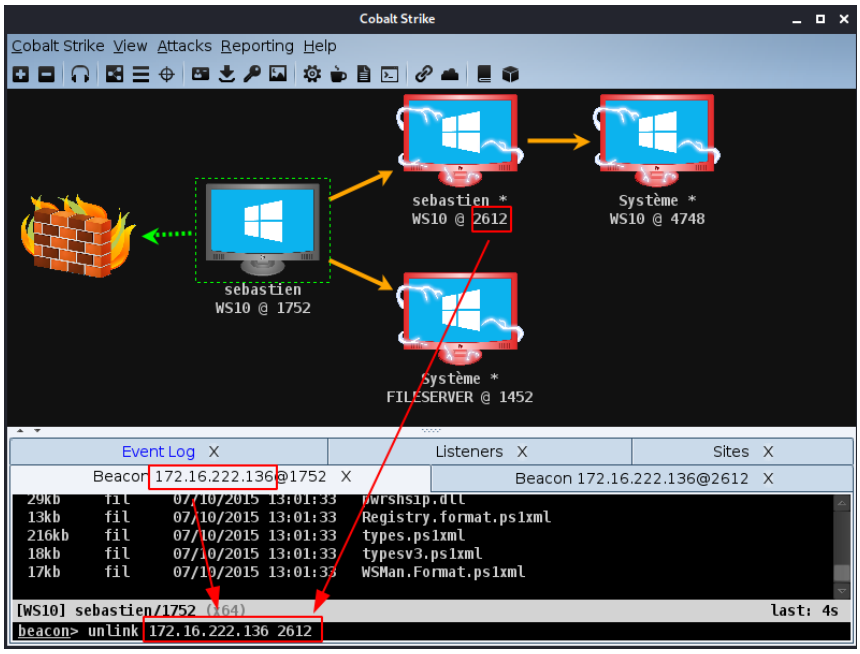


Figura 32. Aspecto de Cobalt Strike.

Si bien el autor de Cobalt Strike ha implementado muchas protecciones y esquemas de licencia (cuesta alrededor de 3.500 dólares por usuario) para mantener el código fuera de las manos equivocadas, las versiones descifradas parecen utilizar todo el marco de la solución. Los grupos de amenazas pueden obtener Cobalt Strike de varias maneras: comprándola directamente en el sitio web de un proveedor, previa verificación; comprando una versión en la "web oscura" (*Dark Web*) a través de distintos foros de hacking; o utilizando versiones pirateadas ilegítimas del software. En marzo de 2020 se publicó una versión pirateada de Cobalt Strike 4.0 y se puso a disposición de los grupos de amenazas.

CIBERACOSO

Aunque no se puede considerar estrictamente una ciberamenaza, sí que se puede asociar a ellas. Así, según propia definición de UNICEF:

Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento de manera intencionada que se repite y que busca atemorizar, enfadar o humillar a otras personas. Por ejemplo:

- Difundir mentiras o publicar fotografías o videos vergonzosos de alguien en las redes sociales. Distribuir en Internet una imagen (sexting) o datos comprometidos de contenido sexual (reales o falsos).
- Enviar mensajes, imágenes o videos hirientes, abusivos o amenazantes a través de plataformas de mensajería
- Manipular materiales digitales: fotos, conversaciones grabadas, correos electrónicos,
- cambiarlos, trucarlos y modificarlos para ridiculizar y dañar a personas
- Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha personao a través de cuentas falsas.

Los medios más habituales con los que se puede realizar el ciberacoso son: smartphones, chats, SMS, foros, redes sociales, juegos online, blog, o a través de email.

En el ciberacoso, al tratarse de una forma de acoso indirecto y no presencial, el ciberagresor no tiene contacto con la víctima, con lo cual difícilmente podrá llegar a empatizar o despertar su compasión por el otro. El ciberacosador obtiene satisfacción en la elaboración del acto violento y de imaginar el daño ocasionado en el otro, ya que no puede vivirlo in situ.

Figura 33. Ciberacoso.

Una de las modalidades es el ciberacoso escolar o ciberbullying (otra es el *grooming* o acoso sexual. El grooming es una manera de acoso que supone el contacto de un adulto, que se hace pasar por un menor, con un menor para ganarse su confianza poco a poco y después implicarle en alguna actuación sexual), que es una realidad en los colegios e institutos, y cada vez más casos salen a la luz, afectando a niños, niñas y jóvenes de edades y contextos diferentes. Es un tipo de acoso que se produce entre menores y en el que se utilizan los medios digitales para hacer daño a la víctima, conscientemente y de forma repetida en el tiempo:

- Daño intencional: el acoso puede tomar muchas formas, burlas, humillaciones, insultos, difusión de mentiras y rumores, hacerse pasar por la víctima para ridiculizarle, cerrar sus cuentas con denuncias falsas en las redes sociales, presión a sus compañeros para aislarle, etc. con la intención de hacerle daño psicológica, emocional y socialmente.
- Repetido: el daño se produce habitualmente, pudiendo llegar a ser algo cotidiano y rutinario. No se trata de incidentes aislados, peleas ni discusiones puntuales.
- Entre menores: por parte de un menor o grupo de menores hacia otro menor, pudiendo adoptar un rol de superioridad (o mayor estatus social) sobre la víctima.
- Con medios digitales: utilizan como herramienta los móviles, las redes sociales, fotos, vídeos, correo electrónico, juegos online a través de videoconsola, foros y cualquier otra aplicación móvil o servicio de Internet.

Cada situación es diferente, y también lo son las vivencias de cada menor. Aun así, es habitual que estos casos generen secuelas psicológicas graves, dañando la autoestima de las víctimas y su capacidad de relacionarse con los demás, incluso en algunas ocasiones pueden llevarles hasta una depresión o ideaciones suicidas.

Dos guías de actuación contra el ciberacoso, publicada por el INTECEO (Instituto Nacional de Tecnologías de la Comunicación, y Red.es, se encuentran en:
https://www.is4k.es/sites/default/files/contenidos/herramientas/guia_ciberacoso.pdf
https://www.is4k.es/sites/default/files/contenidos/recursos/guia_sos_educadores.pdf

Un blog dedicado a la ciberseguridad, con muchos artículos, es: https://ciberseguridad.blog/

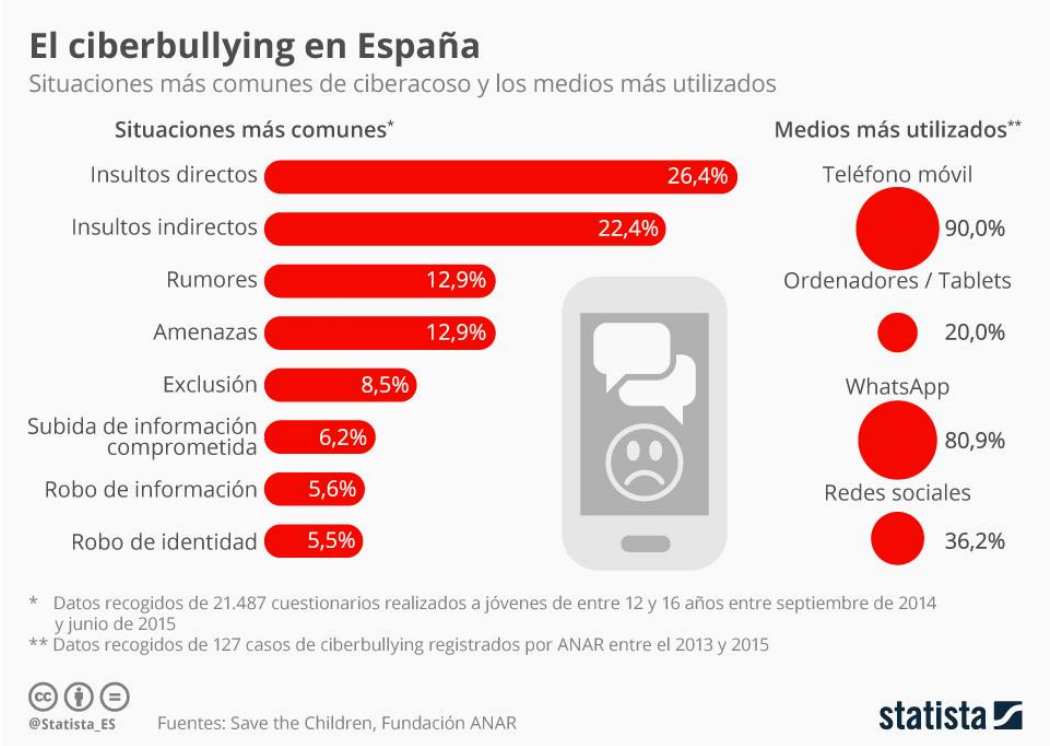


Figura 34. Datos de ciberacoso en España. Fuente: Statista.

