

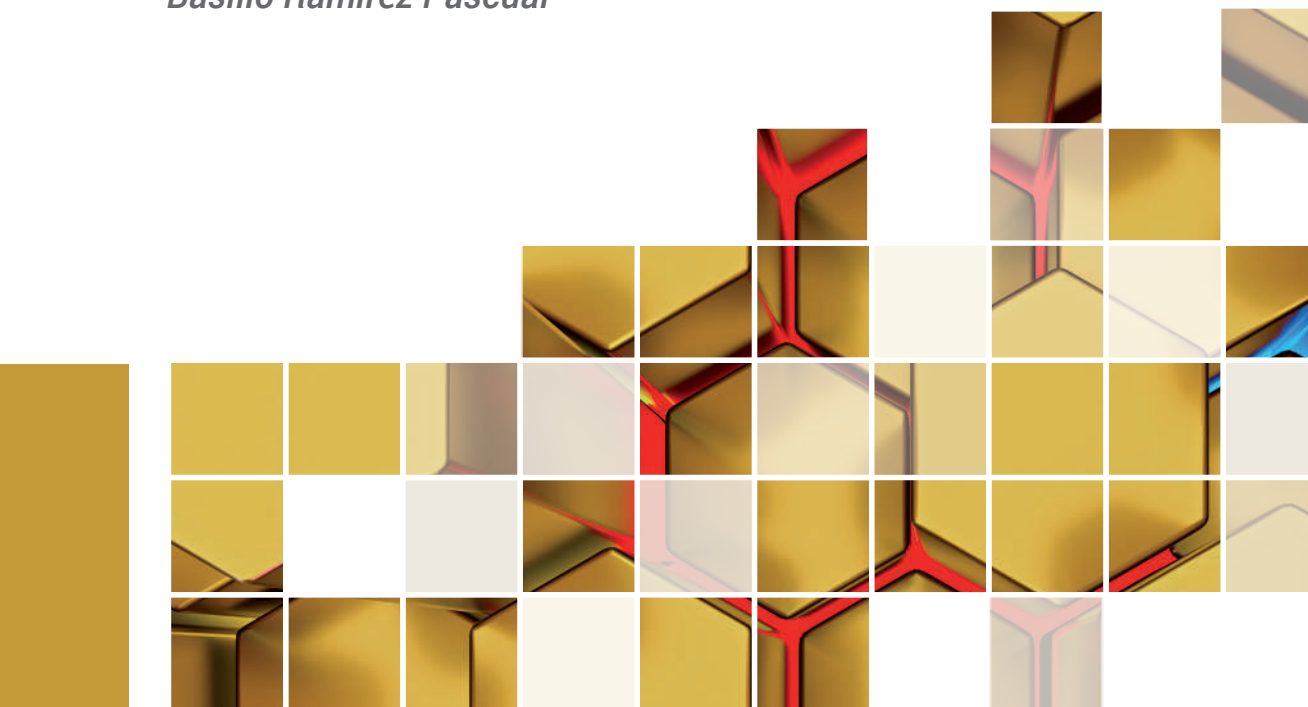
TEMAS

La ciberseguridad en la era de la Inteligencia Artificial

Dilemas y retos empresariales

Coordinador

Basilio Ramírez Pascual



III LA LEY

TEMAS

La ciberseguridad en la era de la Inteligencia Artificial

Dilemas y retos empresariales

Coordinador

Basilio Ramírez Pascual

© Autores, 2023
© LA LEY Soluciones Legales, S.A.

LA LEY Soluciones Legales, S.A.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 91 602 01 82
e-mail: clienteslaley@aranzadilaley.es
<https://www.laley.es>

Primera edición: Octubre 2023

Depósito Legal: M-31493-2023
ISBN versión impresa: 978-84-19905-03-1
ISBN versión electrónica: 978-84-19905-04-8

Diseño, Preimpresión e Impresión: LA LEY Soluciones Legales, S.A.
Printed in Spain

© **LA LEY Soluciones Legales, S.A.** Todos los derechos reservados. A los efectos del art. 32 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba la Ley de Propiedad Intelectual, LA LEY Soluciones Legales, S.A., se opone expresamente a cualquier utilización del contenido de esta publicación sin su expresa autorización, lo cual incluye especialmente cualquier reproducción, modificación, registro, copia, explotación, distribución, comunicación, transmisión, envío, reutilización, publicación, tratamiento o cualquier otra utilización total o parcial en cualquier modo, medio o formato de esta publicación.

