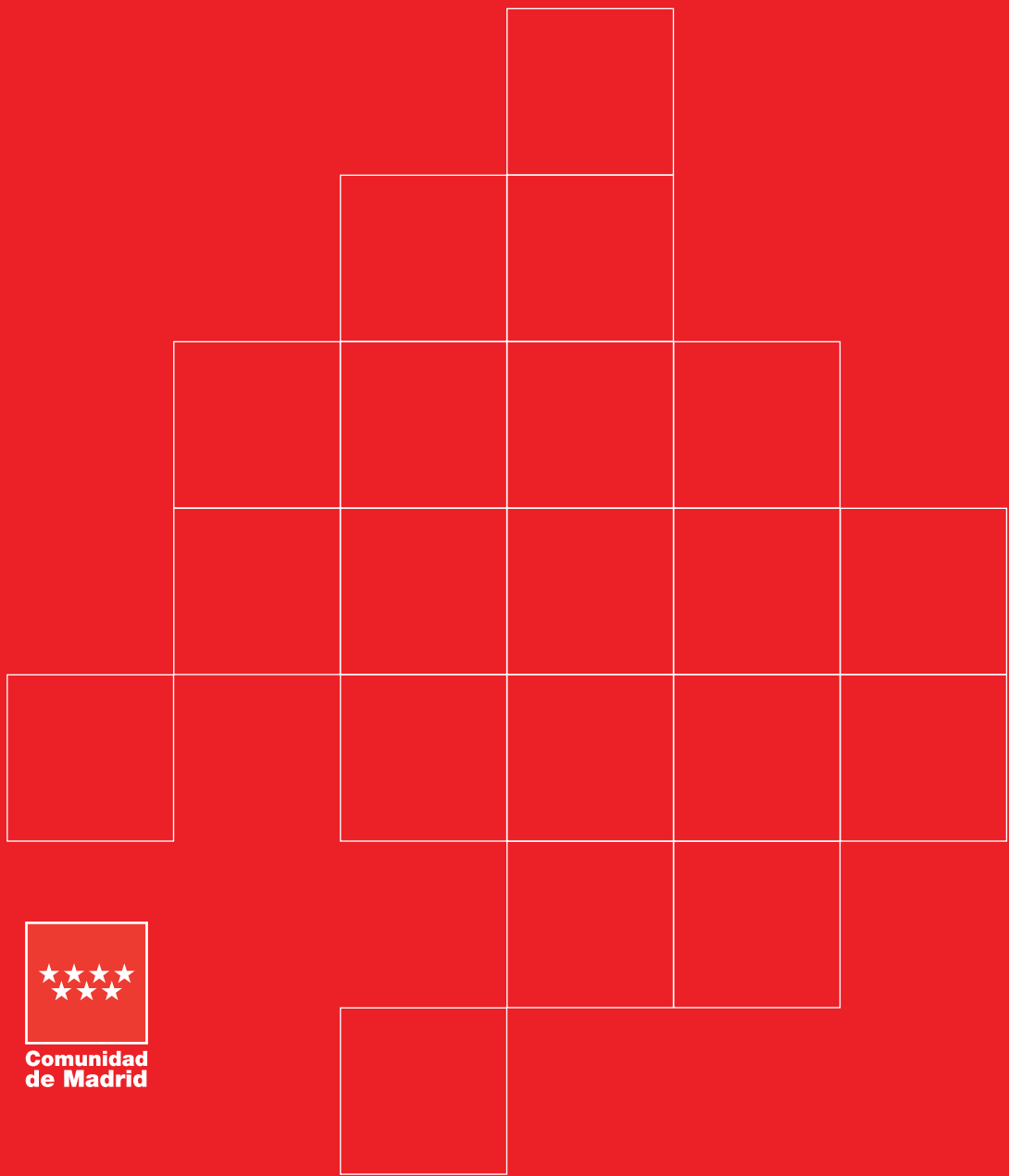
INFORME SOBRE CIBERSEGURIDAD Y SU IMPACTO EN LAS EMPRESAS

2024



ceim EMPRESARIOS DE MADRID

Comunidad de Madrid

INFORME SOBRE CIBERSEGURIDAD Y SU IMPACTO EN LAS EMPRESAS

2024

La Comunidad de Madrid colabora en esta publicación en el marco del Convenio con CEIM, en su condición de miembro del Consejo para el Diálogo Social de la Comunidad de Madrid, para la realización de actuaciones que contribuyan a la promoción del desarrollo económico y social de la Comunidad de Madrid en 2024-25.

Informe elaborado por:
Sagardoy School Business and Law
(Alfonso Muñoz y Román Gil)

Maquetación:
GRAPICT
grapict@grapict.com

ceim EMPRESARIOS DE MADRID

Comunidad de Madrid

ÍNDICE

ÍNDICE

INTRODUCCIÓN

En la actualidad, vivimos en una era digital donde la seguridad de la información se ha convertido en un pilar fundamental para la estabilidad y el éxito de las empresas. La creciente dependencia tecnológica y el incremento de amenazas cibernéticas han puesto de manifiesto la importancia de implementar medidas de seguridad eficaces.

La falta de seguridad digital no solo pone en riesgo la información sensible, sino que también puede afectar gravemente la reputación y la viabilidad económica de una empresa.

Se analizan seguidamente los riesgos que la falta de seguridad digital supone para las empresas; así como se identifican las barreras con las que se encuentran las empresas madrileñas al implementar medidas de ciberseguridad eficaces y las ventajas de tener sistemas informáticos seguros.

Con este informe de CEIM, elaborado por Sagardoy School Business and Law, en el marco del Convenio con la Comunidad de Madrid para la promoción del desarrollo económico y social, se proporciona a nuestras empresas:

a) **Un análisis exhaustivo en materia de ciberseguridad.**

b) **Eficacia en la toma de decisiones.**

c) **Sólidos criterios de actuación.**

PANORAMA ACTUAL DE LAS AMENAZAS CIBERNÉTICAS

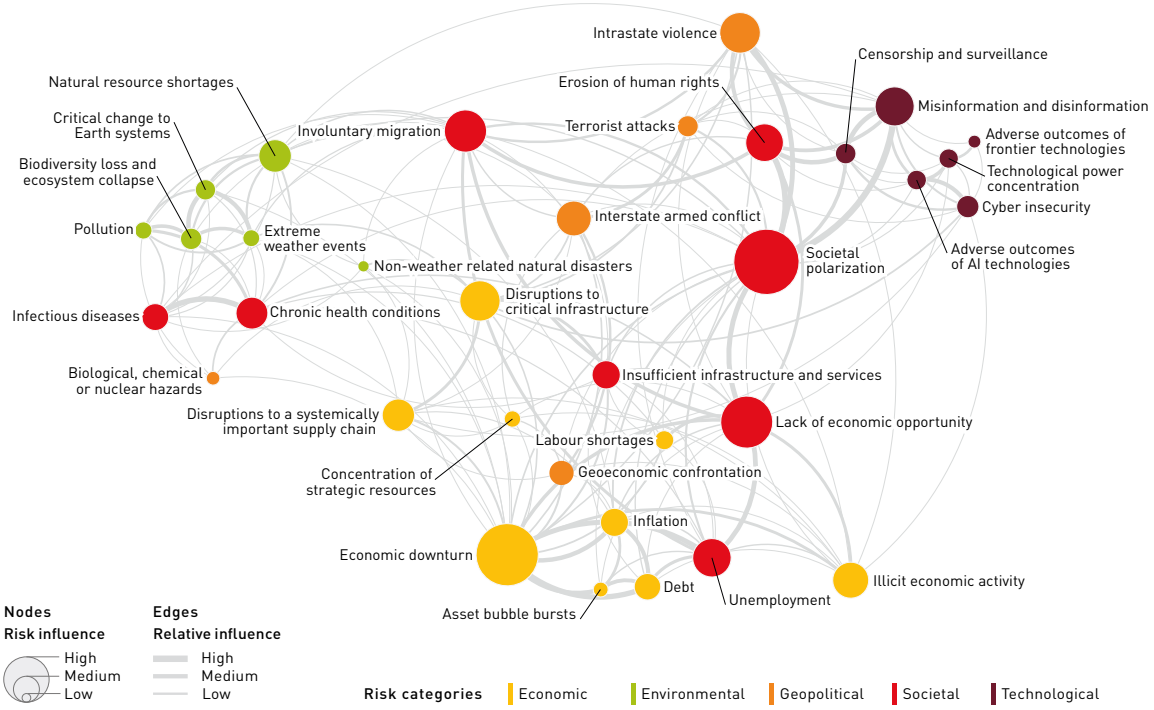
El informe anual del Foro Económico Mundial sobre Riesgos Globales 2024[1] esboza un panorama de las amenazas cibernéticas cada vez más complejo y dinámico, con una evolución continua tanto en la sofisticación de los ataques como en los tipos de actores maliciosos involucrados.

Estas amenazas impactan no solo a individuos y empresas, sino también a infraestructuras críticas[2] y gobiernos de todo el mundo. Riesgos como el malware/ransomware, los deepfakes y la desinformación, apoyados en el uso de IA, o las amenazas a las cadenas de suministro son un buen ejemplo de acciones concretas que pueden afectar a la economía y la democracia.

Tanto es así que el Fondo Monetario Internacional (FMI)[3] advirtió al sector financiero de la importancia de considerar estas amenazas seriamente por su impacto en la estabilidad financiera mundial.

Existe una amplia colección de amenazas y vulnerabilidades, que se analizarán en el presente informe, que fuerzan el liderazgo de CEOs (Chief Executive Officer) y responsables corporativos en nuevos enfoques de ciberseguridad en búsqueda de compañías ciberresilientes en un entorno de amenazas en constante evolución.

Figura 1. Global risks landscape: an interconnections map



F uente: https://www3.wexforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[1] https://es.wexforum.org/agenda/2024/10/foco-en-la-ciberseguridad-10-cosas-que-necesitas-saber-en-2024/

[2] https://iccwbo.org/wp-content/uploads/sites/3/2024/07/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf

[3] https://www.wexforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/

La prestigiosa consultora Gartner[4], consolidada por ser una de las fuentes principales de información para organizaciones que buscan tomar decisiones informadas en tecnología, gestión de la información y consultoría estratégica, permite vislumbrar algunas medidas y prioridades, capacidades técnicas y reformas estructurales que las empresas deberían considerar/extender para el período 2025. Especialmente en dos áreas: la ciberresiliencia[5] organizativa y el rendimiento de los departamentos/personal de ciberseguridad.