Durante la pandemia, el ciberacoso escolar disminuyó (una de las conclusiones del informe anual sobre acoso escolar de Fundación ANAR y Fundación Mutua Madrileña, que recoge la opinión de 10.900 estudiantes y 491 docentes entre enero de 2020 y junio de 2021), como se puede ver en la siguiente figura:

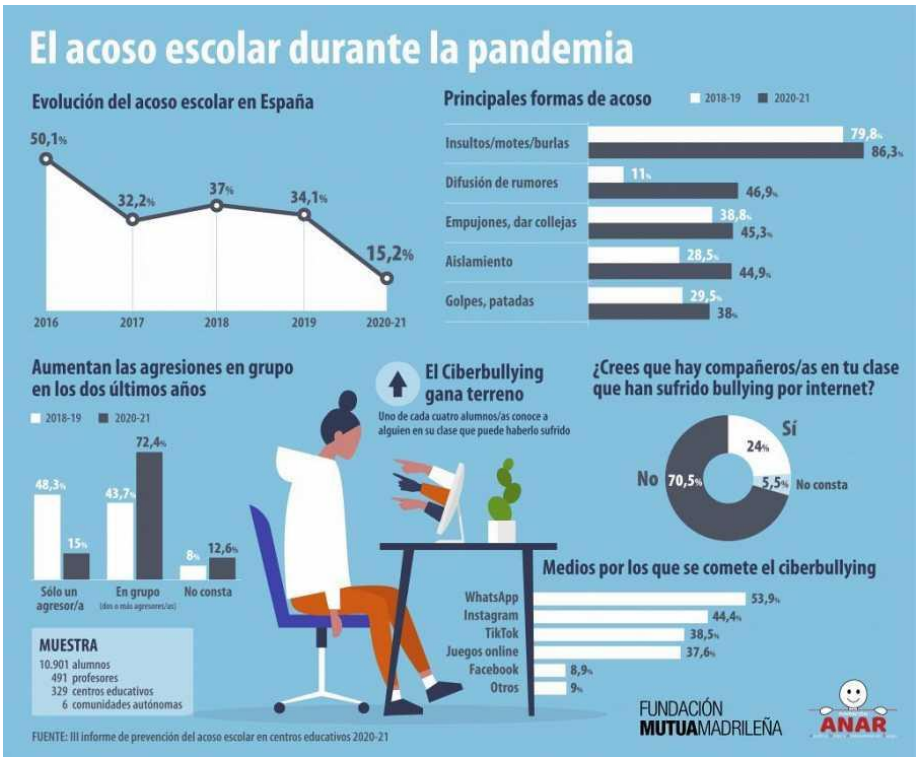


Figura 35. Evolución del ciberacoso durante la pandemia.

CRYPTOJACKING. MALWARE DE CRIPTOMINADO

El cryptojacking (también denominado minería de criptomonedas maliciosa) es un tipo de ciberdelito que consiste en el uso de manera subrepticia de la potencia de los ordenadores para generar criptomoneda. Esto suele ocurrir cuando, sin darse cuenta (por ejemplo, al hacer clic en un enlace desconocido enviado por e-mail o al visitar un sitio web infectado), un usuario instala un programa con secuencias de comando maliciosas que permiten al ciberdelincuente acceder al ordenador o a cualquier otro dispositivo de la víctima que esté conectado a Internet. A continuación los ciberdelincuentes utilizan programas llamados "mineros de monedas" para generar o extraer criptodivisas.

Al tratarse de divisas digitales, para crearlas solo es necesario disponer de programas informáticos y de la potencia de los ordenadores. Las criptomonedas que más se ven extraídas a partir de ordenadores personales son las llamadas Monero (un tipo de criptomoneda digital, utilizada para transacciones entre pares y minería. Monero utiliza varias tecnologías que mejoran la privacidad para garantizar el anonimato de sus usuarios).

El cryptojacking puede parecer un delito inofensivo, puesto que solo se aprovecha la potencia del ordenador de la víctima, pero lo cierto es que se utiliza con fines delictivos y sin el conocimiento ni consentimiento de ella, en beneficio del delincuente que crea divisas de manera ilícita. Al haber un número elevado de dispositivos afectados, generan grandes cantidades de criptomonedas, por lo que es considerado por los ciberdelincuentes como un delito lucrativo.

Las principales repercusiones de esta minería ilícita se notan en el rendimiento. Además, pueden entrañar mayores gastos para las empresas y los particulares afectados, ya que esta actividad consume mucha electricidad y potencia de los ordenadores.

Señales de ser víctimas de cryptojacking. El criptominado y el cryptojacking provocan una actividad de procesador extremadamente alta que tiene efectos secundarios notables. Las víctimas a menudo informan de un rendimiento visiblemente reducido de su dispositivo, su sobrecalentamiento y una mayor actividad del ventilador (y, por lo tanto, un ruido superior).

- Descenso evidente del rendimiento de nuestro dispositivo.
- Sobrecalentamiento de las baterías de los dispositivos.
- Los dispositivos se apagan al no disponer de la potencia necesaria.
- Reducción de la productividad de los dispositivos o el router.
- Aumento inesperado en la factura de electricidad.

Consejos para prevenir estos delitos. Usar siempre una solución de seguridad multicapa de confianza para bloquear los ataques de criptominados y el cryptojacking.

- Controlar siempre los recursos del ordenador (la velocidad de procesamiento y el uso de la potencia).
- Utilizar las extensiones del navegador diseñadas para bloquear la minería de criptomonedas.
- Utilizar más bloqueadores de anuncios destinados a proteger la privacidad.
- Instalar las últimas actualizaciones de software y los parches para el sistema operativo y las aplicaciones, especialmente en lo que se refiere a los navegadores de Internet.
- Bloquear las páginas si creemos que pueden contener secuencias de comando de cryptojacking.

TIPOS DE CIBERSEGURIDAD

Una buena estrategia de ciberseguridad para empresas o particulares se debe centrar en 3 objetivos principales: Prevención de ataques, detección de amenazas y recuperación.

Ciberseguridad preventiva

De prevenir ataques se encarga la estrategia de ciberseguridad preventiva. En este caso, el objetivo es evitar que las amenazas lleguen a tocar nuestros dispositivos. Es decir, se trata de blindar los dispositivos, redes y software frente a los ataques e impedir que entren.

Este es el tipo de ciberseguridad más común. En su nivel más básico, encontramos las aplicaciones de cortafuegos, antivirus, etc. Algo más avanzados son los nuevos *Next Generation Firewall*, que supervisan las conexiones a Internet. Todas estas aplicaciones son necesarias, pero para empresas de gran tamaño se pueden aplicar también otras soluciones personalizadas.

Una técnica común de ciberseguridad preventiva es el "pentesting", o "test de penetración". que consiste en ataques controlados a diferentes entornos o sistemas con el objetivo de detectar y prevenir posibles fallos. Se trata de una técnica para encontrar debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos, para identificar los puntos débiles y fallos del sistema de ciberseguridad.

Ciberseguridad de detección

La ciberseguridad de detección sería el siguiente nivel. En caso de que haya una amenaza intentando acceder a nuestro dispositivo o que de alguna forma ya haya conseguido entrar, el sistema de ciberseguridad debería detectarla y bloquearla (en el caso de detección antes de entrada) o reaccionar a la amenaza (si ya ha entrado en el dispositivo).

Ciberseguridad de recuperación

Este sería el último nivel de ciberseguridad. Si la amenaza consigue superar las barreras anteriores, entrarían en juego las estrategias de recuperación del dispositivo, aislando y expulsando la amenaza. En este caso sería necesario también iniciar acciones para recuperar-restaurar, mediante copias de seguridad almacenadas en centros de contingencia dotados con las debidas medidas, cualquier archivo o sistema que haya podido resultar dañado o comprometido durante el ataque.

Consecuencias de un ciberataque

Las formas de obtener beneficios económicos de los hackers son cada vez más diversas y en función de los objetivos y el nivel de sofisticación, se emplean unas tácticas u otras.

- **Extorsión**. Cuando un hacker consigue paralizar un servicio a través del bloqueo de los servidores, es posible que pidan un rescate para liberarlo de nuevo. Además, una vez llegado a este punto, los ciberdelincuentes ya tienen muchísima información acerca de la empresa, así que la cantidad exigida la miden en función de la facturación de su víctima.
  Según datos de Incibe, el Instituto Nacional de Ciberseguridad, pagar un rescate no garantiza que los datos vayan a ser recuperados, y en muchos casos sirve a los ciberdelincuentes para pedir más de la cantidad originalmente exigida e incluso volver a atacar en el futuro, entendiendo que es una empresa que está dispuesta a pagar.

- **Venta de datos**. Otra forma de monetizar su trabajo es a través de la venta de datos. Una vez adentrados en los servidores, los ciberdelincuentes tienen acceso a la información corporativa, que pueden vender a competidores, y a la información de sus clientes -datos personales como correo, teléfono o contraseñas- que suelen ser vendidos en la Deep Web a otros delincuentes que reutilizarán esas credenciales.
  Habitualmente los datos son vendidos sin que la empresa tenga conocimiento de esta situación. Solo se entera cuando es un caso de extorsión.

- **Multa de incumplimiento**. Además, al quedar comprometidos los datos sensibles de sus clientes, las empresas quedan expuestas a graves sanciones al no haber protegido lo suficiente estos datos y vulnerar así el reglamento europeo de protección de datos GDPR.