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la Ley. Diríjase a **Cedro** (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.

El editor y los autores no asumirán ningún tipo de responsabilidad que pueda derivarse frente a terceros como consecuencia de la utilización total o parcial de cualquier modo y en cualquier medio o formato de esta publicación (reproducción, modificación, registro, copia, explotación, distribución, comunicación pública, transformación, publicación, reutilización, etc.) que no haya sido expresa y previamente autorizada.

El editor y los autores no aceptarán responsabilidades por las posibles consecuencias ocasionadas a las personas naturales o jurídicas que actúen o dejen de actuar como resultado de alguna información contenida en esta publicación.

LA LEY SOLUCIONES LEGALES no será responsable de las opiniones vertidas por los autores de los contenidos, así como en foros, chats, u cualesquiera otras herramientas de participación. Igualmente, LA LEY SOLUCIONES LEGALES se exime de las posibles vulneraciones de derechos de propiedad intelectual y que sean imputables a dichos autores.

LA LEY SOLUCIONES LEGALES queda eximida de cualquier responsabilidad por los daños y perjuicios de toda naturaleza que puedan deberse a la falta de veracidad, exactitud, exhaustividad y/o actualidad de los contenidos transmitidos, difundidos, almacenados, puestos a disposición o recibidos, obtenidos o a los que se haya accedido a través de sus PRODUCTOS. Ni tampoco por los Contenidos prestados u ofertados por terceras personas o entidades.

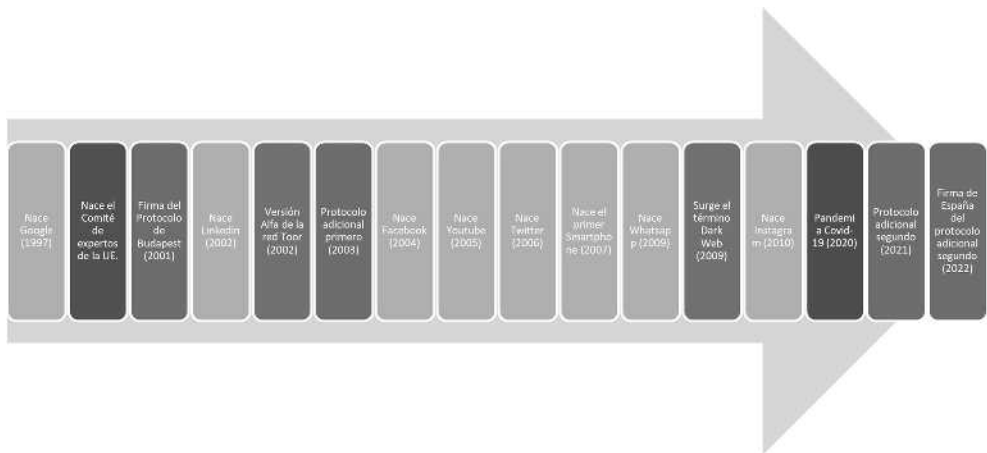
LA LEY SOLUCIONES LEGALES se reserva el derecho de eliminación de aquellos contenidos que resulten inveraces, inexactos y contrarios a la ley, la moral, el orden público y las buenas costumbres.

Nota de la Editorial: El texto de las resoluciones judiciales contenido en las publicaciones y productos de **LA LEY Soluciones Legales, S.A.**, es suministrado por el Centro de Documentación Judicial del Consejo General del Poder Judicial (Cendoj), excepto aquellas que puntualmente nos han sido proporcionadas por parte de los gabinetes de comunicación de los órganos judiciales colegiados. El Cendoj es el único organismo legalmente facultado para la recopilación de dichas resoluciones. El tratamiento de los datos de carácter personal contenidos en dichas resoluciones es realizado directamente por el citado organismo, desde julio de 2003, con sus propios criterios en cumplimiento de la normativa vigente sobre el particular, siendo por tanto de su exclusiva responsabilidad cualquier error o incidencia en esta materia.

1. LOS 3 ATAQUES MÁS USADOS CONTRA LAS EMPRESAS

En abril de 2022, Internet llegaba al 63% de la población mundial, lo que representaba unos 5.000 millones de personas. De este total, 4 650 millones —más del 93%— eran usuarios de redes sociales. Según Statista, la cantidad total de datos que se preveía que se crearan, capturaran, copiaran y consumieran en todo el mundo en 2022 era de 97 zettabytes, cifra que se preveía en crecimiento hasta los 181 zettabytes en 2025.