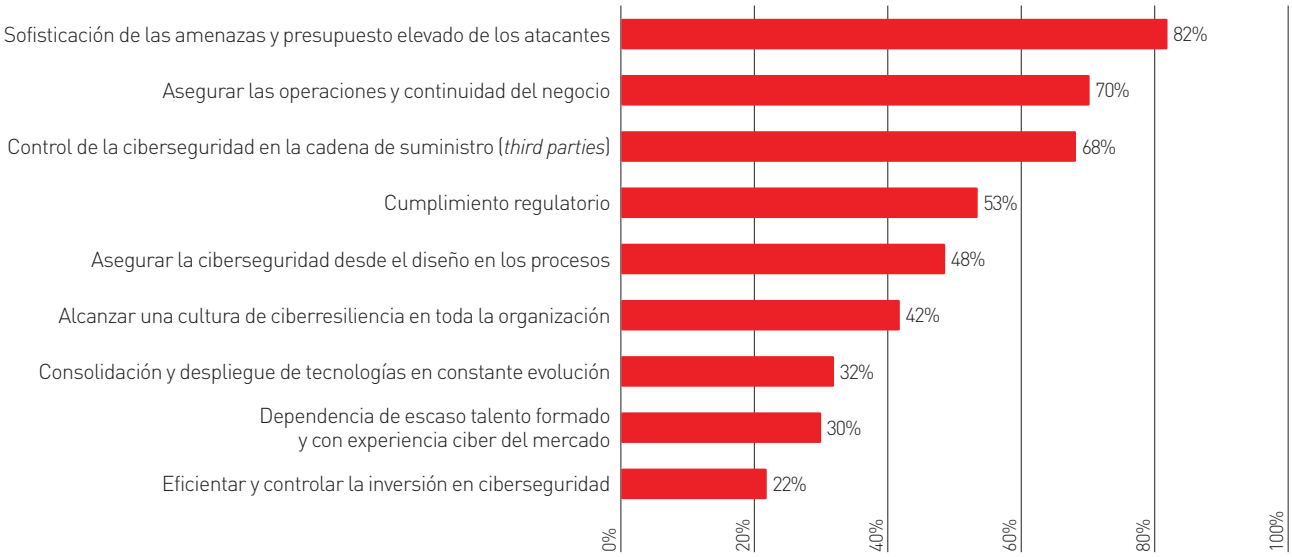
"La resiliencia organizativa, para impulsar las inversiones en seguridad en un contexto de continua dispersión de los ecosistemas digitales (p. ej., una mayor adopción de la nube, acuerdos de trabajo híbrido y un entorno de amenazas cambiantes)"

"El rendimiento del departamento de ciberseguridad, mediante el aprovechamiento de las capacidades de IA generativa, la priorización de los programas de comportamiento y cultura de la seguridad y la adopción de métricas basadas en resultados (ODM, por sus siglas en inglés), para facilitar la toma de decisiones"

En un ámbito local, los retos que enfrentan las empresas españolas en términos de ciberseguridad no difieren mucho de los anteriores. En un estudio reciente realizado por la consultora Deloitte[6], con un enfoque multisectorial, puede observarse los principales retos que los responsables tecnológicos y de ciberseguridad (CISO – Chief Information Security Officer) necesitarán abordar para los próximos años. Entre ellos, la sofisticación de las amenazas derivadas del presupuesto elevado de los atacantes, la seguridad en las operaciones y la continuidad de negocio y el control de la ciberseguridad en las cadenas de suministro.

Es significativo, como el 90% del total de las entidades encuestadas confirma haber aumentado o mantenido el número de ciberataques y de ese grupo, solo un 30% es capaz de calcular de forma objetiva con cierto grado de certeza/veracidad los costes reales derivados del impacto del ataque. El 70% no dispone de la información y eleva a la dirección una aproximación.

Figura 2. Principales retos para las empresas españolas



[4] https://www.gartner.es/es/tecnologia-de-la-informacion/temas/tendencias-ciberseguridad

[5] El desarrollo de la ciberresiliencia y el aumento de la confianza digital es un trabajo complejo que requiere una mayor cooperación entre diversos actores, marcos adecuados que mejoren la armonización y la coherencia y el desarrollo de capacidades e incentivos (incluida la financiación o los incentivos fiscales).

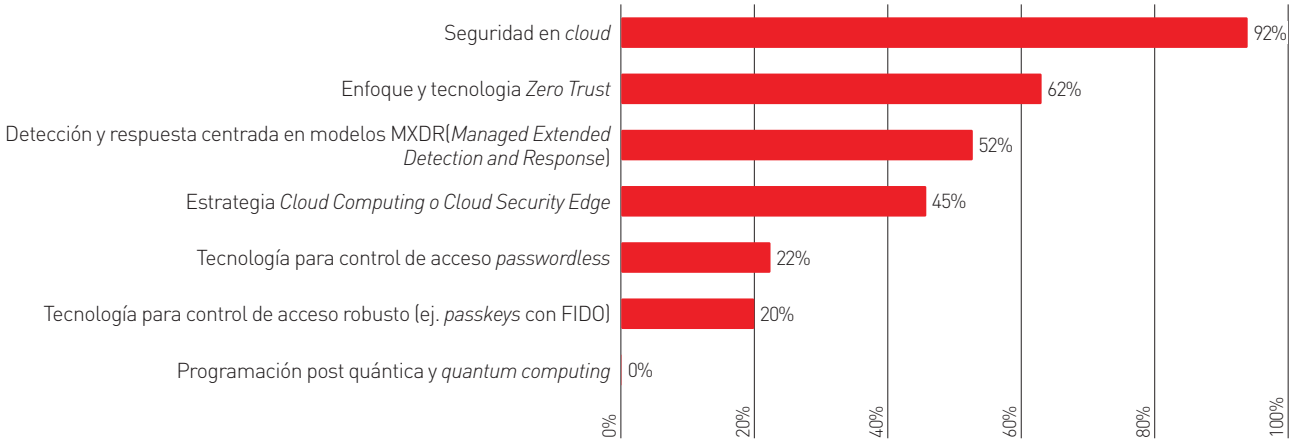
[6] Estado de la ciberseguridad en España 2024
https://perspectivas.deloxitte.com/l/915781/2024-04-04/svkg8/915781/1712225507RAcAAWir/Deloitte_Informe_Estado_Ciberseguridad_2024.pdf

Para las PYMES, la situación es especialmente crítica, ya que el 60% de las pequeñas y medianas empresas que sufren un ciberataque desaparecen en menos de seis meses tras el incidente. Este dato resalta la importancia de una ciberseguridad robusta para la supervivencia empresarial en la era digital[7].

El reto, por tanto, para el período 2025 de las empresas españolas residirá en continuar implementando medidas de seguridad de demostrada eficacia que redunden en la reducción de las preocupaciones corporativas en términos de continuidad de las operaciones de negocio, protección de la marca/reputación organizacional ante ciberataques, cumplimiento regulatorio y un entendimiento del presupuesto de ciberseguridad y la idoneidad o no del mismo.

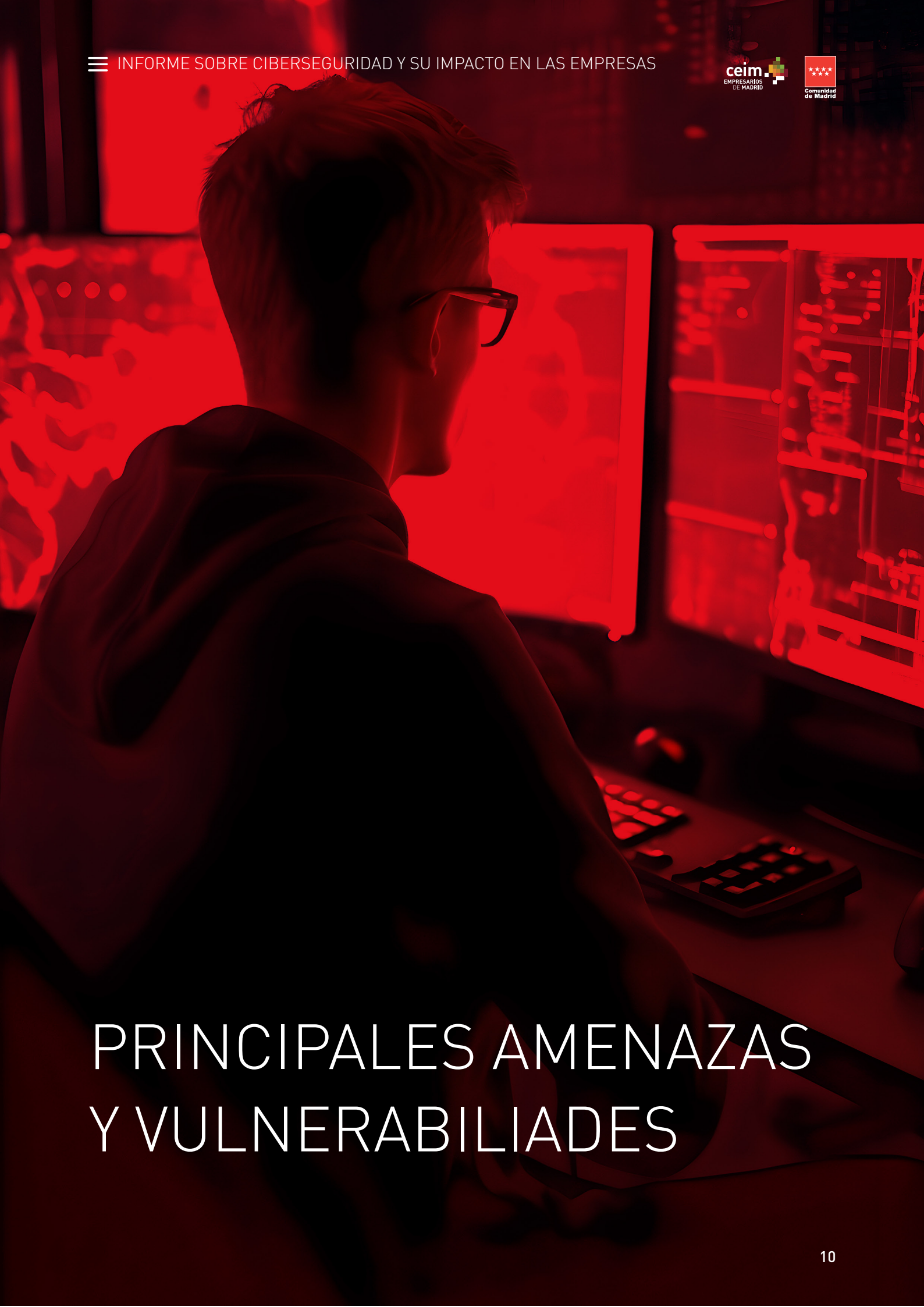
Algunas de estas contramedidas recaen en tecnologías de autenticación e identificación robusta, la protección adecuada de la información o tecnologías/sistemas adecuados para la monitorización, detección y respuesta frente a ciberataques.

Figura 3. Tecnologías y contramedidas recomendadas frente a ciberataques comunes



El propósito de este informe, por tanto, es entender en mejor manera los retos y oportunidades existentes desde el punto de vista de la ciberseguridad para las empresas españolas y madrileñas facilitando palancas para una mejora cualitativa en cada organización, reduciendo su complejidad y facilitando nuevas oportunidades de negocio.