- **Despidos IT**. Una posible consecuencia de que la empresa haya sido atacada es el despido de los responsables de la ciberseguridad. Es el caso de empresas como Prosegur, que despidió a su cúpula de ciberseguridad tras el hackeo de sus cuentas, o Innovatech, que despidió a más de 300 empleados debido a una infección masiva de ransomware.

MEDIDAS DE SEGURIDAD. INCIBE-CERT

A continuación se recogen una serie de medidas destinadas a protegernos frente a ciberataques, publicadas recientemente en la página web del INCIBE_CERT, con el objetivo de ofrecer una mejora en la protección de ciberseguridad y las mejores prácticas, aglutinamos una serie de medidas y acciones que recomendamos adoptar y revisar para proteger la información de las organizaciones, y su aplicación en los dispositivos que utilizan, así como en su presencia digital en el ciberespacio. Estas medidas están orientadas a mejorar su nivel de protección ante incidentes de ciberseguridad y, por lo tanto, minimizar su riesgo ante ciberataques que puedan afectar a la prestación de servicios de su negocio.

Fuente: https://www.incibe-cert.es/blog/medidas-ciberseguridad-perspectiva-global

Estas medidas pueden ser aplicadas, o revisadas en caso de estar ya establecidas, por cualquier organización o usuario en cualquier circunstancia que pueda considerarse necesaria en función de su contexto y necesidades propias. Su principal utilidad radica en que pueden adaptarse a las distintas características y capacidades (tanto técnicas como humanas) de las que disponga la entidad que desee ponerlas en práctica.

MEDIDAS CONCRETAS

Estas pautas de seguridad se pueden complementar con otras más específicas y concretas que pueden estar más orientadas al alcance y la actividad realizada en cada organización, pero consideramos que suponen un conjunto mínimo de medidas que recomendamos aplicar, priorizándose en cada organización en función de sus capacidades específicas:

Autenticación

- ✓ Asegurar mecanismos de autenticación de usuarios a través de la revisión y cambio de todas las contraseñas en la organización, también aquellas que son por defecto en productos y servicios. Estableciendo, de la mano de una política de concienciación general, un modelo de uso de contraseñas seguras, y para revisar su correcta aplicación, se recomiendan dos acciones: suficiente complejidad de las credenciales y cambio periódico de contraseñas. Es

importante que estas medidas sean implementadas en todas las aplicaciones y servicios en uso, y no únicamente en las cuentas de equipos de trabajo.

- ✓ Establecer medidas de concienciación a los usuarios, específicas y referidas a no reutilizar nunca las credenciales, ya que a menudo los actores de las amenazas comprometen a las organizaciones realizando ataques de relleno de credenciales (*credential stuffing*), para lo que utilizan credenciales obtenidas de filtraciones de datos anteriores contra otro servicio no relacionado.

- ✓ Resulta de especial relevancia el establecimiento de mecanismos de autenticación multifactor, a través de medidas que incluyan la utilización de elementos OTP (*One Time Password*) o similar en los accesos a sistemas de la organización, no solo accesos VPN (*Virtual Private Network*) o accesos remotos, sino también a todos los servicios y aplicaciones en la medida de lo posible.

- ✓ Aplicar, siempre que sea operativo, el principio de mínimos privilegios y evitar utilizar los equipos con privilegios de administrador, asignando a los usuarios cuentas con los permisos mínimos necesarios para operar los programas y llevar a cabo su actividad.

CERT / *Computer Emergency Response Team*. Equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

Elementos de ciberseguridad

- ✓ Mantener actualizado todo el software, priorizando las actualizaciones en aquel con vulnerabilidades conocidas y explotadas en los ciclos y mecanismos de gestión de parches establecidos en la organización para evitar la exposición a los fallos de gravedad crítica y alta lo más rápidamente posible. Esta política de actualizaciones también debe incluir los dispositivos de uso individual en la organización, como son los teléfonos corporativos.

- ✓ Monitorizar e identificar sistemas vulnerables a nuevas amenazas, mediante el uso de herramientas de análisis de vulnerabilidades, que complementen los ciclos de parcheado establecidos en la organización. Se recomienda establecer un seguimiento de las posibles amenazas y los avisos de los productos y fabricantes utilizados en la organización, así como de las notificaciones, feeds de información y avisos de CSIRT (*Computer Security Incident Response Team*) mediante boletines informativos o similares.

- ✓ Desplegar siempre que sea posible sistemas de detección y bloqueo de intrusiones (IDS/IPS, *Intrusion Detection System/Intrusion Prevention System*), y completar la implementación del mismo con otros elementos de seguridad, como un SIEM (*Security Information and Event Management*), facilitando el identificar y detectar anomalías en el tráfico para aplicar una respuesta de forma temprana, consiguiendo limitar los posibles impactos. Además, suelen tener la posibilidad de elegir 'modos de funcionamiento' en función del nivel de riesgo que se quiera asumir.

- ✓ Es muy recomendable implementar un sistema EDR (*Endpoint Detection Response*) para proteger los equipos e infraestructuras de la empresa a través de una gestión unificada de las alertas, al combinar el antivirus tradicional con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente. Asimismo, siempre que se pueda, se aconseja adoptar soluciones DLP (*Data Loss Prevention*) para prevenir las fugas de información cuyo origen está dentro de la propia organización.

- ✓ Promover un catálogo de activos de la organización, en particular resulta muy útil disponer de un listado de dispositivos utilizados por el personal que trabaja en la organización, la conectividad de red, las tecnologías empleadas en la infraestructura de la empresa, el equipamiento auxiliar, las direcciones o rangos de IP (*Internet Protocol*) expuestas a Internet. En general, todo el equipamiento hardware y software con el fin de saber lo que tiene instalado cada equipo para valorar la parte de la organización que se podría ver afectada por la nueva amenaza y las instalaciones donde se alojan los equipos más relevantes para la organización.

- ✓ Sería deseable disponer de un programa de auditorías internas y externas realizadas por entidades independientes, que les permitan validar su SGSI y análisis de riesgos y, en último término, certificarlo mediante la correspondiente auditoría de certificación.

Redes y sistemas

- ✓ Es altamente recomendable el desarrollo e implementación de un PCN (Plan de Continuidad de Negocio) para analizar el posible impacto en el negocio, elaborar planes operativos de recuperación y ejecutar periódicamente pruebas de validación del propio PCN. Asimismo, también lo es mantener, revisar y probar planes de contingencia.

- ✓ La cadena de suministro podría ser atacada y afectar a nuestra organización (*supply chain attack*) mediante el compromiso de los proveedores de nuestros servicios externalizados. Por eso, es recomendable revisar los accesos establecidos para los proveedores y dependencias con sus sistemas y sus redes, como medida de seguridad para prevenir este tipo de incidentes, en caso de que un tercero con el que se colabora pueda ser utilizado como vector de entrada en la organización. Los proveedores externos deberán contar con estándares mínimos de seguridad, acordes con la política de seguridad de la organización.

- ✓ Implementar y desarrollar un nivel de segmentación óptimo de las diferentes redes utilizadas, que debería incorporar redes aisladas con reglas de firewall adecuadas, diodos de datos (sólo permiten el tráfico en una dirección), dispositivos IDS y una red DMZ (*DeMilitarized Zone*) para separar la red corporativa de la red de datos. Adicionalmente, revisar las políticas de filtrado y tráfico entre las mismas para limitar el acceso y utilizar atributos adicionales en las comunicaciones entre las aplicaciones y servicios.

- ✓ Es recomendable la fortificación y bastionado de sistemas expuestos, en entornos críticos, DMZ o en entornos en la nube (*cloud*), incrementando las medidas de seguridad en los mismos (*hardening*) y aplicando los controles de seguridad, segmentación, políticas de mínimo privilegio de acceso, y bloqueos en los entornos de menor confianza, para evitar que un ciberataque pueda propagarse en los distintos entornos de su organización.

- ✓ Se aconseja revisar y comprobar la estrategia de copias de seguridad de la organización, prestando especial atención a los diferentes medios utilizados, tanto para las locales como para la copia remota fuera de sus instalaciones, revisando las estrategias de continuidad de negocio, y de recuperación ante desastres, que permitan recuperar la actividad en caso de pérdida o indisponibilidad de la información. Es importante que estas medidas se prueben periódicamente. Una buena práctica a la hora de realizar copias de seguridad es adoptar la estrategia 3-2-1, que se basa en diversificar las copias de seguridad para garantizar que siempre haya alguna recuperable. Sus claves de actuación son las siguientes:

Mantener 3 copias de cualquier fichero importante (el archivo original y dos *backups*).

Almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos.

Almacenar 1 copia de seguridad fuera de nuestra empresa (*backup offsite*), por ejemplo en la nube.

- ✓ Para minimizar los posibles incidentes de DoS/DDoS (*Denial of Service/Destributed Denial of Service*), es recomendable para los elementos que requieran una alta disponibilidad, el disponer de un servicio de CDN (*Content Delivery Network*), o al menos tener activas las medidas específicas de balanceo de carga y configurar los umbrales de conexiones en ellos. Algunas recomendaciones de seguridad a aplicar en el uso de CDN son:

  Configurar SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) en la conexión entre el usuario y el CDN.