Si hacemos un poco de memoria para repasar la evolución de las nuevas tecnologías en los últimos años, podemos ver la velocidad de incursión que están teniendo estas en nuestras vidas y en nuestro día a día.



Vamos a repasar los hitos más importantes de los últimos años para ponernos en situación ante el problema de los ciberdelitos y los ciberataques a empresas:

— Por decisión CDPC/103/211196, el Comité europeo para los problemas criminales (CDPC) decidió en noviembre de 1996 establecer un comité de expertos encargado de los delitos informáticos. El Comité PC-CY inició su labor en abril de 1997 y llevó a cabo negociaciones acerca del proyecto de un convenio internacional sobre la ciberdelincuencia. Conforme a los

términos de referencia originales, el Comité debía terminar su trabajo para el 31 de diciembre de 1999.

— Nacimiento de Google (1997).

— Firma del Convenio de Budapest. El Convenio y su Informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001) y el Convenio fue abierto a la firma en Budapest, el 23 de noviembre de 2001, con motivo de la celebración de la Conferencia Internacional sobre la ciberdelincuencia.

— Nacimiento de LinkedIn (2002).

— Versión Alfa de la red TOOR (2002).

— Protocolo adicional primero del Convenio de Budapest (2003).

— Nacimiento de Facebook (2004).

— Nacimiento de youtube (2005).

— Nacimiento de Twitter (2006).

— Nacimiento de los Smartphone (2007).

— Nacimiento de Whatsapp (2009).

— Surge el término Darkweb (2009).

— Nacimiento Instagram (2010).

— Pandemia Covid-19 (2020).

— Segundo Protocolo adicional al Convenio de Budapest (2021).

— Firma de España del segundo protocolo adicional al Convenio de Budapest (2022).

Lo que nos parecían temas de película de ciencia ficción en títulos como «Juegos de Guerra», donde un joven hackea el sistema de defensa de los EEUU desde su ordenador conectado a un módem, o «Superman III», donde un empleado descontento idea un programa que quita un céntimo de cada nómina de todos los empleados de la empresa para írselos ingresando a Él, de tal forma que no levanta sospechas sobre el robo, hoy en día nos resultan situaciones muy conocidas y en los medios de comunicación se dan a conocer ciberdelitos parecidos muy a menudo.

La evolución de las nuevas tecnologías, el auge en el acceso a las mismas y la mejora de las comunicaciones a nivel mundial, han propiciado marcos fantásticos de colaboración y expansión para muchos negocios, pero los delincuentes han encontrado un campo de juego muy interesante para sus actividades delictivas.

Según algunos informes, el coste medio de una brecha de ciberseguridad en las empresas españolas puede variar entre 54.388 euros y 743.000 euros, dependiendo del tamaño de la empresa, el tipo de ataque y el nivel de actualización de los sistemas. Cifra que con el paso del tiempo crece exponencialmente.

La cibercriminalidad se ha convertido en un problema complejo para las empresas, aumenta la complejidad para protegerse y para defenderse ya que las empresas necesitan contar con equipos multidisciplinares que les ayuden en estas tareas. Según el tamaño de la empresa y el mercado al que se dediquen tendrán más o menos complicado contar con este tipo de equipos dentro de sus plantillas, aunque si es verdad que podrán contratar estos servicios a empresas especializadas.

Lo importante es no separar la Ciberseguridad del negocio y de sus procesos, tenemos que plantearnos siempre las acciones con la Ciberseguridad implícita y olvidarnos de pensar en la Ciberseguridad como algo opcional o algo *a posteriori*. Debemos desarrollar los procesos de nuestros negocios siempre de manera Cibersegura y tener muy claro que la Ciberseguridad no es un gasto, es una inversión.

En este aspecto, también debemos tener en cuenta que Fuerzas y Cuerpos de Seguridad del estado han creado sus propios grupos expertos en la investigación de estos ciberdelitos, creando equipos multidisciplinares y en constante formación.

El mayor problema ante los ciberataques es pensar aquello de «A mí no me pasa» o «¿A quién le van a interesar mis datos?», porque nadie está libre de ser ciberatacado, pero lo importante es estar preparado para cuando llegue ese momento, habiendo tomado todas las medidas necesarias para dar una buena respuesta y que, en caso de que el ataque sea exitoso, podamos minimizar daños y que no afecte a nuestra producción.