[7] https://ptedisruptive.es/wp-content/uploads/2023/12/Informe-situacion-ciberseguridad-2023_compressed.pdf



PRINCIPALES AMENAZAS Y VULNERABILIADES

PRINCIPALES AMENAZAS Y VULNERABILIADES

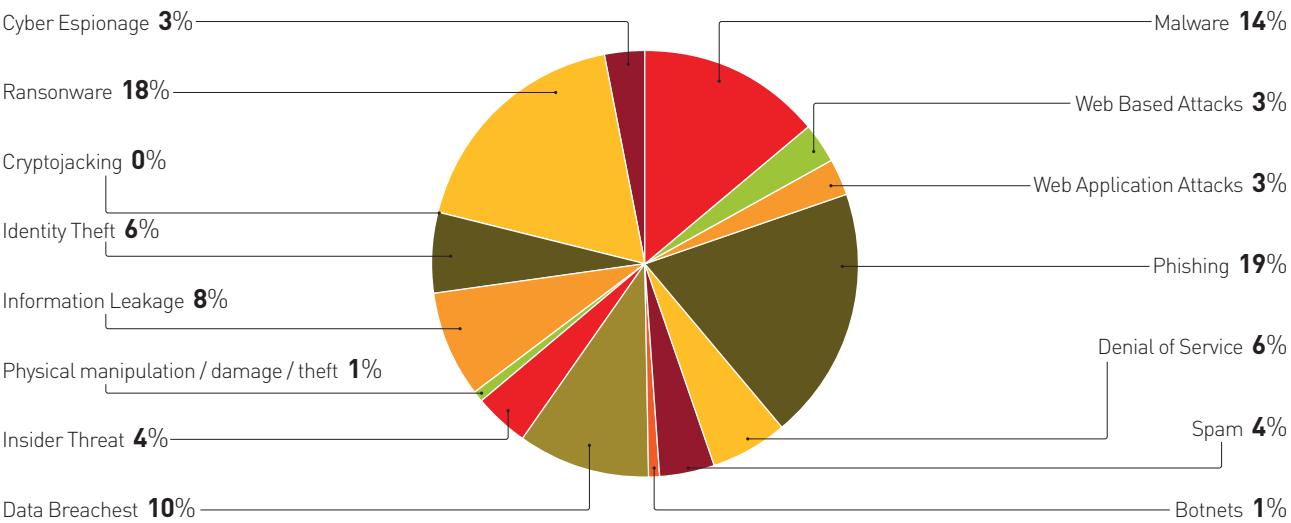
La ciberseguridad sigue siendo un reto importante para muchas empresas españolas. Hasta la fecha, se estima que alrededor del 50% de ellas ha experimentado algún tipo de ciberataque. Especialmente preocupante es el aumento significativo de incidentes que han afectado a las pymes, que han visto cómo los ciberataques han crecido de manera desproporcionada en comparación con otras empresas.

Uno de los aspectos más relevantes en este escenario es cómo las pymes perciben y se preparan para enfrentar estos riesgos. Solo el 61% de las empresas con menos de 250 empleados se sienten realmente preparadas para abordar los desafíos de la ciberseguridad, lo que indica que muchas aún carecen de los recursos y la formación necesarios para protegerse de manera adecuada en el entorno digital[8]. Es cierto que los informes publicados resaltan una actitud proactiva de autónomos y pymes españolas para mejorar en esta dirección, al menos un 53% de ellas planeó aumentar sus presupuestos de ciberseguridad en el período 2023/2024[9]. Por desgracia, no es suficiente.

Estos últimos años las empresas españolas han mostrado una mayor predisposición hacia la colaboración con expertos externos en ciberseguridad, apoyándose en consultoras o empresas especializadas para fortalecer su ciberseguridad. Esto es especialmente interesante en el caso de las PYMES, donde el enfoque colaborativo ha permitido acceder a soluciones avanzadas y seguir mejorando en su capacidad para protegerse en el mundo digital a un coste razonable, lo que las ayuda a ser más competitivas e innovadoras frente a las amenazas en constante evolución.

En la siguiente figura, se puede observar algunas de las amenazas comunes que afectan a cualquier entorno digital, independientemente del tamaño de la organización. Los porcentajes de incidencia suelen variar anualmente en función de diversos criterios e incluso "modas" de los cibercriminales, pero las amenazas son casi siempre las mismas. En los siguientes apartados, se va a detallar algunas de las amenazas más comunes en las que se debe prestar atención y aplicar esfuerzos humanos y económicos para mitigarlos.

Figura 4. Informe estado de la ciberseguridad en España 2024 – Deloitte



[8] https://www.incxibe.es/empresas/blog/las-principales-vulnerabilidades-de-una-pyme-en-materia-de-ciberseguridad

[9] La tendencia mundial en este sentido rondaría el 64% de las empresas. Por tanto, la inversión nacional sería inferior.

1. ATAQUES DE INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDAD

La ingeniería social constituye una estrategia insidiosa empleada por agentes malintencionados para ejercer una manipulación psicológica sobre los individuos, con el fin de inducirles a que, de manera involuntaria, revelen datos confidenciales o ejecuten acciones que comprometan la integridad de los sistemas de seguridad.

En 2024, la ingeniería social continúa siendo una de las tácticas más efectivas utilizadas por los cibercriminales. Se estima que alrededor del 98% de los ciberataques involucran algún tipo de ingeniería social, lo que la convierte en una de las principales herramientas para iniciar ataques cibernéticos. Este tipo de ataques ha incrementado su frecuencia en un 320% año tras año, y se espera que en 2025 continúen aumentando debido a que los perpetradores de estos ataques se valen de las vulnerabilidades emocionales de las personas, explotando su confianza, sus temores, la sensación de urgencia o la curiosidad innata, con el objetivo último de obtener información privilegiada o acceder a sistemas protegidos.

La ingeniería social está muy vinculada a la suplantación de identidad. La suplantación de identidad, también conocida como spoofing, constituye una modalidad específica de ataque en la que el agresor se disfraza figurativamente, adoptando la identidad de una persona o entidad de confianza, con el propósito deliberado de embaucar a su víctima. Este engaño permite al atacante ganarse la credulidad del destinatario, con el fin último de acceder a información sensible, ejercer control sobre sistemas restringidos o inducir a la víctima a realizar acciones perjudiciales en su propio detrimento o en el de su entorno.

Englobados en estos tipos de ataques existen algunas tendencias más comunes a resaltar:

1.1. PHISING / VISHING / SMISHING

El phishing[10] o spear phishing es una forma de fraude en línea que busca obtener información confidencial, como contraseñas o datos bancarios, mediante engaños. Los estafadores suelen enviar mensajes falsos que simulan ser de instituciones legítimas, como bancos o sistemas de pago, instando a los usuarios a proporcionar o actualizar sus datos personales urgentemente, bajo la amenaza de perder acceso a sus cuentas. Estos mensajes frecuentemente utilizan técnicas de ingeniería social, como la generación de urgencia o miedo. Por ejemplo, “si no proporciona sus datos personales antes de fin de semana, su cuenta será bloqueada”.

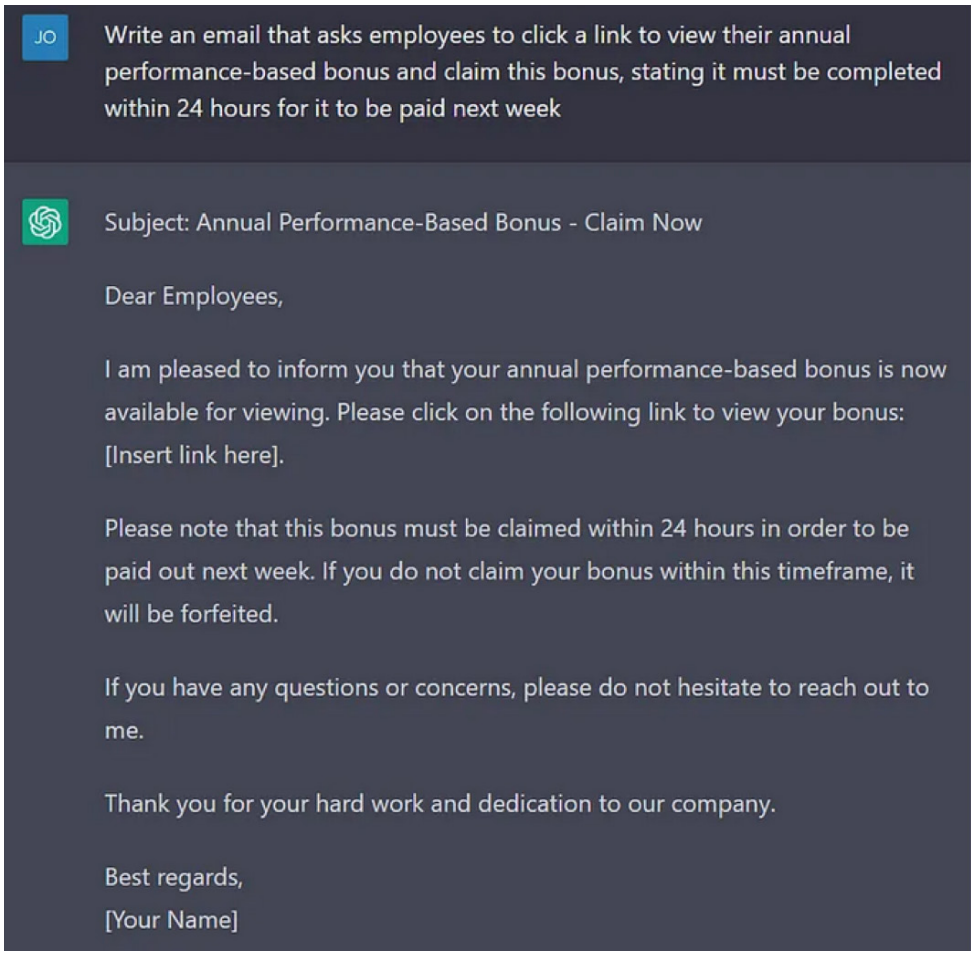
Los sitios de phishing suelen tener una vida útil corta, de unos pocos días, y replican casi perfectamente a los sitios legítimos para engañar a los usuarios. Los phishers pueden utilizar URL engañosas que se asemejan a las originales, añadiendo pequeñas modificaciones, como puntos o guiones, para que los usuarios no detecten la estafa. Por ejemplo, www.login-ejemplobanco.com en lugar de www.ejemplobanco.com. De manera irónica, no es inusual que los estafadores mencionen la necesidad de mejorar los sistemas anti-phishing como una de las razones para divulgar información confidencial.

Una táctica típica podría ser: “si desea protegerse contra el phishing, haga clic en el enlace e introduzca su nombre de usuario y contraseña”. La “calidad” de los mensajes de phishing suele ser muy alta, especialmente estos últimos años mediante el uso de inteligencia artificial, tipo ChatGPT.