  Activar la utilización de HSTS (*HTTP Strict Transport Security*) para proteger servidores HTTPS (*HyperText Transfer Protocol Secure*) contra ataques de degradación.

  Cambiar la dirección IP original asociada al servidor.

  Establecer límites de conexiones para proteger el sitio web ante ataques DoS e intentos de inicio de sesión por fuerza bruta.

  Alojar el correo en un servidor diferente para evitar que un atacante pudiese encontrar la dirección IP en un correo electrónico saliente.

  Evitar los motores de búsqueda de servicios.

- ✓ A la hora de configurar un servidor web, además de firewall, es aconsejable instalar un WAF (*Web Application Firewall*), especializado en controlar las conexiones, filtrarlas, monitorizarlas y bloquearlas en el caso de que consideren maliciosas. Además de bloquear ataques de denegación de servicio (DoS), los WAF también son capaces de detectar y bloquear ataques como XSS (*Cross-Site Scripting*) o inyección SQL.

Correo electrónico y concienciación

- ✓ Debido al uso extendido de correo electrónico en las organizaciones, se recomienda aplicar políticas de protección y medidas como protocolos SPF/DKIM/DMARC (*Sender Policy Framework/DomainKeys Identified Mail/Domain-based Message Authentication, Reporting and Conformance*), medidas antispam y en especial reglas para los intentos de *phishing* y suplantaciones de identidad, como por ejemplo el fraude del CEO, *spear phishing* (una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas, en el que los atacantes intentan, mediante un correo electrónico, conseguir información confidencial de la víctima) o BEC (*Bussines Email Compromise*), que consiste en una técnica llevada a cabo por los ciberdelincuentes para robar fondos de las empresas suplantando la identidad de un alto directivo.

- ✓ Iniciar, mantener o potenciar las políticas de concienciación y formación a sus empleados, que les ayuden a identificar y protegerse de amenazas dirigidas, y a aplicar las mejores prácticas de seguridad en el uso de la tecnología. También se pueden poner a prueba las lecciones aprendidas con la organización de ciberejercicios.

La aplicación de este conjunto de medidas, ampliables y adaptables según el ámbito de actuación y las capacidades de cada organización que las quiera poner en práctica, debe realizarse de forma gradual. Muchas veces requieren de soluciones tecnológicas complejas, con implicaciones en procedimientos que alargan inevitablemente el proceso. Por ello, lo ideal es tener muy en cuenta los tiempos de implementación y ejecución de las mismas, siendo conscientes de la inversión de esfuerzos que deberá realizarse.

MEDIDAS DE SEGURIDAD EN LAS EMPRESAS

Recientemente, la empresa de tecnología Cisco ha publicado una encuesta de los resultados obtenidos en cinco países, entre ellos España, sobre diversos aspectos de la ciberseguridad, que han sido publicados en diversos medios:

https://news-blogs.cisco.com/emear/es/2022/04/28/uno-de-cada-tres-trabajadores-espanoles-creen-que-la-seguridad-merma-su-productividad/

"Los trabajadores españoles se saltan las medidas de ciberseguridad Seguridad". Así lo admiten el 80% de las personas consultadas. "Lo hacen para cumplir con sus tareas y es un acto que se repite de media 14 veces al mes".

Las medidas de seguridad restan productividad. Así lo consideran un 34% de trabajadores españoles, quienes afirman que la estrategia de ciberseguridad de su compañía ofrece una mala experiencia de usuario en términos de complejidad y consumo de tiempo.

Los consultados en España se quejan de dedicar 15 minutos de media al día a cumplir con las medidas impuestas, como insertar contraseñas, autenticarse mediante códigos o usar gestores de claves (un minuto más que la media en EMEAR).

Estas son algunas de las principales conclusiones de un nuevo estudio de Cisco realizado en cinco países de EMEAR incluido España. Según el informe, la ciberseguridad aún está lejos de ser prioritaria para los trabajadores españoles. Ocho de cada diez consultados en España admiten saltarse los controles de seguridad de su empresa con mayor o menor frecuencia para poder cumplir con sus tareas, un acto que se repite de media 14 veces al mes.

Figura 36. Informe sobre ciberseguridad de CISCO.

Falta de confianza

Trabajadores de múltiples sectores y de empresas españolas de todos los tamaños (desde 1 a más de 500 empleados) no confían en las soluciones de protección corporativas, y esta falta de confianza está aumentando con el teletrabajo generalizado por la pandemia.

- El 30% de empleados españoles consideran que su empresa no se toma la ciberseguridad lo suficientemente en serio.
- Una cuarta parte de los consultados no confían en que su organización les mantenga seguros, y el 35% afirman que esta situación ha empeorado desde la instauración del trabajo híbrido.
- Casi tres de cada diez (el 28%) tampoco confían en que su empresa respete la protección de sus datos personales una vez que abandonan la compañía.

Malas prácticas

Aunque el 66% de los consultados en España consideran sencillo cumplir con su trabajo de manera segura, el 34% restante creen que la experiencia con las medidas de seguridad adoptadas es compleja (15%), que obstaculiza sus tareas (10%) o que resulta innecesaria al suponer una pérdida de tiempo (9%).

Los usuarios que no confían en la estrategia de ciberseguridad de su empresa buscan sus propias soluciones alternativas, contribuyendo así a incrementar malas prácticas como instalar software no autorizado o escribir sus contraseñas.

- Casi uno de cada cinco empleados españoles (el 17%) optan por utilizar la misma contraseña para varias cuentas y aplicaciones, mientras el 16% las escriben en papel, poniendo en riesgo la red y los dispositivos de su empresa.
- Sólo el 18% afirman utilizar un gestor de contraseñas seguro para sus aplicaciones y servicios en línea, y únicamente el 12% se apoyan en la autenticación sin contraseñas (como huella dactilar o reconocimiento facial en el smartphone).

Soluciones empleadas

Con respecto a las soluciones de protección de acceso utilizadas por las empresas, la VPN (*Virtual Private Network*) es la opción más extendida (53%), seguida de la autenticación multifactor (41%) y los recursos internos para detectar intentos de phising y otros incidentes (43%). Curiosamente, sólo cuatro de cada diez trabajadores consultados en España (el 39%) afirman que su organización ofrece mecanismos de *Single Sign On* (una única contraseña para acceder a todas las aplicaciones y datos corporativos).

No obstante, aunque los trabajadores españoles se resisten a recordar las contraseñas, la gran mayoría están dispuestos a iniciar sesión mediante el reconocimiento dactilar (75%) o facial (51%), reflejando la creciente opción de métodos de autenticación biométrica.

"Con el aumento del trabajo híbrido, los empleados operan cada vez más desde entornos no controlados, utilizando redes públicas y privadas y múltiples dispositivos", destaca Ángel Ortiz, ingeniero de Telecomunicación y director de Ciberseguridad en Cisco España. "Para garantizar la protección, las empresas deben centrarse tanto en la concienciación de los trabajadores como en la elección de tecnologías de seguridad integradas y que ofrezcan una experiencia de uso sencilla que no afecte al rendimiento ni a la productividad".

Recomendaciones de Cisco

Para que las organizaciones puedan optimizar la protección de los trabajadores híbridos, Cisco recomienda:

- Formar al personal y fomentar una cultura de ciberseguridad.
- Implementar la autenticación multifactor (MFA) como un paso fundamental hacia Zero Trust.
- Considerar un enfoque SASE (*Secure Access Service Edge*) para proteger el acceso a las aplicaciones y mantener la seguridad del entorno dondequiera que se encuentren los usuarios.
- Blindar el correo electrónico frente a amenazas avanzadas (trasladar el e-mail a la nube proporciona comodidad y escalabilidad, pero también implica un mayor riesgo de malware).
- Mantener una primera y una última línea de defensa con DNS y seguridad de los terminales.

NORMATIVA DE CIBERSEGURIDAD

¿Cómo se articula la legislación sobre ciberseguridad? ¿Cómo afecta esta normativa a las empresa? ¿Cuáles son las principales medidas de seguridad informática?

Internet y la aparición de nuevas tecnologías ha originado la aparición de nuevas modalidades de delitos e infracciones a las normas que ni siquiera estaban previstas. Por tanto, es necesario que las diferentes leyes existentes se adapten para regular y proteger a ciudadanos y empresas de todos estos ataques cibernéticos en la medida de lo posible. Y que se establezcan nuevas normativas que regulan las situaciones nuevas, no previstas hasta ahora en el mundo físico.

La ciberseguridad abarca muchas materias relacionadas con el derecho penal, civil, la protección del honor o la intimidad, entre otros, que se aplicarían no solo en el mundo virtual, sino en el real. Lo que hay que tener en cuenta es la vertiente online en la que se producen esas actuaciones ilegales o ilícitas, y el impacto que se deriva del hecho que se produzcan en el mundo digital.