Si seguimos repasando la historia, vemos grandes ciberataques que fueron noticia:

— Sony Pictures: En 2014, ciberdelincuentes desconocidos filtraron información confidencial de la empresa, como correos electrónicos, guiones y datos de empleados.

— Equifax: En 2017, la compañía de servicios financieros sufrió una brecha de seguridad que expuso los datos personales de 143 millones de clientes en EE.UU., Canadá y Reino Unido.

— Yahoo: Entre 2013 y 2014, la empresa de internet fue víctima de dos ataques que comprometieron las cuentas de más de 3.000 millones de usuarios.

— Wannacry: En 2017, este ransomware infectó a más de 200.000 ordenadores en 150 países, afectando a empresas como Telefónica, Renault o el Servicio Nacional de Salud británico.

— Microsoft: En 2021, la empresa tecnológica sufrió un ataque a su servicio de correo Exchange que afectó a unas 60.000 organizaciones en todo el mundo.

Si miramos los datos de España de 2019 y 2020 año de la pandemia (según statista e ituser.es), podemos observar el crecimiento de los ciberataques:

Año	Porcentaje de empresas atacadas	Procedimientos judiciales por Ciberdelincuencia
2019	36%	11.670
2020	70%	16.900

Teniendo en cuenta que estas cifras sólo se sacan de los ataques conocidos o puestos en conocimiento por las empresas que lo han sufrido, esta estadística se queda corta porque hay muchos ciberataques que no se comunican y no pueden entrar en la misma, lo que debería hacernos pensar que el problema es más preocupante aún de lo que los datos nos muestran.

Otra información importante que nos puede ayudar a conocer mejor el problema es saber cuáles son las principales causas de estos ciberataques. Según una infografía de Willis Towers Watson, las principales causas de ciberataques a empresas en España son:

- Divulgación accidental de información por parte de los empleados (32% de las incidencias).
- Pérdida y robo de dispositivos (21% de las incidencias).
- Hacking o pirateo (18% de las incidencias).
- Empleados malintencionados (12% de las incidencias).
- Brecha en terceros (9% de las incidencias).
- Ingeniería social (6% de las incidencias).
- Interrupción del negocio por colapso de la red (2% de las incidencias).

Según el informe sobre la Cibercriminalidad en España de 2021, podemos ver el tipo de amenazas a los que se enfrenta la Unión Europea:

- **Programas de secuestro:** tipo de ataque en el que se encriptan los datos de la víctima y se pide rescate por los mismos. En 2021 se duplicó el precio solicitado por los rescates.
- **Programas malignos:** tipo de ataque que busca dañar los dispositivos, acceder a los mismos o alterar su buen funcionamiento.
- **Criptosequestros o criptominería maliciosa:** uso no autorizado de los dispositivos para minar criptomonedas.
- **Ataques por correo electrónico:** ataque usado para obtener credenciales o datos bancarios a través de distintas técnicas.

— **Violación de los datos sensibles y fugas de datos:** ataque dirigido a la divulgación de datos confidenciales o sensibles protegidos en entornos poco confiables.

— **Ataques distribuidos de denegación de servicio:** Ataque que busca impedir que los usuarios accedan a ciertos servicios o cierta información.

— **Desinformación:** ataques dirigidos a cambiar opiniones a través de campañas de noticias falsas.

— **Amenazas no malintencionadas:** fallos, normalmente humanos, que se producen sin intención de causar daños.

— **Amenazas a la Cadena de suministro:** ataque dirigido contra una organización, aprovechando alguna vulnerabilidad de su cadena de suministro, buscando producir efectos en cascada.

Toda esta información nos da una idea del problema de los ciberataques a las empresas y su rápido aumento en poco tiempo. En la línea temporal tenemos marcado en rojo el año 2020, año en que nos tuvimos que encerrar todos en nuestras casas y que obligó a todas las empresas a mandar a sus empleados a «Teletrabajar», pero el problema en ese momento es que las empresas no tenían en muchas ocasiones planes para ese teletrabajo, y a marchas forzadas se montaron sistemas de «trabajo a distancia», es decir sistemas de conexión remota a los ordenadores de la empresa para realizar el trabajo como si se estuviese sentado en la oficina.

Este hecho produjo que muchas empresas abriesen muchas puertas a los ciberdelincuentes fruto de esa necesidad de tener a la gente trabajando en sus casas en tiempo record y sin una planificación de los procesos y los sistemas para ejecutar el teletrabajo de forma segura.