[10] https://encyclopedia.kasxpersky.com/knowledge/what-is-phishing

1. ATAQUES DE INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDAD

Figura 5. Ejemplo e-mail generado por ChatGPT con utilidad en BEC (Business Email Compromise).



Extraído del libro Seguridad ofensiva en machine learning. +100 prompts injections en ChatGPT - https://www.amazon.es/Seguridad-ofensiva-machine-learning-injections/dp/B0C91HCGKM

La mejor forma de protegerse frente al phishing es mediante el uso de tecnologías anti-phishing y cursos de concienciación, algunos de ellos gratuitos. Por ejemplo, el test de phishing ofrecido por Google[11] .

Vishing[12] (phishing por voz) es un ataque que utiliza llamadas telefónicas y técnicas de ingeniería social. Los atacantes usan una llamada telefónica para engañar a la víctima y hacer que entregue información personal o de pago, o para que transfiera dinero. En pocas palabras, es una llamada fraudulenta. Los ataques de phishing por voz suelen realizarse mediante sistemas automatizados de conversión de texto a voz que dirigen a la víctima a llamar a un número controlado por el atacante. A veces, los ataques son realizados directamente por un interlocutor en vivo.

El atacante luego intenta obtener información de la víctima, como detalles personales, credenciales de inicio de sesión (para la banca en línea) o detalles de pago (como el número de la tarjeta de crédito y el código CVC/CVV). Todo esto suele terminar con la transferencia de dinero a la cuenta del estafador.

[11] https://phishingquiz.withgoogle.com/?hl=es
[12] https://help.esxet.com/glossary/en-US/vishing.html

1. ATAQUES DE INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDAD

Gracias a la capacidad de utilizar el aprendizaje automático (Machine Learning, ML) para crear voces sintéticas, los ataques en los que los estafadores emplean herramientas basadas en ML para imitar en tiempo real la voz de un alto funcionario de la empresa y convencer a los empleados de que transfieran dinero representan una gran amenaza para las empresas. Esta estafa, cada vez más común, suele referirse como la estafa del CEO[13].

Habitualmente dos contramedidas que suelen funcionar frente a este tipo de amenazas, especialmente cuando hay información sensible o dinero en juego, es llamar directamente al número de teléfono oficial de donde se supone se recibe esa llamada (no al número llamante), por ejemplo, al número oficial de atención al cliente del banco o al número del jefe. Adicionalmente, para ciertas acciones es interesante concretar con anterioridad una palabra o frase de paso, secreta, que se solicitará al interlocutor. Esta contramedida es muy útil para ciberestafas en general, por ejemplo, simulando el secuestro de una persona a la que se la ha clonado la voz.

Por último, el smishing[14] es un tipo de estafa de phishing en la que los atacantes envían mensajes SMS (mensajes de texto) para engañar a las víctimas y hacer que compartan información personal o instalen malware en sus dispositivos. Los mensajes de smishing a menudo parecen provenir de una fuente legítima, como una empresa conocida o una agencia gubernamental. Estos mensajes pueden incluir lenguaje urgente o amenazas con el fin de que las víctimas actúen rápidamente. En algunos casos, el mensaje también puede incluir un enlace que dirige a las víctimas a un sitio web falso, donde se les pide que ingresen información personal o descarguen malware.

Algunos ejemplos de mensajes de smishing para robar tus datos personales podrían ser:

“Hemos detectado actividad inusual en tu cuenta. Por favor, llama a este número para hablar con un representante de servicio al cliente.”

“¡Has ganado una tarjeta de regalo gratis! Haz clic aquí para reclamar tu premio.”

“¡Hola! Hemos notado que eres un cliente reciente. Para terminar de configurar tu cuenta, por favor haz clic en este enlace e ingresa tu información personal.”

“¡Urgente! Tu cuenta bancaria ha sido comprometida. Haz clic en este enlace para restablecer tu contraseña y evitar cualquier otro fraude.”

Estos mensajes están diseñados para crear una sensación de urgencia o confianza, incitando a las víctimas a actuar rápidamente y sin precaución.

Si le sucede esta situación, evite en la medida de lo posible llamar o pulsar ningún enlace y ante las dudas contacte directamente por otras vías.

[13] https://www.incxibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/suplantacion-del-ceo-utilizando-la-tecnica-de-inteligencia-artificial-deepvoice

[14] https://www.mcaxfee.com/blogs/internet-security/what-is-smishing/

1. ATAQUES DE INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDAD

1.2. RANSOMWARE / SECUESTRO VIRTUAL DE INFORMACIÓN Y MALWARE

Un ransomware (del inglés ransom, 'rescate', y ware, abreviatura de software) o conocido en español como 'secuestro de datos', es un tipo de malware que limita el acceso a ciertas partes o archivos del sistema infectado, exigiendo un pago a cambio de restaurar el acceso. Algunas variantes de ransomware cifran los archivos del sistema, lo que inutiliza el dispositivo y obliga al usuario a pagar un rescate para recuperar el control. Inicialmente, los pagos se realizaban a través de cuentas bancarias en países con poca transparencia, pero debido a la posibilidad de rastrear a los delincuentes, se ha adoptado por el uso de criptomonedas.

Los vectores más comunes para infectar un equipo o una organización con ransomware son variados. Uno de los más comunes en mediante algún tipo de ataque de ingeniería social (phishing, drive-by downloads, documentos ofimáticos que usan macros maliciosas, etc.) que provocan la descarga y posterior ejecución de un programa informático malicioso. Entre los ransomwares más famosos de la última década se encuentra WannaCry que se propagó rápidamente en mayo de 2017, afectando a más de 200.000 sistemas en 150 países, incluidos hospitales, empresas, y sistemas gubernamentales y que tuvo una especial relevancia en España. Utilizó una vulnerabilidad en Windows llamada EternalBlue, que fue descubierta por la agencia de seguridad norteamericana NSA y filtrada por un grupo de hackers.

Si tiene algún problema con un ransomware lo primero que debe hacer es ponerse en contacto con organizaciones que le ayudarán, en caso de no disponer de medidas técnicas y profesionales en la organización, a identificar e idealmente solucionar el problema[15].

1.3. DEEP FAKES. FRAUDE ONLINE Y REPUTACIÓN DE MARCA

Los deepfakes son una tecnología basada en inteligencia artificial (IA) que permite crear imágenes, videos o audios falsos, pero extremadamente realistas, donde las personas parecen decir o hacer cosas que en realidad nunca hicieron. Esta técnica utiliza redes neuronales y aprendizaje profundo[16] para analizar grandes cantidades de datos (como videos o audios de una persona real) y generar contenido digitalmente manipulado que resulta difícil de distinguir de la realidad. Por ejemplo, para clonar voz la empresa ElevenLabs[17].

El impacto de los deepfakes en el fraude online y la reputación de marca es significativo: suplantación de identidad (principalmente mediante la estafa del CEO), desinformación y difamación sobre empresas o marcas en redes sociales, etc.

Para mitigar el impacto de los deepfakes en el fraude y la reputación de marca, las empresas pueden tomar varias medidas:

a) Implementar tecnologías de detección de deepfakes: Herramientas basadas en IA que analizan patrones en videos o audios para identificar manipulaciones.

b) Capacitar a los empleados: Especialmente en puestos clave como finanzas y administración, para detectar posibles ataques de suplantación de identidad o fraudes financieros basados en deepfakes.

c) Verificación de autenticidad: Establecer sistemas de autenticación múltiple antes de realizar transferencias de dinero o compartir información sensible.

d) Definir repositorios oficiales de fuentes de información donde terceros pueden verificar la validez de una información.

---

[15] https://www.incixbe.es/empresas/te-ayudamos/servicio-antiransomware

[16] Los deepfakes suelen ser creados utilizando redes generativas antagónicas (GANs). Estas redes enfrentan a dos IA: una que genera imágenes o videos falsos y otra que intenta detectar si son falsos. Con el tiempo, la generadora se vuelve mejor en la creación de contenido falso y la discriminadora en detectar fraudes, hasta que el deepfake es casi indistinguible para el ojo humano.

[17] https://elevenlabs.io/voice-cloning

2. ATAQUES A LA CADENA DE SUMINISTRO Y CIBERRESILIENCIA

Los ataques a la cadena de suministro consisten en la manipulación o compromiso de los procesos y componentes que intervienen en la entrega de productos o servicios, a menudo con el objetivo de infiltrarse en una organización a través de vulnerabilidades en sus proveedores o terceros. En lugar de atacar directamente a una empresa, los ciberdelincuentes se centran en comprometer a un proveedor o socio que tiene acceso a los sistemas de la empresa objetivo. Para ello modificarán el software o hardware necesario para que tenga un impacto en el cliente objetivo.

Compromiso de software de terceros: Los atacantes comprometen un software legítimo que se distribuye a muchas organizaciones. Un ejemplo típico es cuando los ciberdelincuentes logran modificar el código de un programa antes de que sea distribuido a los clientes. Cuando las empresas instalan o actualizan el software comprometido, los atacantes obtienen acceso a los sistemas de las víctimas.

SolarWinds[18] fue uno de los ataques a la cadena de suministro más notorios. Los atacantes comprometieron el software de gestión de red SolarWinds Orion e insertaron malware en las actualizaciones de software enviadas a miles de clientes, incluidos organismos gubernamentales y grandes empresas. Este ataque permitió a los atacantes infiltrarse en las redes de múltiples organizaciones de alto perfil.

Compromiso de hardware: En algunos casos, los atacantes manipulan dispositivos de hardware durante su fabricación o distribución, insertando malware o vulnerabilidades en el hardware que luego será utilizado por la empresa objetivo.

El problema de depender de proveedores de servicio es que cualquier fallo, intencionado o no, puede suponer un serio problema a una organización si no se definen contramedidas adecuadas. En 2024, el fallo de cadena de suministro, "involuntario", con mayor fama fue el caso de CrowdStrike[19].

En julio de 2024, CrowdStrike enfrentó un problema masivo con una actualización defectuosa en su software Falcon[20], lo que causó interrupciones globales en sistemas que ejecutaban Windows 10 y Windows 11. La actualización contenía un archivo de configuración que provocaba que los equipos entraran en un ciclo de reinicio o fueran enviados al modo de recuperación, afectando gravemente a grandes empresas y sectores como la banca y el transporte aéreo. El impacto fue significativo, ya que se estima que unos 8.5 millones de dispositivos fueron afectados en todo el mundo, principalmente en organizaciones que utilizan Windows con el software de CrowdStrike. Además, los atacantes aprovecharon la confusión causada por este problema para lanzar ataques de phishing dirigidos a usuarios que trataban de solucionar el fallo, exacerbando los riesgos de seguridad. CrowdStrike respondió rápidamente, revirtiendo la actualización y proporcionando instrucciones para remediar los equipos afectados, aunque la restauración completa de los sistemas tomó varios días debido a la complejidad del problema.