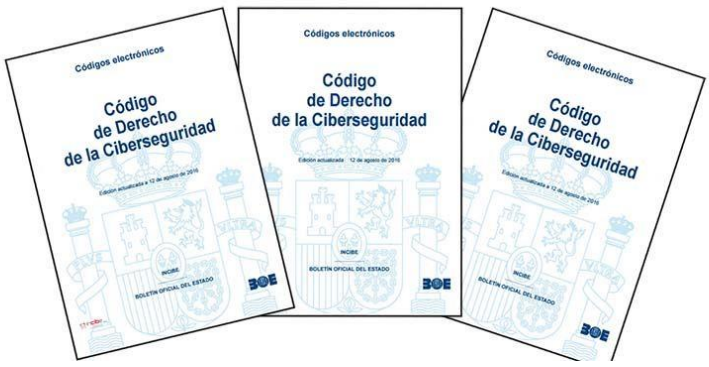


Figura 37. Código de Derecho de la Ciberseguridad. Accesible en: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=2

Publicado por primera vez el 9 de Agosto de 2016, el Código del Derecho de la Ciberseguridad es un iniciativa conjunta del Instituto Nacional de Ciberseguridad (INCIBE) y el Boletín Oficial del Estado (BOE) que pone a disposición de todos los profesionales del Derecho, en un compendio de normas, el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimiento en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado.

La última versión, actualizada, a día 31 de marzo de 2022, introduce estos cambios:

> Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información por inclusión de las diferentes normas.
>
> Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.
>
> Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.

Diferentes códigos electrónicos relacionados con la ciberseguridad se pueden obtener/descargar del BOE, por ejemplo "Ámbitos de la Seguridad Nacional: Ciberseguridad" en el siguiente enlace: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=397_Ambitos_de_la_Seguridad_Nacional_Ciberseguridad&modo=2

NORMATIVA DE CIBERSEGURIDAD EN EUROPA

La normativa europea de ciberseguridad se rige por las siguientes leyes:

> Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información de la Unión.
>
> Esta Directiva dispone de un par de artículos relacionados con la seguridad de las redes y sistemas de información para los operadores de servicios esenciales y para los proveedores de servicios digitales.
>
> De este modo, se establece en el artículo 14 que "Los Estados miembros velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado."
>
> Es decir, los Estados miembros velarán para que se cumpla con las medidas proporcionadas o adecuadas al riesgo planteado. Y también para que se adopten medidas a efectos de minimizar, reducir o prevenir incidentes que afecten a la seguridad.
>
> Así mismo, también se deberá notificar sin dilación indebida a la autoridad competente o al CSIRT (*Computer Security Incident Response Teams*) los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que se presten para que se puedan tomar medidas con carácter institucional o nacional al respecto, en su caso.
>
> También en el artículo 16 se establece el deber del Estado para que los proveedores de servicios digitales determinen y adopten medidas de seguridad técnicas, organizativas y proporcionadas para gestionar los riesgos existentes a la seguridad de las redes y sistemas de información que se utilizan. Por ello, deben adoptar medidas con relación a la seguridad

de sistemas e instalaciones, gestión de incidentes, gestión de la continuidad de las actividades, supervisión, auditorías y pruebas y cumplimiento de normas internacionales.

Sin embargo, en diciembre de 2020, la Comisión Europea propuso una revisión de la Directiva SRI (SRI 2) para sustituir a la Directiva de 2016 y dar respuesta a la evolución de las amenazas, teniendo en cuenta la transformación digital, acelerada por la crisis del COVID-19.

El Consejo llegó a una orientación general sobre la nueva Directiva en diciembre de 2021. Una vez adoptada, la nueva Directiva (SRI2), sustituirá a la de 2016 a fin de "seguir mejorando la resiliencia y las capacidades de respuesta ante incidentes tanto del sector público como del privado y de la UE en su conjunto".

Y, además, en junio de 2019 entró en vigor el Reglamento de Ciberseguridad de la UE, e introdujo:

- ✓ Un sistema de certificación para toda la Unión Europea,
- ✓ Un mandato nuevo y reforzado para la Agencia para la Ciberseguridad.

Gracias a este, la UE ha implantado un marco único de certificación a escala de la UE que generará confianza, aumentará el crecimiento del mercado de la ciberseguridad y facilitará el comercio en toda la UE.

Reglamento Europeo de Protección de Datos 2016/679 (RGPD). Establece la implantación de nuevas medidas de seguridad para las empresas europeas, los autónomos y la Administración pública.

Figura 38. Calendario sobre Ciberseguridad en la UE.

Ley de Seguridad Cibernética (*Cybersecurity Act*), aprobada el 27 de junio de 2019 por la UE. Esta ley moderniza y refuerza la Agencia de la UE para la ciberseguridad (ENISA) y establece un marco de certificación de la ciberseguridad en toda la UE para productos, servicios y procesos digitales.

Así, el 16 de diciembre de 2020 se presentó la nueva estrategia de Ciberseguridad de la Unión Europea para lograr reforzar la resiliencia colectiva de Europa frente a las ciberamenazas y garantizar, así, que la ciudadanía y empresas puedan beneficiarse completamente de los servicios y herramientas digitales de manera fiable. Y obviamente, poder confiar en todos los dispositivos conectados a la red en los hogares, oficinas y fábricas (los *IoT devices*).

En 2020, el número de ciberataques ha sido más alto que nunca y han sido más sofisticados. Por lo que se ha detectado, provienen tanto de dentro como de fuera de la Unión Europea. Y por eso, la UE desea liderar los esfuerzos para conseguir una digitalización segura.

Normativa de ciberseguridad en España

En nuestro país existe un Código de Derecho de la Ciberseguridad, publicado en el Boletín Oficial del Estado, que cita las principales normas a tener en cuenta con relación a la protección del ciberespacio. Este código hace referencia a las siguientes leyes sobre ciberseguridad. Accesible en: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=2

Normativas de seguridad nacional

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Este RD actualiza el ENS y se enmarca en el paquete de actuaciones urgentes, adoptado el 25 de mayo de 2021, para reforzar las capacidades de defensa frente a las ciberamenazas sobre el sector público y las entidades colaboradoras que suministran tecnologías y servicios al mismo. Con ello se deroga el Real Decreto 3/2010, de 8 de enero, que hasta ahora regulaba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Entre las nuevas medidas, se han incluido las relativas a servicios en la nube, interconexión de sistemas, protección de la cadena de suministro, medios alternativos, vigilancia y otros dispositivos conectados a la red.

Objetivos del Esquema Nacional de Seguridad

1. Mejorar y alinear el ENS con el marco legal y estratégico actual para facilitar la seguridad de la administración digital.
2. Introducir la capacidad de ajustar los requisitos del ENS a determinados colectivos o ámbitos tecnológicos.
3. Revisar de forma pormenorizada principios básicos, requisitos mínimos y medidas de seguridad.
4. Incorporar un nuevo sistema de codificación de los requisitos de las medidas basadas en refuerzos alineados con el nivel de seguridad perseguido.

Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional.

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que regula los principios y organismos clave así como las funciones a desempeñar para la defensa de la Seguridad Nacional.

Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

Normativas de seguridad

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

Ley 5/2014, de 4 de abril, de Seguridad Privada.

Referidas a las telecomunicaciones

Ley 34/2002, de 11 de julio, de Servicios a la Sociedad de la Información y Comercio Electrónico.

Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.

Ley 50/2003, de 19 de diciembre, de Firma Electrónica.

Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Real Decreto-ley 7/2022, de 29 de marzo, que establece requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología 5G.

> La aprobación de la llamada «Ley de Ciberseguridad 5G» (con la que identifica este real decreto-ley) está incluida como una de las reformas (Reforma C15R2) de la Componente 15 del Plan de Recuperación, Transformación y Resiliencia dedicado a «Conectividad digital, impulso de la ciberseguridad y despliegue del 5G», estando, en concreto, prevista como Hito CID 235 «la entrada en vigor de la Ley de Ciberseguridad 5G».

Todas esas leyes relacionadas con la seguridad de la información están diseñadas con el objetivo de ofrecer un marco normativo que permita garantizar la seguridad de la información digital y establecer una legislación común a nivel europeo.

Sobre la ciberdelincuencia

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

Real Decreto de 14 de septiembre de 1882 aprobatorio de la Ley de Enjuiciamiento Criminal.

Normativa de protección de datos y privacidad

El marco legal para la protección de datos personales en España está regulado por el Tratado de Lisboa; Artículo 18, apartado 4, de la Constitución española; el RGPD y la Ley de Protección de Datos Española. Esto es bastante importante para los autores científico-técnicos y académicos, agrupados en ACTA.

> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 06/12/2018.

La normativa sectorial también puede contener disposiciones de protección de datos, como la Ley 34/2002 de Comercio Electrónico (LSSI), la Ley General de Telecomunicaciones 9/2014 (GTL), la legislación contra el blanqueo de capitales, la regulación financiera o la normativa sobre historias clínicas. o investigación biomédica. Sin embargo, generalmente se refieren a la

antigua normativa española de protección de datos y, ahora que el RGPD y la Ley de Protección de Datos española están en vigor, serán objeto de revisión o al menos deberán reinterpretarse de acuerdo con la nueva normativa.

Los derechos de privacidad están regulados principalmente por la Constitución española, la Ley 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen de la persona física, y por el Código Penal español.

Los datos personales y los datos privados no son sinónimos. Los datos personales son cualquier tipo de información (alfanumérica, gráfica, fotográfica, acústica, etc.) relativa a una persona física identificada o identificable, con independencia de que esta información sea privada o no. Sin embargo, los datos sobre menores, opiniones políticas, afiliación sindical, religión o creencias filosóficas, origen racial o étnico, datos genéticos, datos biométricos, salud, delitos, y orientación sexual se consideran más sensibles y requieren una protección específica.