Viendo cómo avanzan las tecnologías y la incursión imparable de la Inteligencia Artificial en nuestras vidas, podemos pensar que los tres ciberataques que más se van a seguir utilizando contra las empresas, según una publicación de KeepCoding, son:

— **Ransomware:** un malware que cifra los datos del sistema y pide un rescate para liberarlos.

— **Phishing:** un engaño que busca obtener información confidencial de los usuarios mediante correos electrónicos o páginas web falsas.

— **Wifi Hacking:** un ataque que aprovecha las vulnerabilidades de las redes wifi para acceder a los dispositivos conectados.

Otras fuentes también mencionan los ataques de denegación de servicio, el fraude financiero y la intrusión física a instalaciones como amenazas más comunes. Pero vamos analizar el top tres y cómo podemos proteger nuestras empresas de estos peligros.

1.1. Ransomware

El ransomware es un tipo de *software* malicioso o malware diseñado específicamente para cifrar los archivos y datos de un usuario o una organización de forma que el propietario de esos archivos no pueda acceder a ellos sin una clave de descifrado. Una vez que los archivos han sido cifrados, el atacante suele exigir un rescate en forma de pago para proporcionar la clave de descifrado y devolver el acceso a los datos. Es importante destacar que pagar el rescate no garantiza necesariamente la recuperación de los archivos ni la eliminación del ransomware.

Este tipo de ciberataque puede tener un alto impacto en nuestra empresa y en nuestro negocio, afectándonos de las siguientes maneras:

1. Interrupción de las operaciones:

Cuando el ransomware infecta los sistemas de una empresa, se cifran archivos y datos cruciales para las operaciones diarias. Esto puede dar como resultado una paralización de las actividades comerciales normales, lo que afecta la productividad y la capacidad de prestar servicios o producir bienes.

2. Pérdida de datos:

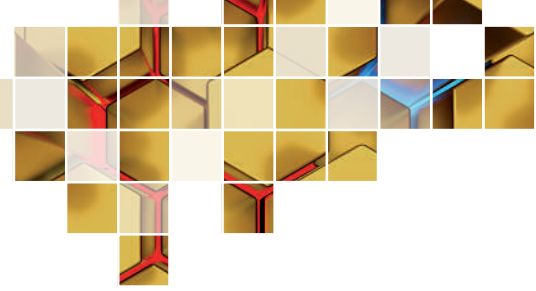
Si la empresa no puede recuperar los archivos cifrados, se enfrenta la pérdida potencial de datos críticos. Esto incluye información financiera, registros de clientes, datos de inventario, documentos de recursos humanos y otros activos digitales esenciales. La pérdida de datos puede tener un impacto duradero en la operación de la empresa y por lo tanto en el negocio.

3. Costos financieros:

Un ataque de ransomware conlleva costos financieros significativos. Estos pueden incluir el posible pago del rescate, los gastos asociados con la recuperación de datos, la contratación de expertos en ciberseguridad, la adquisición de herramientas de descifrado y la restauración de sistemas. También se deben considerar los costos relacionados con la investigación forense para determinar cómo ocurrió el ataque.

4. Pérdida de productividad:

Además de los costos financieros directos, el ransomware afecta a la productividad de los empleados. Durante un ataque y la posterior recuperación, los equipos de IT pueden verse abrumados, y los empleados pueden tener dificultades para realizar sus tareas habituales debido a la falta de acceso a datos y sistemas críticos. En más de una ocasión, los empleados han sido enviados a sus



En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en una preocupación fundamental también en el ámbito empresarial. *La ciberseguridad en la era de la Inteligencia Artificial* es una obra pionera que aborda de manera exhaustiva las problemáticas más apremiantes en este campo. Este libro desentraña la complejidad de los algoritmos de IA y explica cómo pueden convertir a las empresas en blancos vulnerables para los ciberdelincuentes.

Se examinan en detalle los tres ataques de ingeniería social más comunes y sus implicaciones para la seguridad de las empresas. Del mismo modo, también se proponen estrategias efectivas para proteger y recuperar activos, además de describir el papel crucial del Responsable de Seguridad de la Información (RSI) en España y cómo establecer políticas de seguridad de la información.

En definitiva, *La ciberseguridad en la era de la Inteligencia Artificial* busca crear una cultura empresarial donde la ciberseguridad sea una preocupación compartida por todos y facilite la comprensión de las tácticas empleadas por los ciberdelincuentes para poder proteger así el futuro digital de las empresas.

ISBN: 978-84-19905-03-1



31652463846



ER-0280/2005



GA-200501100