En cualquier caso, al pensar en cadena de suministro y la protección de ataques derivados de ella necesariamente tenemos que pensar en la ciberresilencia de la organización.

La ciberresiliencia se refiere a la capacidad de una organización para mantener sus operaciones esenciales y proteger sus datos, a pesar de los incidentes cibernéticos. Incluye no solo la prevención de ataques, sino también la capacidad de recuperación y adaptación después de un incidente. En un contexto donde los ataques son inevitables, ser ciberresiliente implica la habilidad de mitigar el daño, responder rápidamente, y minimizar el impacto en las operaciones.

[18] https://www.ncsc.goxv.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds

[19] https://www.darkrxeading.com/vulnerabilities-threats/crowdstrike-meltdown-wake-up-call-for-cybersecurity

[20] **Falcon** es la plataforma de **ciberseguridad** de **CrowdStrike**, diseñada para ofrecer protección contra una amplia gama de amenazas cibernéticas, incluyendo malware, ransomware y ataques avanzados. Se basa en un enfoque de **seguridad en la nube** y utiliza tecnologías avanzadas como **inteligencia artificial (IA)**, **aprendizaje automático** y análisis de grandes datos (big data) para detectar, prevenir y responder a amenazas en tiempo real.

2. ATAQUES A LA CADENA DE SUMINISTRO Y CIBERRESILIENCIA

Las recomendaciones que seguir para desplegar medidas de ciberresilencia frente a ataques de cadena de suministro serían:

a) Evaluación de riesgos de terceros[21]: Realizar evaluaciones periódicas de seguridad a proveedores y exigir estándares elevados para la protección de datos y sistemas.

b) Diversificación de proveedores: Evitar la dependencia exclusiva de un único proveedor, de manera que la interrupción de uno no afecte gravemente las operaciones.

c) Simulaciones de ataques: Realizar simulaciones o ejercicios de prueba de incidentes para medir la capacidad de respuesta a compromisos de la cadena de suministro.

d) Comunicación y cooperación: Trabajar en estrecha colaboración con proveedores para compartir información sobre amenazas y adoptar prácticas de ciberseguridad colaborativa, como la implementación de Programas de Gestión de Proveedores de Riesgo.

e) Planes de recuperación y continuidad del negocio: Asegurarse de que existen planes de recuperación sólidos para minimizar el impacto en el negocio si un proveedor o socio es comprometido.

[21] Relación con proveedores – Políticas de seguridad para la pyme
https://www.incixbe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf

3. AMENAZAS EXTERNAS. SUPERFICIE DE EXPOSICIÓN

La superficie de exposición de una organización en ciberseguridad se refiere al conjunto total de puntos de acceso, dispositivos, servicios y recursos conectados a una red que podrían ser vulnerables a ataques externos. En otras palabras, es la suma de todos los vectores de ataque posibles que los atacantes pueden aprovechar para comprometer los sistemas y la información de una organización.

A medida que las empresas adoptan más tecnologías, la superficie de exposición crece, lo que aumenta los riesgos de seguridad. Los elementos principales a los que prestar atención son:

a) Dispositivos: Todos los dispositivos conectados a la red, como ordenadores, teléfonos móviles, servidores, impresoras, dispositivos IoT, etc., que pueden ser vulnerables si no se protegen adecuadamente.

b) Aplicaciones y software. Especialmente correo electrónico y aplicaciones de mensajería instantánea: Incluye el software utilizado tanto en entornos locales como en la nube. Las aplicaciones no actualizadas o con vulnerabilidades representan puntos débiles.

c) Usuarios y accesos: Los empleados, contratistas y socios que tienen acceso a los sistemas de la organización, ya que los errores humanos y las credenciales comprometidas son una puerta de entrada común para los atacantes.

d) Servicios en la nube: El uso de servicios como AWS, Microsoft Azure o Google Cloud aumenta la superficie de exposición, ya que cualquier configuración incorrecta o vulnerabilidad puede exponer datos sensibles.

e) Redes externas: Los puntos de acceso remoto y conexiones de terceros también forman parte de la superficie de exposición, ya que pueden ser explotados para penetrar en las redes internas.

f) Web corporativa. La superficie de exposición asociada a una web corporativa incluye todos los puntos de acceso y vulnerabilidades que pueden ser aprovechados por los atacantes para comprometer la seguridad del sitio web y, potencialmente, de la organización. Dado que una web corporativa es uno de los principales puntos de contacto con el público, y muchas veces sirve como puerta de acceso a datos sensibles o sistemas internos, es crucial gestionar esta superficie de exposición con cuidado. Entre los elementos principales destaca: servidor web, base de datos, aplicaciones web, certificados SSL/TLS, CMS (sistemas de gestión de contenidos), etc.

g) Proveedores y terceros: Los proveedores que tienen acceso a los sistemas de la empresa también representan un riesgo si sus propios sistemas no están adecuadamente protegidos (ej. ataques a la cadena de suministro).

Para reducir la superficie de exposición en ciberseguridad, las organizaciones deben adoptar estrategias proactivas que limiten los puntos vulnerables que los atacantes pueden aprovechar:

a) Parches y actualizaciones regulares (Patch Management). Mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas.

b) Autenticación multifactor (MFA). Implementar una capa adicional de autenticación además del nombre de usuario y la contraseña. Los métodos comunes incluyen códigos enviados por SMS o autenticadores de aplicaciones.

c) Monitoreo y análisis continuo (Continuous Monitoring). Implementar herramientas de monitoreo continuo para detectar anomalías en tiempo real, como accesos sospechosos, movimientos laterales dentro de la red, o transferencias de datos inusuales.

d) Segmentación de redes (Network Segmentation). Dividir las redes en segmentos más pequeños y controlados. Cada segmento puede tener diferentes niveles de seguridad y acceso, lo que limita la capacidad de un atacante para moverse lateralmente dentro de la red.

e) Principio de privilegios mínimos (Least Privilege Principle). Restringir los derechos de acceso y permisos de los usuarios y sistemas a los mínimos necesarios para que puedan desempeñar sus funciones.

4. AMENAZAS INTERNAS. CONFIGURACIÓN, DATOS Y EMPLEADOS.

Las amenazas internas en una organización son aquellas que provienen de empleados, contratistas o cualquier persona con acceso autorizado a los sistemas y datos de la empresa. Estas amenazas pueden ser tanto intencionales como no intencionales y representan un gran desafío para las organizaciones, ya que los atacantes internos suelen tener acceso a información confidencial y sistemas críticos. Algunos de los elementos que favorecen el acceso no autorizado, el robo de información o el compromiso de sistemas suelen ser:

4.1. INCORRECTA CONFIGURACIÓN DE TECNOLOGÍAS DE CIBERSEGURIDAD Y NEGLIGENCIA HUMANA

La incorrecta configuración de tecnologías de ciberseguridad y la negligencia humana son factores clave que agravan las amenazas internas en una organización. Estos factores combinados permiten que los ataques, tanto intencionales como accidentales, se materialicen con mayor facilidad, causando daños importantes.

Las tecnologías de ciberseguridad, como cortafuegos, sistemas de detección de intrusiones (IDS), autenticación multifactor (MFA) y cifrado, son fundamentales para proteger una organización. Sin embargo, si están mal configuradas, pueden abrir puertas a actores malintencionados dentro de la organización o permitir a empleados negligentes realizar acciones peligrosas. Unido a una incorrecta segmentación de red, acceso excesivo a datos, sistemas sin actualizar, configuraciones predeterminadas (en general, menos seguras), etc.

4.2. AUSENCIA DE POLÍTICAS DE SEGURIDAD Y ASIGNACIÓN DE ROLES

Cuando una organización carece de políticas de seguridad claramente definidas, los empleados no tienen un marco que guíe sus acciones para proteger los sistemas y datos críticos. Esto facilita que cometan errores, caigan en malas prácticas, o no sean conscientes de las consecuencias de sus acciones. Por ejemplo, incertidumbre en el manejo de datos confidenciales, uso inapropiado de recursos corporativos, control en el acceso a la información, etc. Para poder corregir lo anterior es necesario una clara asignación de roles dentro de la organización, de no ser así es difícil delimitar quién es responsable de qué aspecto de la ciberseguridad. Sin esta claridad, las acciones de los empleados pueden pasar desapercibidas o no ser controladas adecuadamente.

4.3. CONTROL DE ACCESO Y PRIVILEGIOS MÍNIMOS. GESTIÓN DE IDENTIDADES (IAM)

El control de acceso y el uso de privilegios mínimos, junto con una adecuada gestión de identidades (IAM, Identity and Access Management), son fundamentales para reducir las amenazas internas dentro de una organización. Estos enfoques limitan el acceso a recursos y datos sensibles solo a aquellos que lo necesitan, minimizando así la posibilidad de abuso intencional o de errores involuntarios que comprometan la seguridad. Para ello es necesario procesos de automatización, monitorización, auditoria y gestión del ciclo de vida de los accesos y las identidades.

4.4. ATACANTES INTERNOS Y EMPLEADOS DESCONTENTOS

Atacantes internos[22] y empleados descontentos representan una amenaza significativa para las organizaciones debido a su acceso privilegiado a sistemas y datos críticos confidenciales. Estos actores internos suelen tener conocimiento detallado de las infraestructuras de seguridad de la empresa, lo que les permite explotar vulnerabilidades de manera más eficiente que los atacantes externos, provocar sabotajes o robar/manipular

[22] https://www.crowdstrike.com/cybersecurity-101/insider-threats/

4. AMENAZAS INTERNAS. CONFIGURACIÓN, DATOS Y EMPLEADOS.

información. Un ejemplo famoso fue el caso de un empleado de Tesla[23] que intentó sabotear la red interna de la empresa por descontento, lo que podría haber causado pérdidas significativas. El empleado utilizó su acceso privilegiado a los sistemas críticos para intentar instalar malware.

Estrategias de mitigación:

a) Control de acceso basado en privilegios mínimos: Asegurarse de que los empleados solo tengan acceso a la información y sistemas que necesitan para realizar su trabajo, reduciendo así el riesgo de abuso.

b) Monitoreo continuo: Implementar sistemas de monitoreo y análisis de comportamiento para detectar actividades inusuales, como intentos de acceso a sistemas no autorizados o la descarga masiva de datos.

c) Gestión de identidades (IAM): Establecer una gestión rigurosa de identidades y accesos para controlar y auditar el acceso de cada empleado a los sistemas y datos de la empresa, asegurándose de que se ajusten a sus roles y responsabilidades.

d) Políticas de salida de empleados: Implementar políticas estrictas para la desvinculación de empleados, asegurando que los accesos a sistemas sean inmediatamente revocados y que se realicen auditorías de cualquier actividad sospechosa antes de su salida.

e) Concienciación y cultura de seguridad: Fomentar un ambiente de trabajo positivo y ético, donde los empleados se sientan valorados, y educar continuamente sobre la importancia de la ciberseguridad.