Ley sobre la seguridad de las redes y sistemas de información

El Real Decreto 43/2021, de 28 de enero, supone el desarrollo efectivo del RD-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, transposición de la Directiva europea (UE) 2016/1148 de ciberseguridad (Directiva NIS), del Parlamento Europeo y del Consejo conocida como "Directiva europea sobre ciberseguridad", en armonización de la normativa nacional vigente de aplicación con el Derecho comunitario. La Directiva NIS busca mejorar la seguridad de las redes y sistemas de información en su territorio y entró en vigor en agosto de 2017.

Su ámbito de aplicación incluye a las empresas de servicios esenciales, del mantenimiento de las funciones sociales básicas y las que velan por el bienestar social y económico de las personas. Tendrán que cumplirla los proveedores de servicios digitales, que manejan datos sensibles.

Principales medidas Directiva NIS (***Security of Network and Information Systems***)

El objetivo principal de la Directiva NIS es lograr un elevado nivel común de las redes y sistemas de información dentro de la Unión Europea. Establece cinco medidas concretas:

1. Todos los estados miembros estarán obligados a adoptar una estrategia nacional de seguridad de las redes y sistemas de información. Una gran heterogeneidad entre países ha llevado a planteamientos fragmentados, generando desigualdades en la protección de consumidores y empresas y comprometiendo la seguridad de la UE a nivel general.
2. Se creará un grupo de cooperación con el objetivo de formular una estrategia común y de permitir el intercambio de información entre los estados miembros.
3. Se creará una red de Equipos de Respuesta a Incidentes de Seguridad Informática (red CSIRT) que ayude a constituir una cooperación más rápida y eficaz y a que se forme un clima de confianza entre los distintos países.
4. Se establecerán condiciones de seguridad para operadores de servicios esenciales y de servicios digitales. Por operador de servicios esenciales se entiende a cualquier entidad pública o privada que preste un servicio dependiente de redes y sistemas de información para el mantenimiento de actividades sociales o económicas. Estas entidades pueden pertenecer a distintos sectores como el energético, bancario o sanitario. En cuanto a los proveedores de servicios digitales, se refiere a toda persona jurídica que preste un servicio digital.

5. Las autoridades nacionales de cada estado miembro tendrán obligaciones en todas las tareas relacionadas con la seguridad de redes y sistemas de información.

Figura 39. RD 43/2021 sobre ciberseguridad.

El objetivo perseguido con este nuevo Real Decreto sigue siendo el de aumentar la protección frente a ataques y vulneraciones en las redes y sistemas de información, bajo el marco normativo de la Unión Europea. Para ello, la red CSIRT, como red de Equipos de Respuesta de Incidentes de Seguridad Informática, cuenta con el apoyo de un grupo de cooperación estratégica. Este último se encarga de intermediar en el intercambio de información y provee de soporte experto a los Estados miembros en lo relativo a sus estrategias de mejora de la capacidad técnica y organizativa en materia de ciberseguridad. El objetivo es tratar de gestionar riesgos de forma conjunta, discutir problemas de seguridad transfronterizos e idear respuestas coordinadas.

Esta Ley de seguridad de la información identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan dichos servicios. La normativa de seguridad informática se aplica a los operadores de servicios esenciales.

PLAN NACIONAL DE CIBERSEGURIDAD

El Consejo de Ministros aprobó el martes 29 de marzo de 2022 el Plan Nacional de Ciberseguridad, con lo que cumple el mandato emitido por el Consejo de Seguridad Nacional y desarrolla la Estrategia Nacional de Ciberseguridad 2019. El plan, coordinado por el Departamento de Seguridad Nacional de la Presidencia del Gobierno, prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Con este acuerdo y el real decreto-ley de seguridad en las comunicaciones 5G aprobado, el Gobierno refuerza la ciberseguridad, en el marco del Plan Nacional de Respuesta a las Consecuencias Económicas y Sociales de la Guerra en Ucrania, con el fin de intensificar la vigilancia y apuntalar las capacidades de planificación, preparación, detección y respuesta en el ciberespacio.

Entre las principales actuaciones del Plan Nacional de Ciberseguridad, dotado con un presupuesto de 1.200 millones de euros, destacan:

- La creación de la plataforma nacional de notificación y seguimiento de ciberincidentes y de amenazas que permita intercambiar información, en tiempo real, entre organismos públicos y privados.
- Impulsar la puesta en marcha del Centro de Operaciones de Ciberseguridad (COCS) de la Administración General del Estado y sus Organismos Públicos.
- El desarrollo de un sistema integrado de indicadores de ciberseguridad a nivel nacional.

- Incrementar la creación de infraestructuras de ciberseguridad en las comunidades y ciudades autónomas y las entidades locales.
- Impulsar la ciberseguridad de pymes, micropymes y autónomos.
- Promover un mayor nivel de cultura de ciberseguridad.

Además, el plan prevé la creación de un sistema de seguimiento y control, con el fin de poder identificar el grado de ejecución de las medidas y emitir un informe anual de evaluación.

Ley de Ciberseguridad 5G

El marco legal para la protección de datos personales en España está regulado por el Tratado de Lisboa; Artículo 18, apartado 4, de la Constitución española; el Reglamento General de Protección de Datos (RGPD), Ley Orgánica de Protección de Datos Española (LOPD), Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) y Ley de Propiedad Intelectual (LPI).

La aprobación de la Ley de Ciberseguridad 5G por parte del Gobierno, que estaba prevista para la segunda mitad del año 2022 pero que el Ejecutivo ha acelerado a través de un real decreto ley debido al conflicto de la guerra Ucrania-Rusia, permitirá el impulso y la implantación definitiva de las redes de quinta generación (5G) en España.

En este sentido, el Ejecutivo ha decidido acelerar la aprobación de esta norma porque, según explica en el texto del Real Decreto, "el conflicto (invasión rusa de Ucrania) está provocando importantes implicaciones para la Unión Europea, entre las que se encuentra el incremento considerable del riesgo de ciberataques por motivos geoestratégicos" y ya se han registrado importantes ataques a servicios gubernamentales en Ucrania y se han emitido alertas internacionales que "destacan la necesidad de reforzar la protección de los países europeos frente a posibles ciberamenazas".

Respecto a los riesgos de ciberseguridad, las autoridades europeas observan que el 5G aumentará la exposición a los ciberataques. Y ello es así porque, teniendo en cuenta que las redes se basan cada vez más en programas informáticos, habrá más fallos de seguridad en los sistemas que podrán ser explotados por los ciberdelincuentes.

La nueva normativa sobre 5G se enmarca dentro del Plan Nacional para responder al impacto económico y social de la invasión de Ucrania, que también ha incluido la aprobación del Plan Nacional de Ciberseguridad con una dotación de 1.200 millones de euros (200 más de los previstos) y un paquete de 150 iniciativas.

El Real Decreto Ley de Ciberseguridad 5G es la llave para el despliegue del 5G en todo el territorio, esta tecnología revolucionará no solo el mundo de las telecomunicaciones sino todo el tejido empresarial a través de la creación de nuevos servicios y modelos de negocio.

Figura 40. Fuente: https://www.lamoncloa.gob.es

El Real Decreto-ley 7/2022, de 29 de marzo establece normas especiales o adicionales a las existentes en otras leyes aplicables en materia de seguridad, incluidas la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, la Ley 36/2015, de 28 de septiembre, de seguridad nacional, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (Reglamento general de protección de datos personales), la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, o el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

El decreto-ley con la nueva norma sobre ciberseguridad en las redes 5G establece un mecanismo claro que prohibirá instalar en las redes equipos de grupos de "alto riesgo", que faciliten el ciberespionaje. La Ley de Ciberseguridad 5G obliga a las operadoras a retirar los equipos de ciertas marcas de los puntos críticos de la red, y cualquier elemento fabricado por ellas en zonas sensibles del país. El objetivo es blindar la seguridad de las redes 5G, en vista de que en el futuro se convertirán en un elemento esencial para el funcionamiento de la economía y la sociedad en un entorno fuertemente digitalizado.

Figura 41. Huawei, un fabricante en el punto de mira.

Un punto destacado de la nueva legislación es que se incluye una lista de calificación de riesgo para proveedores, que se determinará en un plazo de tres meses, según el nivel de seguridad y fiabilidad de sus equipos y establece una serie de controles para los operadores que deben aplicar en sus redes.

Según un estudio recientemente publicado por la consultora Dell'Oro (https://www.delloro.com), los principales proveedores de telecomunicaciones y redes a nivel global son Huawei, con una cuota de mercado del 28,7%, Ericsson con un 15% y Nokia con un 14,9%.

El acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como "suministradores de alto riesgo" determinará el plazo en que lo operadores 5G deberán llevar a cabo la sustitución de los equipos, productos y servicios proporcionados por dicho suministrador en la red y servicios del operador 5G, cuando ello fuera necesario, para lo cual deberá tener en cuenta la situación del mercado de los suministradores, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G y en función de cuáles son en concreto los elementos críticos afectados, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, la migración de las redes 5G no autónomas a autónomas, así como su impacto económico, si bien, en ningún caso, este plazo podrá ser inferior a un año.