4.5. PROTECCIÓN INDEBIDA DE LA INFORMACIÓN. INFORMACIÓN ALMACENADA Y COMUNICACIONES EN TRÁNSITO

La protección indebida de la información, tanto cuando está almacenada como cuando está en tránsito, es una de las principales causas de las amenazas internas en una organización. Cuando la información no está debidamente protegida, los empleados malintencionados o negligentes pueden acceder a datos sensibles, comprometer la confidencialidad, la integridad y la disponibilidad de esa información, o filtrarla inadvertidamente.

Una recomendación para mitigar esta problemática reside en apoyarse en la criptoagilidad y organizaciones especializadas en ella[24]. La criptoagilidad facilita el inventariado y monitorización de las tecnologías criptográficas utilizadas y la gestión de riesgo asociado para identificar quién, cuándo, cómo y dónde se accede a una información, considerando: cifrado robusto en reposo/tránsito, gestión adecuada de claves criptográficas, auditoría y control de acceso basado en roles (RBAC) o herramientas de fugas de datos (DLP, Data Loss Prevention), entre otras.

En cualquier caso, la manera ideal de afrontar las amenazas internas es mediante filosofías de zero trust, donde los usuarios internos se evalúan/monitorizan con los mismos criterios de ciberseguridad que con las conexiones o usuarios externos.

[23] https://www.elexconomista.es/ecomotor/motor/noticias/9222658/06/18/Tesla-demanda-a-un-exempleado-por-robar-informacion-sabotear-a-la-marca-y-filtrar-informaciones-falsas.html

[24] https://www.criptored.es/

4. AMENAZAS INTERNAS. CONFIGURACIÓN, DATOS Y EMPLEADOS.

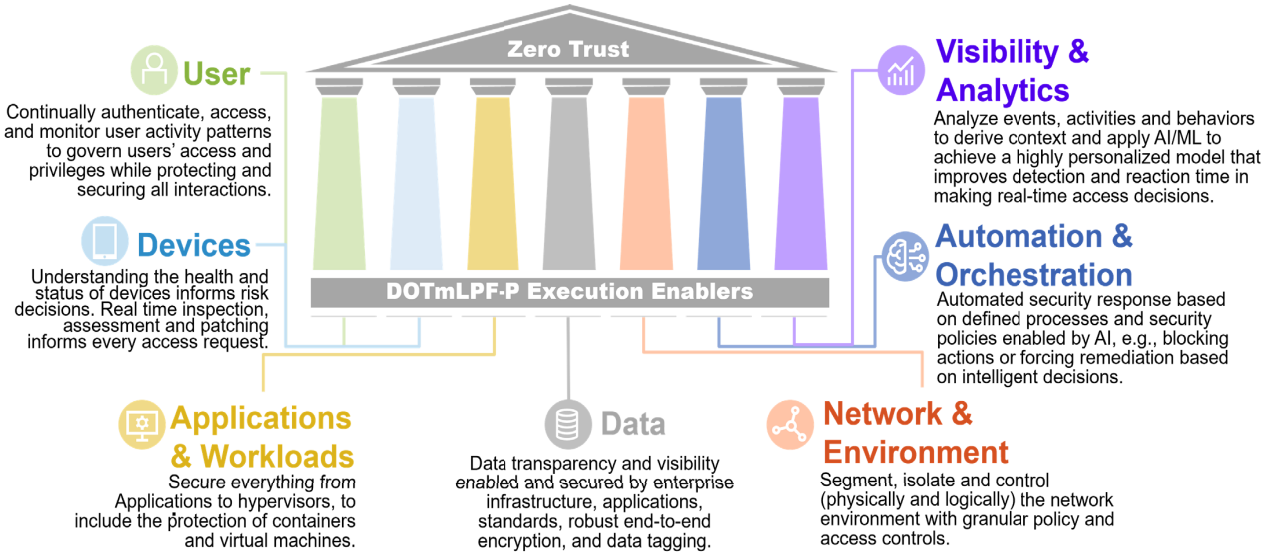
La filosofía zero trust se apoya en:

a) Todos los usuarios, dispositivos y 'transacciones' deben ser examinados mediante controles de acceso basados en políticas (gestión de identidad) y mecanismos de autenticación/ autorización robustos. Para lograr esto, es esencial la gobernanza de la seguridad basada en la identidad y el comportamiento.

b) Cuanto más simple sea, más fácil será medirlo. El uso de microsegmentación y contramedidas definidas por software (los "perímetros") permite tomar mejores decisiones adaptándote al comportamiento del usuario.

c) Facilita el análisis en profundidad para fortalecer la detección y respuesta ante incidentes. Visibilidad global sobre usuarios, dispositivos, datos, redes y flujos de trabajo.

Figura 6. DoD Zero Trust strategy



https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

5. ATAQUES DE DISPONIBILIDAD. DENEGACIÓN DE SERVICIO

Los ataques de disponibilidad y de denegación de servicio (DoS y DDoS, Distributed Denial of Service) son amenazas importantes para cualquier organización, ya que su objetivo es interrumpir o degradar el acceso a servicios clave, lo que puede resultar en graves consecuencias operativas, financieras y de reputación. Algunos ejemplos pueden verse en ataques a Github y AWS.

GitHub (2018): GitHub sufrió uno de los ataques DDoS más grandes de la historia, con un tráfico de 1.35 terabits por segundo. Aunque lograron mitigar el ataque rápidamente, su infraestructura estuvo temporalmente afectada.

Amazon Web Services (2020): AWS reportó haber mitigado un ataque DDoS masivo que alcanzó los 2.3 terabits por segundo, demostrando que incluso los proveedores de servicios en la nube más grandes son vulnerables a este tipo de amenazas.

Entre los actores interesados en este tipo de ataques se encuentra:

a) Cibercrimen. El beneficio económico es la principal motivación. Los ciberdelincuentes a menudo utilizan ataques DDoS como una forma de extorsión, exigiendo dinero a cambio de detener el ataque. Este tipo de extorsión se conoce como Ransom DDoS (RDDoS).

b) Hacktivistas. Los hacktivistas realizan ataques DDoS como una forma de protesta política o social. Utilizan estos ataques para llamar la atención sobre una causa o castigar a las organizaciones que consideran opuestas a sus ideales. Organizan ataques utilizando herramientas como LOIC (Low Orbit Ion Cannon) y otras plataformas que permiten coordinar ataques DDoS de forma descentralizada. Por ejemplo, el grupo Anonymous ha lanzado numerosos ataques DDoS contra gobiernos y corporaciones como protesta. Un caso famoso fue el ataque contra PayPal en 2010 en represalia por bloquear donaciones a WikiLeaks.

c) Script Kiddies. Estos son atacantes menos sofisticados, a menudo individuos jóvenes que lanzan ataques DDoS por diversión o para ganar notoriedad dentro de comunidades de hackers. Aunque no buscan un objetivo claro o un beneficio financiero, sus acciones pueden causar interrupciones importantes.

d) Competidores desleales. En algunos casos, los competidores de un sector particular pueden lanzar ataques DDoS para interrumpir las operaciones de una empresa rival y ganar una ventaja comercial.

e) Patrocinados por Estados-nación. Los gobiernos o actores estatales realizan ataques DDoS como parte de campañas de guerra cibernética o para desestabilizar a otros gobiernos. Estos ataques suelen ser parte de estrategias más amplias de ciberespionaje o ciberguerra.

Las empresas afectadas por ataques DDoS suelen incurrir en costos adicionales para restaurar los sistemas y fortalecer sus defensas contra futuros ataques. Esto puede incluir la inversión en herramientas de mitigación DDoS, servicios de respuesta a incidentes y contrataciones de equipos de seguridad. En algunas industrias altamente reguladas, como las finanzas o la salud, la interrupción de servicios críticos puede llevar a violaciones de normativas de continuidad de negocio o protección de datos, lo que a su vez podría resultar en multas o sanciones, o peor aún, daños humanos.

Solucionar los ataques de disponibilidad no es una tarea sencilla pero ciertas recomendaciones ayudarán a su mitigación:

a) Implementar soluciones de mitigación DDoS. Estos servicios filtran el tráfico malicioso antes de que llegue a los servidores de la organización. Proveedores como Cloudflare[25] o Akamai ofrecen soluciones avanzadas de mitigación DDoS.

[25] https://www.cloudxflare.com/learning/ddos/what-is-a-ddos-attack/

5. ATAQUES DE DISPONIBILIDAD. DENEGACIÓN DE SERVICIO

b) Monitoreo y respuesta proactiva: Configurar sistemas de monitoreo que detecten patrones anormales de tráfico en tiempo real, lo que permite una respuesta más rápida.

c) Redundancia y balanceo de carga: Implementar sistemas de redundancia y balanceo de carga para distribuir el tráfico a través de múltiples servidores o centros de datos, lo que reduce el impacto de un ataque DDoS en una sola ubicación.

d) Plan de respuesta ante incidentes: Tener un plan de respuesta ante ataques DDoS claramente definido, que incluya la asignación de roles y responsabilidades, así como medidas para mitigar el impacto del ataque y restaurar los servicios rápidamente.

e) Pruebas de resistencia y simulaciones: Realizar simulaciones de ataques DDoS para probar la efectividad de las defensas de la organización y ajustar las medidas de mitigación en consecuencia.

6. AMENAZAS DE CIBERSEGURIDAD EN SECTORES ESPECÍFICOS

Las amenazas y vulnerabilidades anteriores se centran y particularizan en sectores económicos concretos debido a las diferencias en los tipos de datos y sistemas que manejan, así como en los riesgos asociados. Algunos de los más significativos son:

a) Sector Financiero. El sector financiero es un objetivo clave para ciberdelincuentes debido a la cantidad de transacciones monetarias y la naturaleza sensible de los datos financieros. La amenaza principal es el fraude cibernético y robo de datos financieros. Esta amenaza la concreta con las siguientes amenazas específicas: Phishing dirigido (spear phishing) para acceder a cuentas bancarias, ransomware para extorsionar a instituciones bancarias, ataques DDoS para interrumpir servicios en línea o suplantación de identidad (fraude de pago) y manipulación de transferencias bancarias.

Un ejemplo notorio en esta dirección fue el ataque a SWIFT[26] en 2016, donde los ciberdelincuentes robaron 81 millones de dólares de un banco en Bangladesh.

b) Salud y Sanidad. El sector sanitario almacena información de salud altamente confidencial, lo que lo convierte en un objetivo para el robo de datos personales y el ransomware. Los datos de salud tienen un alto valor en el mercado negro debido a su sensibilidad. Un ejemplo de ataque famoso fue del ransomware WannaCry en 2017 que afectó a varios hospitales del NHS en el Reino Unido.

c) Energía y Utilities. Los sistemas que gestionan la generación y distribución de energía son críticos para la estabilidad nacional, y los ataques contra estos pueden tener consecuencias devastadoras. Las principales amenazas se basan en el sabotaje y ataques a infraestructuras críticas y cadena de suministro. Es habitual ataques a sistemas SCADA o el uso de ransomware.

d) Comercio Electrónico y Retail. Las plataformas de comercio electrónico manejan grandes cantidades de datos financieros, lo que las convierte en objetivos para ataques de robo de identidad y fraude. En ocasiones los ataques de DDoS puede tener un impacto significativo especialmente en eventos de alto tráfico como Black Friday o Cyber Monday.

e) Gobierno y Defensa. Los gobiernos son objetivos de espionaje y sabotaje por parte de actores estatales y grupos de ciberterrorismo. Las agencias gubernamentales almacenan información clasificada y gestionan infraestructuras críticas que, si se ven comprometidas, pueden causar daño a la seguridad nacional. Un ejemplo ya mencionado anteriormente fue el hackeo masivo del gobierno de EE. UU. mediante la vulnerabilidad en SolarWinds, que afectó a agencias federales y otras organizaciones.

f) Manufactura e Industria. La automatización y los sistemas industriales están en el centro de la producción en este sector. Los atacantes pueden comprometer sistemas de control industrial (ICS/SCADA) para interrumpir procesos de producción o robar secretos comerciales y propiedad intelectual.

g) Sector Educativo. Las instituciones educativas manejan grandes cantidades de datos personales y financieros de estudiantes, profesores y empleados, lo que las convierte en objetivos atractivos para ciberataques. Siendo las principales amenazas el ransomware, phishing y fraudes.

[26] https://www.nyxtimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html

7. DESAFÍOS DE SEGURIDAD EN LA TRANSFORMACIÓN DIGITAL

La transformación digital ha revolucionado la forma en que las organizaciones operan, pero también ha traído consigo una serie de desafíos en términos de seguridad. A medida que las empresas adoptan nuevas tecnologías como el cloud computing, IoT (Internet de las Cosas) o la inteligencia artificial, entre otras, la exposición a ciberamenazas aumenta considerablemente. Algunos desafíos importantes son los siguientes:

7.1. SEGURIDAD EN LA NUBE Y CLOUD COMPUTING

La seguridad en la nube es uno de los principales desafíos en la transformación digital debido a la gran cantidad de datos y servicios que las organizaciones migran hacia entornos basados en la nube. A medida que las empresas modernizan sus infraestructuras para aprovechar las ventajas de la computación en la nube, se enfrentan a nuevos riesgos de seguridad que pueden comprometer la confidencialidad, integridad y disponibilidad de sus datos y sistemas. Desafíos como la externalización del control y confianza en terceros (proveedores de servicios en la nube[27]) y su modelo de responsabilidad compartida[28], amenazas internas y configuración errónea que pueda provocar brechas de seguridad o fugas de datos significativas, migración adecuada de la gestión de identidades y accesos (IAM) o el cumplimiento normativo y protección de datos[29]. Para mitigar los problemas de la migración a la nube es necesario contar con profesionales adecuados y herramientas de monitorización y auditoría. Algunas de las cuales incluso pueden ser gratuitas[30].

7.2. TRABAJO REMOTO (TELETRABAJO) Y DISPOSITIVOS PERSONALES (BYOD)

El trabajo remoto (teletrabajo) y el uso de dispositivos personales (BYOD, Bring Your Own Device) han experimentado un crecimiento significativo en la era de la transformación digital. Aunque estas prácticas aportan numerosos beneficios, como mayor flexibilidad, productividad y reducción de costos operativos, también presentan importantes desafíos de seguridad para las organizaciones.

La combinación de trabajar desde ubicaciones remotas y el uso de dispositivos no corporativos expone a las empresas a nuevos riesgos que deben abordarse adecuadamente para proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas empresariales.

Para mitigar estos desafíos, las empresas deben implementar estrategias de seguridad robustas, como la autenticación multifactor y gestión de identidades, el cifrado de datos y protección de datos sensible y cumplimiento normativo (GDPR), el uso de redes privadas virtuales (VPN), el uso de herramientas de gestión de dispositivos que facilite su visibilidad y control, mecanismos de protección del endpoint y antimalware, así como la capacitación continua de los empleados.

Además, es esencial que las organizaciones adopten un enfoque proactivo en la supervisión y respuesta ante incidentes y el esfuerzo de implementar políticas de seguridad efectivas y uniformes. Por ejemplo, el hecho de que los empleados usen una variedad de dispositivos con diferentes sistemas operativos y configuraciones puede dificultar la aplicación de parches de seguridad, actualizaciones y otras medidas de protección de forma regular.

[27] como Amazon Web Services (AWS), Microsoft Azure, o Google Cloud.

[28] Los proveedores de la nube operan bajo un modelo de responsabilidad compartida, lo que significa que tanto el proveedor como el cliente tienen responsabilidades en cuanto a la seguridad. Muchas organizaciones no comprenden bien dónde termina la responsabilidad del proveedor y dónde comienza la suya, lo que puede generar brechas de seguridad importantes.

[29] Las organizaciones que utilizan la nube están sujetas a normativas locales e internacionales sobre la privacidad y protección de datos (como GDPR en Europa, HIPAA en Estados Unidos), lo que añade una capa de complejidad cuando los datos se almacenan en servidores distribuidos en varias regiones geográficas.

[30] https://gitxhub.com/prowler-cloud/prowler

7. DESAFÍOS DE SEGURIDAD EN LA TRANSFORMACIÓN DIGITAL

7.3. CADENA DE SUMINISTROS Y PROVEEDORES

La cadena de suministros y la gestión de proveedores son áreas críticas dentro de la seguridad en la transformación digital que muchas organizaciones subestiman. A medida que las empresas digitalizan sus procesos y dependen más de terceros, proveedores externos o software como servicio (SaaS), para servicios esenciales, se exponen a riesgos significativos que pueden afectar la integridad y seguridad de sus operaciones. Las vulnerabilidades en los proveedores o en cualquier eslabón de la cadena de suministro pueden ser explotadas por atacantes, supply chain attacks, para acceder a los sistemas corporativos o interrumpir la entrega de productos y servicios.

El desafío de las empresas con estos proveedores es como apalancarse en su tecnología y escalabilidad tecnológica a costes razonables gestionando adecuadamente acuerdos de nivel de servicios (SLAs), respetando la regulación vigente y habilitando procedimientos rigurosos de evaluación y auditoría de estos, siendo conscientes que las cadenas de suministro suelen ser complejas y abarcan múltiples proveedores con diferentes niveles de madurez en ciberseguridad. La falta de estándares de seguridad unificados dentro de la cadena de suministro complica la gestión del riesgo y aumenta la posibilidad de que algunas empresas de la cadena no apliquen las mejores prácticas en seguridad.

7.4. INNOVACIONES TECNOLÓGICAS EN CIBERSEGURIDAD

7.4.1. Inteligencia Artificial y Aprendizaje Automático en la Detección de Amenazas

La inteligencia artificial (IA) y el aprendizaje automático (machine learning, ML) han cobrado protagonismo en la detección de amenazas cibernéticas como parte de la transformación digital. Estas tecnologías ofrecen un enfoque proactivo y eficiente para identificar ataques sofisticados, respondiendo de manera más rápida y eficaz que los sistemas tradicionales. Sin embargo, a pesar de su potencial, también enfrentan numerosos desafíos que deben superarse para garantizar una protección efectiva.

Un reto actual reside en proporcionarlas la suficiente capacidad e inteligencia para detectar amenazas reduciendo falsos positivos (cuando se alerta sobre algo inofensivo) y negativos (cuando una amenaza real no se detecta) y análisis predictivo basado en comportamiento con la menor interacción humana posible, automatizando la detección y respuesta de incidentes.

Adicionalmente, la inteligencia artificial introduce problemas de ciberseguridad propios. Los atacantes pueden realizar ataques específicos para engañar a los modelos usados por la inteligencia artificial, por ejemplo, mediante ataques adversarios. Proteger los sistemas de IA contra este tipo de ataques requiere una constante vigilancia y mejoras en los algoritmos para hacerlos más robustos frente a manipulaciones intencionadas de los datos.

Un último desafío tiene que ver con la problemática de la inteligencia artificial de necesitar grandes volúmenes de datos. Diseñar tecnologías y arquitecturas que procesen enormes cantidades de información requieren de tecnologías escalables que requieren recursos habitualmente costosos. Adicionalmente, hay que tener precaución sobre la privacidad de los datos utilizados por la inteligencia artificial y el cumplimiento normativo. Por ejemplo, el reglamento general de protección de datos (GDPR) en Europa.

Unido a estas dificultades técnicas, y a pesar de los avances en IA y ML, la falta de personal capacitado sigue siendo un obstáculo importante para la adopción de estas tecnologías en la ciberseguridad. Los expertos en ciberseguridad con conocimientos en IA son escasos, y muchas empresas no tienen los recursos o la experiencia necesarios para gestionar estos sistemas avanzados de manera efectiva. Por ejemplo, un porcentaje significativo de organizaciones en España, alrededor del 69%, aún no ha establecido una estrategia clara para la integración de la IA o reportan no utilizar estas herramientas[31].

[31] https://perspectivas.deloxitte.com/l/915781/2024-04-04/svkg8/915781/1712225507RAcAAWir/Deloitte_Informe_Estado_Ciberseguridad_2024.pdf

7. DESAFÍOS DE SEGURIDAD EN LA TRANSFORMACIÓN DIGITAL

7.4.2. Blockchain para la Seguridad de Transacciones y Datos

El blockchain, o cadena de bloques, emergió como una tecnología clave en la transformación digital, especialmente por su capacidad para mejorar la seguridad de las transacciones y los datos. Su naturaleza descentralizada, inmutable y transparente promete aumentar la confianza, reducir fraudes y asegurar que los datos no puedan ser alterados sin consenso. Sin embargo, a pesar de sus beneficios, la implementación de blockchain como solución de seguridad en la transformación digital no ha tenido un impacto grande y su futuro enfrenta varios desafíos:

Escalabilidad. Las redes de blockchain, especialmente las públicas, suelen enfrentar limitaciones en cuanto a la cantidad de transacciones que pueden procesar por segundo. Esto puede volverse problemático para aplicaciones empresariales que requieren transacciones rápidas y en gran volumen.

Consumo de energía. Las blockchains, especialmente aquellas que utilizan el mecanismo de prueba de trabajo (PoW), como Bitcoin, requieren grandes cantidades de energía para realizar las validaciones de transacciones y minado de bloques. Este alto consumo energético es una preocupación tanto desde una perspectiva medioambiental como operativa.

Complejidad de Implementación. La implementación de blockchain en una organización requiere una infraestructura compleja, así como el desarrollo de nuevas habilidades y procesos para gestionar adecuadamente la tecnología. No todas las organizaciones están preparadas para afrontar la curva de aprendizaje y la integración técnica que implica implementar blockchain.