Los suministradores de alto riesgo cuyos equipos de telecomunicación, hardware, software o servicios auxiliares proporcionados sean utilizados única y exclusivamente en redes privadas 5G o para la prestación de servicios 5G en régimen de autoprestación son calificados como suministradores de riesgo medio.

Las administraciones públicas deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G. En particular, las administraciones públicas que quieran llevar a cabo la instalación, despliegue y explotación de redes 5G, ya sean públicas o privadas, o la prestación de servicios 5G, disponibles al público o en autoprestación, no podrán, por razones de seguridad nacional, utilizar equipos, productos y servicios proporcionados por suministradores de alto riesgo o riesgo medio.

Estas compañías son las que proporcionan las infraestructuras de redes y 5G a los principales operadores del país, que son los que han estado estos últimos años acometiendo todas las inversiones para el despliegue de redes de quinta generación.

Además, otro de los puntos que se incluyen en la normativa es que los operadores tendrán que implantar una estrategia de diversificación de proveedores para minimizar los riesgos con, al menos, dos proveedores por red.

Con la aprobación de este decreto ley se da luz verde a todo el sector de cara al despliegue del 5G en España. El único gran punto que queda pendiente en la agenda del Gobierno es la subasta de 26 GHz, que se considera "prioritaria" para el desarrollo de esta tecnología y que está prevista para el segundo semestre del año.

La tecnología 5G y la ciberseguridad

La tecnología 5G tiene el potencial de impulsar el mercado de consumo y empresarial, aportando una serie de beneficios como altas velocidades, menor latencia y más ancho de banda. La quinta generación de estándares móviles también allana el camino para mejorar ámbitos como la atención sanitaria, el transporte con vehículos autónomos o las ciudades inteligentes que ofrecen nuevos usos y mejoran la vida cotidiana. De ello son conscientes las empresas de telecomunicaciones que son optimistas ante la oportunidad que representa, según una investigación de Fortinet, llevada a cabo por TelecomTV en colaboración con HardenStance y ETSI: *White Paper: 5G SA Networks Trigger a New Era in 5G Security.* Descarga: https://www.hardenstance.com/wp-content/uploads/2020/10/A-New-Era-in-Stand-Alone-SA-5G-Security-FINAL.pdf

Figura 42. Nueva tecnología-Nuevos riesgos. Fuente: https://www.itdigitalsecurity.es

Según este trabajo, los operadores podrían llegar a captar el 75% del negocio 5G, pero para lograr estos beneficios será fundamental aumentar la seguridad existente -tanto en términos de arquitectura como de operaciones-, así como adaptar las soluciones a casos de uso empresarial específicos que son críticos o muy importantes para casi tres cuartas partes de los encuestados, especialmente en los mercados verticales clave del transporte, la logística, la automatización, la fabricación y la atención sanitaria. Así piensan un 64% de los encuestados.

El estudio subraya que los operadores de redes móviles y las empresas deben adoptar "una estrategia de ciberseguridad fuerte que proteja toda su infraestructura, desde el núcleo móvil hasta el perímetro".

Figura 43. Nueva tecnología implica nuevos riesgos. Fuente: https://www.segurilatam.com

La explotación de vulnerabilidades en servicios de conectividad remota, a través de Internet o redes móviles, se ha convertido en el método más exitoso de acceso inicial a una red. Con 5G, señalan los autores, el antiguo modelo de negocio basado en proporcionar servicios de conectividad móvil indiferenciados ya no será suficiente. Para tener éxito, deberán establecerse acuerdos de responsabilidad compartida con otros proveedores, así como con sus clientes empresariales.

Estas conclusiones van en línea con la división de responsabilidades existente entre los proveedores cloud y sus empresas clientes, en la que el mantenimiento y la seguridad de la infraestructura recae en el proveedor, mientras que la empresa se encarga de asegurar sus propios datos y aplicaciones, repartiéndose así la responsabilidad entre ambos.

Figura 44. Certificación para redes 5G.Fuente: ENISA.

Mencionar que la Comisión Europea ha encomendado a la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés *European Union Agency for Cybersecurity*) la elaboración del esquema de certificación de ciberseguridad de la UE para las redes 5G que ayudará a abordar los riesgos relacionados con las vulnerabilidades técnicas y mejorar su seguridad. El sistema de certificación de ciberseguridad 5G contribuirá a abordar los riesgos relacionados con las vulnerabilidades técnicas.

Reglamento de Privacidad (RGPD)

Cuando las organizaciones escuchan la palabra privacidad, pueden pensar en el Reglamento General de Protección de Datos (RGPD) y en Europa. En otras palabras, si una organización no hace negocios en Europa, entonces la regulación de privacidad no es una preocupación y no es aplicable. Históricamente, esa mentalidad no estaba del todo equivocada, sin embargo, la regulación que rodea el panorama de la privacidad cambia continuamente y las empresas deben garantizar que la privacidad siga siendo una consideración principal en 2022.

El Parlamento Europeo adoptó el RGPD en abril de 2016 y entró en vigor el 25 de mayo de 2018, reemplazando una directiva de protección de datos desactualizada de 1995. El RGPD trae disposiciones que requieren que las empresas protejan los datos personales y la privacidad de los ciudadanos de la UE para las transacciones que ocurren dentro de los estados miembros de la UE. El RGPD también regula la exportación de datos personales fuera de la UE.

Aunque se habían establecido otras leyes y reglamentos antes del RGPD, el RGPD mejoró significativamente el control de una persona sobre la recopilación y el uso de sus datos personales, así como las sanciones financieras por incumplimiento. Esta ley se ha redactado para proteger los derechos de los ciudadanos de la Unión Europea. Por tanto, es de obligado cumplimiento para cualquier empresa que trate datos de ciudadanos europeos. Independientemente de la nacionalidad de la empresa. Eso quiere decir que empresas como Amazon, Facebook o Google también deben cumplirla, y así, en 2021, Amazon recibió una multa de casi 1.000 millones de dólares por violaciones de protección de datos GDPR denunciadas.

Figura 45. El RGPD entró en vigor el 25 de mayo de 2018.

Si bien el enfoque de la privacidad se asoció anteriormente con Europa y el RGPD, desde entonces, otros países y estados han adoptado sus propias regulaciones de privacidad. Las organizaciones que históricamente se han sentido cómodas con el hecho de que no hacen negocios en Europa deben reconsiderar su posición. Las organizaciones deben prepararse para un mayor escrutinio y regulación en torno a la privacidad.

Si bien EE. UU. aún no ha adoptado una regulación de privacidad similar a GDPR, las organizaciones deben prepararse ahora mediante la adopción de un marco de control de privacidad sólido, como GDPR o CCPA, y luego hacer ajustes cuando entren en juego diferentes regulaciones estatales o quizás federales.

Ciberseguridad y RGPD

En 2018 entró en vigor una nueva ley sobre la protección de datos. Ésta, más conocida como Reglamento General de Protección de Datos (RGDP), obliga desde entonces a todos los blogs y sitios web que quieran recopilar datos e información personal de terceros, a informar a los usuarios de dicha recopilación y a pedirles permiso para ello. Sin su consentimiento no se pueden recopilar ni utilizar sus datos para fines comerciales. Estos datos sólo pueden ser utilizados por la empresa que los ha recopilado, que es quién tiene el consentimiento para usarlos. En caso de que un tercero no autorizado los utilice, está vulnerando la ley de protección de datos.

Figura 46. Objetivos del RGPD. Fuente: https://www.xplora.eu

A los ciberdelincuentes lo que les interesa son los datos de terceros para comprometer a la empresa y conseguir una compensación económica para su recuperación. Saben que para las empresas los datos son su punto más débil, puesto que su pérdida puede dañar su imagen y reputación de marca, y por tanto, estarían dispuestos a cualquier cosa para recuperarlos.

La fuga de datos y su pérdida, es un incumplimiento del Reglamento de Protección de Datos. Puede parecer que si la empresa es ciberatacada, no es culpa suya y que, por tanto, no tendría que pagar las consecuencias de la pérdida de datos. No obstante, ante la ley, cualquier empresa está obligada a contar con soluciones de ciberseguridad para evitar este tipo de incidentes y establecer una estrategia de ciberseguridad y soluciones de seguridad informática que le ayuden a impedir la entrada de malware en sus dominios (sistema e infraestructura IT).

Protección de los smartphones

Los teléfonos móviles, en concreto los smartphones, de los que ya hay más de 3.800 millones en el mundo según Statista (https://es.statista.com), son ya la principal vía de entrada en los ciberataques corporativos en nuestro país. Según un estudio de la aseguradora Hiscox, el 41% de los ciberataques que sufren las empresas españolas se produce a través del móvil, un 22% a través de los teléfonos corporativos y el 19% desde teléfonos personales. El mal uso de los smartphones se ha vuelto uno de los principales factores de riesgo en la seguridad empresarial. Al gran número de usuarios existentes se suma la falta de protección de estos dispositivos, que los convierte en la vía de entrada perfecta para los atacantes.

Figura 47. Medidas de seguridad en un Smartphone. Fuente Samsung

La especificación ETSI TS 103 732 identifica riesgos clave de seguridad y privacidad para los datos del usuario proporcionando la protección adecuada en dispositivos móviles.

¿Cuáles son las claves para protegerlos de los ciberataques?

- Formación y concienciación. Debido a que el factor humano es uno de los motivos más comunes en los ciberataques, es importante desarrollar una cultura de ciberseguridad para evitar futuros ataques.

- Instalar un buen antivirus y mantener actualizado el software y el sistema operativo, como en los ordenadores personales y tabletas.

- Cifrado de comunicaciones: las conexiones entre los dispositivos de casa y los del trabajo deben estar cifradas. Para ello se deben establecer redes privadas virtuales o VPN, una especie de túneles a través de los cuales pasan los datos protegidos.

- Evitar correos de phishing que puedan llevarnos a una página falsa, aunque parezca legítima, en la que nos engañan o sustraen la información. Esto pueda pasar tanto en ordenadores como en móviles, pero el hecho de estar continuamente conectados mediante los smartphones hace que las probabilidades de sufrir un ataque sean más elevadas. Por este motivo, se recomienda no abrir enlaces o descargar adjuntos en los dispositivos si no se tiene la seguridad de su procedencia.

- Utilizar doble protección (huella + contraseña). El pequeño tamaño del teléfono ha facilitado la movilidad, pero también ha expuesto a robos y pérdidas. Para reducir el riesgo de que alguien acceda a la información, es importante proteger el dispositivo con contraseñas. Pero también es recomendable bloquear el teléfono con el sensor de huella dactilar o el reconocimiento facial, si lo tenemos disponible.

- Emplear el doble factor de autenticación es otra de las formas de complicarles la tarea a los ciberdelincuentes en el acceso a las aplicaciones. Esta capa de seguridad adicional complementa el uso de las contraseñas.

- Evitar usar las mismas credenciales para las apps, páginas webs y desbloqueo del teléfono. También es imprescindible cambiar las contraseñas de forma periódica.

- No abrir archivos confidenciales en redes Wi-Fi abiertas de hoteles, cafeterías, etc., ignorando los riesgos a los que nos exponemos. Si no se tiene la seguridad de la fiabilidad de la red y, especialmente, si se van a realizar operaciones en las que se intercambie información personal, se recomienda hacer uso solo de los datos móviles y desactivar Wi-Fi.

- Siempre descargar apps en las tiendas oficiales. Hay que tener muy presente que una de las principales vías de propagación del malware en móviles son las descargas fuera de las tiendas oficiales.

- Activar la geolocalización y su uso por apps solo cuando sea necesario.

Nunca antes en la historia se han registrado tantos ciberataques como ahora. La pandemia y, sobre todo, en las últimas semanas, la guerra de Ucrania, han provocado un crecimiento sin precedentes en todo el planeta. Estar conectados conlleva estar más expuestos ante los peligros de la Red, pero es innegable que el teléfono móvil ha facilitado la vida, tanto en el ámbito personal como profesional. Por tanto, lo mejor que se puede hacer para utilizarlo de forma segura es seguir las pautas que nos ofrecen los profesionales del sector y, sobre todo, utilizar el sentido común; así, será posible minimizar los riesgos.

Una serie de guías útiles sobre el uso seguro y saludable de Internet y otras TIC, así como el fomento de la ciudadanía digital responsable en la infancia y la adolescencia, se pueden obtener en: https://www.pantallasamigas.net/

CONCLUSIONES

Los primeros ciberataques que se hicieron, en la década de los noventa, no tenían una motivación económica detrás, era sólo una cuestión de poder de conseguir datos que nadie más podía saber que la propia empresa o institución. Ahora el objetivo es, claramente, el dinero y existen grupos organizados de ciberdelincuentes que buscan, exclusivamente, sacar un rédito económico.

"Según estimaciones de la Comisión Europea (CE), el costo de la ciberdelincuencia para la economía global en el año 2020, fue de 5,5 billones de euros, superior al tráfico de drogas".

La ciberdelincuencia crece a un ritmo muy acelerado, con nuevas tendencias emergiendo continuamente. Los ciberdelincuentes se están volviendo más ágiles, explotan las nuevas tecnologías a una velocidad de vértigo, adaptan sus ataques utilizando nuevos métodos, más sofisticados cada día. Las redes delictivas operan a escala global, coordinando ataques complejos contra sus objetivos desde cualquier lugar del mundo.

La ciberseguridad se ha convertido en una de las principales prioridades en las últimas dos décadas. Prevenir el robo de datos, contraseñas, documentos, etc., es de vital importancia para cualquier usuario, sea autor científico-técnico o no, así como para las empresas. En la actualidad las técnicas de ingeniería social se emplean para atacar al eslabón más débil de la ciberseguridad, el ser humano.

Identificar un peligro cibernético, aplicando el sentido común para evitar caer en él, es tan sólo el primer paso; tomar medidas contra las amenazas y crímenes del ciberespacio es el mayor reto al que se enfrentan los países, y muchas empresas y ciudadanos.

El principal objetivo de la ciberseguridad es evitar las amenazas que ponen en riesgo la información a través de distintas herramientas, como: análisis de ciberseguridad, servicios de monitorización y resolución de problemas, formación para concienciar a los empleados, mantenimiento continuo de los sistemas y herramientas, etc.

La mayoría de los países tienen algunas leyes de ciberseguridad. Pueden tener relación con la infraestructura crítica, las redes, y la privacidad corporativa e individual y todas las empresas deben cumplir estas leyes. Las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos y de las empresas en el ámbito digital, tales como la privacidad, la propiedad, así como para aumentar la confianza en las tecnologías y en la transformación digital, y que todos puedan sentirse cómodos accediendo a dichas tecnologías.

El crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo. A nivel agregado, las cifras adquieren aún mayor magnitud pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB. Es por ello que existe un aumento generalizado de la inversión en ciberseguridad en las empresas y la previsión es que se mantenga al alza.

Durante 2021 se ha dado un gran aumento de los ciberataques a nivel mundial, con graves casos de interrupciones, secuestro y robo de datos, entre otros problemas. Y, las perspectivas para este año 2022 no son buenas, ya que se prevé que el riesgo siga creciendo a niveles muy elevados. La consultora tecnológica Gartner estima que la facturación global del sector pasará de los 153.000 millones de dólares en 2018 a los 248.000 millones en 2023, un aumento del 62%.

Figura 48. La ciberseguridad compromete a todos los países. Fuente INCIBE-CERT

En España, tanto en las empresas como en la Administración Pública y en el propio Gobierno, existe una sensibilización creciente hacia la ciberseguridad, con legislación establecida al efecto, pero, sin duda, hay un amplio margen de mejora. Prueba de ello es la reciente Ley sobre Ciberseguridad 5G, o el escándalo a consecuencia del espionaje a políticos con "Pegasus", aunque si bien las grandes y medianas empresas son conscientes de que estos ataques pueden paralizar una compañía o incluso hacerla desaparecer, entre las pymes, existe una baja percepción del problema y estas tienden a autoexcluirse como potencial objetivo de ciberataques.

Con la proliferación del teletrabajo y la adopción de los servicios en la nube, las redes domésticas son el nuevo objetivo de los ciberdelincuentes, que aprovechan la inexperiencia de las empresas en este nuevo ámbito laboral y la falta de formación informática de muchos de los usuarios.

Algunas normas básicas a observar, son:

- ✓ Tener un antivirus actualizado en todos los dispositivos digitales.
- ✓ Evitar el acceso a web sospechosas y no descargar información dudosa.
- ✓ No hacer clic en enlaces sospechosos recibidos por correo electrónico.
- ✓ No revelar información confidencial ni datos personales comprometedores.
- ✓ Ser muy precavidos al revelar información personal en redes sociales.
- ✓ Utilizar contraseñas fuertes, diferentes por aplicación y cambiarlas regularmente.
- ✓ Evitar conectarse a redes Wi-Fi públicas o conexiones inalámbricas desconocidas.
- ✓ Usar una conexión VPN para navegar por internet al usar wifis públicas.
- ✓ Realizar copias de seguridad por si sufrimos ataques o tenemos algún problema.
- ✓ Desconfiar de aquellos email o SMS donde se soliciten datos bancarios o claves de acceso; aun cuando procedan de una entidad conocida, como el Banco, Hacienda o Correos.
- ✓ Verificar siempre que la URL de la dirección web tiene el símbolo del candado.

Además, hay que tener en cuenta que cada vez aparecen nuevas tecnologías, y los cibercriminales son de los primeros en hacer uso de ellas para nuevas estafas y acosos. Cada vez surgen más engaños relacionados a las tendencias más recientes de las redes sociales –con la persona como vector de ataque–, ingeniería social con criptomonedas, e incluso ya se empieza a hablar de la ingeniería social en el metaverso.

Y para finalizar, en el siguiente enlace se proporciona una lista que contiene 33 de los mejores libros de ciberseguridad, en inglés y en español. Algunos del 2021, otros libros imprescindibles para expertos o principiantes: https://ciberseguridad.blog/33-de-los-mejores-libros-de-ciberseguridad/