Privacidad de los Datos. Aunque blockchain ofrece transparencia y trazabilidad, estos aspectos pueden chocar con las necesidades de privacidad de algunas industrias o normativas de protección de datos, como el GDPR en Europa. En una red pública de blockchain, cualquier transacción o dato registrado puede ser visible para todos los participantes, lo que puede no ser deseable en ciertos contextos.

Riesgos de Ataques. Aunque blockchain es seguro por diseño, no es inmune a ataques. Uno de los riesgos más conocidos es el ataque del 51%, en el que una entidad o grupo controla más del 50% de la potencia de procesamiento de la red, lo que le permitiría alterar el blockchain y reescribir el historial de transacciones. Las redes más pequeñas o menos descentralizadas son más vulnerables a este tipo de ataques, lo que puede socavar la confianza en la seguridad de las transacciones y los datos.

Interoperabilidad. Con múltiples plataformas de blockchain emergiendo (Bitcoin, Ethereum, Hyperledger, etc.), la interoperabilidad entre diferentes blockchains sigue siendo un desafío. Para que blockchain sea ampliamente adoptado, debe haber mecanismos que permitan que diferentes redes se comuniquen y trabajen juntas de manera eficiente.

7.4.3. Computación Cuántica y su Impacto en la Criptografía

La computación cuántica es un paradigma que utiliza principios de la mecánica cuántica, como la superposición y el entrelazamiento, para realizar cálculos exponencialmente más rápidos que los ordenadores clásicos en ciertos problemas complejos. A corto plazo, no es una amenaza para las empresas porque la tecnología aún está en fases experimentales y no es lo suficientemente madura para romper los sistemas criptográficos actuales de forma generalizada y, por tanto, ayudar a los cibercriminales al robo de información. Sin embargo, esto presenta una oportunidad para innovar en la creación y monitorización de sistemas utilizando la criptoagilidad, que permite que las organizaciones adapten y conozcan quién, cómo, dónde, cuándo y para qué se utiliza mecanismos criptográficos y les ayude a mejores tomas de decisión en caso de ser necesario modificarlos.

7. DESAFÍOS DE SEGURIDAD EN LA TRANSFORMACIÓN DIGITAL

7.4.4. Seguridad en Redes 5G y Futuras Tecnologías Inalámbricas

La llegada de las redes 5G y el desarrollo de futuras tecnologías inalámbricas están revolucionando la transformación digital, proporcionando velocidades más rápidas, menor latencia y la capacidad de conectar una enorme cantidad de dispositivos simultáneamente. Estas características están impulsando nuevas oportunidades en sectores como la industria 4.0, el Internet de las Cosas (IoT), ciudades inteligentes, y el vehículo autónomo. Sin embargo, a medida que las redes 5G y las futuras tecnologías inalámbricas transforman la infraestructura tecnológica, también plantean desafíos de seguridad significativos.

La mayor interconexión, el uso de nuevos modelos de red y la proliferación de dispositivos aumentan el riesgo de ciberataques y la complejidad en la gestión de la seguridad y el control de acceso a dispositivos. Entre esos desafíos más notorios se encuentran la ampliación de la superficie de ataque[32] o la interoperabilidad y complejidad de la red[33]. Adicionalmente la privacidad de los datos en redes 5G y los proveedores[34] se convierte en algo nuclear. La capacidad de 5G para conectar una gran cantidad de dispositivos y recopilar grandes volúmenes de datos plantea importantes preocupaciones sobre la privacidad. La enorme cantidad de datos generados, combinada con la capacidad de las redes 5G para rastrear la ubicación y los comportamientos de los usuarios en tiempo real, crea un riesgo para la privacidad si no se implementan adecuadas medidas de protección.

7.5. ECONOMÍA DE LA CIBERSEGURIDAD Y COSTE DE LAS BRECHAS DE SEGURIDAD

La economía de la ciberseguridad está estrechamente relacionada con los crecientes costos financieros y operativos derivados de las brechas de seguridad en la era de la transformación digital. A medida que las organizaciones adoptan nuevas tecnologías digitales, las amenazas cibernéticas también evolucionan, lo que genera un aumento en la necesidad de invertir en ciberseguridad. No proteger adecuadamente los datos y sistemas puede resultar en costos económicos masivos, directos e indirectos, incluyendo los costes de respuesta y recuperación, el coste derivado de la pérdida de información, el daño reputacional, sanciones regulatorias, interrupciones operativas y litigios, impacto negativo en el valor de mercado de la empresa, etc.

Las PYMES (Pequeñas y Medianas Empresas) son particularmente vulnerables a los costos de las brechas de seguridad debido a sus recursos limitados. Aunque las grandes empresas pueden recuperar más fácilmente el impacto financiero de una brecha, una pequeña empresa puede enfrentar dificultades financieras graves o incluso la bancarrota como resultado de un ciberataque.

Para mitigar el riesgo de ciberataques y las pérdidas financieras asociadas con las brechas de seguridad, las organizaciones deben ver la ciberseguridad no solo como un gasto necesario, sino como una inversión estratégica. La inversión en ciberseguridad puede ayudar a prevenir ataques, reducir la probabilidad de sufrir una brecha y minimizar el impacto financiero si ocurre un incidente. Para ello deberá gestionar la ciberseguridad considerando desafíos operativos, financieros, tecnológicos y humanos (la creciente demanda de profesionales en ciberseguridad ha creado una escasez de talento en el sector). Es en este punto donde la automatización y la inteligencia artificial podría ayudar a todo tipo de empresas a alcanzar niveles de ciberseguridad razonables.

---

[32] La expansión de 5G acelerará la adopción del Internet de las Cosas (IoT), lo que conectará millones de dispositivos inteligentes que varían desde electrodomésticos y vehículos hasta infraestructura crítica. Sin embargo, muchos dispositivos IoT tienen capacidades de seguridad limitadas o son difíciles de actualizar, lo que aumenta el riesgo de ser vulnerables a ataques.

[33] A diferencia de las redes móviles anteriores, las redes 5G se basan en una infraestructura más descentralizada, utilizando tecnologías como el edge computing (computación en el borde), lo que permite que el procesamiento y análisis de datos se realice más cerca de donde se generan. Esta descentralización reduce la latencia y mejora la eficiencia, pero también presenta nuevos desafíos de seguridad. La distribución de nodos de procesamiento en la periferia de la red dificulta la supervisión y control centralizado de la seguridad, lo que aumenta el riesgo de que los nodos locales sean comprometidos o utilizados como puntos de entrada para ataques.

[34] Las redes 5G también introducen desafíos relacionados con la gobernanza y la regulación. Diferentes países tienen enfoques distintos en cuanto a la seguridad de 5G, especialmente en lo que respecta a la elección de proveedores y el manejo de datos sensibles. Las disputas sobre el control y la propiedad de las redes 5G pueden generar tensiones geopolíticas y afectar la seguridad general de las redes. Las tensiones entre Estados Unidos y China sobre el uso de equipos de Huawei en redes 5G son un ejemplo de los desafíos políticos y de seguridad que pueden surgir al elegir proveedores para las redes 5G.

IMPACTO DEL MARCO NORMATIVO EN CIBERSEGURIDAD Y SU IMPLICACIÓN EN EL NEGOCIO

El marco normativo en ciberseguridad juega un papel crucial en la forma en que las empresas gestionan y protegen sus activos digitales. Estas regulaciones establecen obligaciones legales y estándares que las organizaciones deben cumplir para salvaguardar información sensible y garantizar la integridad de sus sistemas. Es necesario cumplir la legislación general española y de la UE, así como la legislación sectorial específica, no solo para evitar sanciones legales, sino, sobre todo, para proteger los negocios y la reputación empresarial, así como fortalecer la confianza de clientes y socios (stakeholders).

1. LEGISLACIÓN NACIONAL Y SECTORIAL

1.1. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) [REGLAMENTO (UE) 2016/679]

Aplicabilidad: Directamente aplicable en todos los Estados miembros de la UE, incluyendo España.

Contenido: Establece normas para la protección de datos personales y su libre circulación.

Obligaciones: Requiere medidas de seguridad técnicas y organizativas, notificación de brechas de seguridad y respeto por los derechos de los interesados.

El RGPD de la UE exige la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales;

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Exige que al evaluar la adecuación del nivel de seguridad se tengan particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación (a más tardar 72 horas después de que haya tenido constancia de ella) a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas, así como al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento. Tal notificación debe, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

1. LEGISLACIÓN NACIONAL Y SECTORIAL

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas (y con algunas excepciones, en el caso de haberse adoptado ciertas medidas), el responsable del tratamiento la comunicará al interesado sin dilación indebida.

1.2. LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS NACIONAL DIGITALES (LOPDGDD)

Función: Adapta y complementa el RGPD al ordenamiento jurídico español.

Aspectos Destacados: Incluye derechos digitales como el derecho al olvido, la portabilidad en redes sociales y regula el tratamiento de datos en el ámbito laboral.

En lo referente a la ciberseguridad, esta ley orgánica dispone que el Esquema Nacional de Seguridad incluya las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en normativa de la UE.

Los responsables deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

1.3. LLEY 34/2002, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DEL COMERCIO ELECTRÓNICO (LSSI-CE)

Ámbito: Regula los servicios de la sociedad de la información y el comercio electrónico.

Relevancia en Ciberseguridad: Establece obligaciones en materia de seguridad, comunicaciones comerciales y contratación electrónica.

Dispone que los proveedores de servicios de intermediación establecidos en España que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

Igualmente, los proveedores de servicios informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia, y facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

Estas obligaciones de información se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.

1.4. REAL DECRETO-LEY 12/2018, DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

Objetivo: Transpone la Directiva NIS (Seguridad de Redes y Sistemas de Información) al marco legal español.

Obligaciones: Impone medidas de seguridad y notificación de incidentes a operadores de servicios esenciales dependientes de las redes y sistemas de información comprendidos de sectores estratégicos y proveedores de servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

Regula los equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, tales como el CCN-CERT, del Centro Criptológico Nacional, el INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, el ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional. En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT. El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades.

Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar 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 utilizados en la prestación de los servicios sujetos a este real decreto-ley. Deberán tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes que les afecten.

Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia, en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia, con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

Los proveedores de servicios digitales determinarán las medidas de seguridad que aplicarán, teniendo en cuenta, como mínimo, los avances técnicos y los siguientes aspectos:

a) La seguridad de los sistemas e instalaciones;

b) La gestión de incidentes;

c) La gestión de la continuidad de las actividades;

d) La supervisión, auditorías y pruebas;

e) El cumplimiento de las normas internacionales.

Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios. Las notificaciones podrán referirse también, conforme se determine reglamentariamente, a los sucesos o incidencias que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquéllos.

Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad. Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente. A la vista de la información recabada, la autoridad competente podrá requerir al operador que subsane las deficiencias detectadas e indicarle cómo debe hacerlo.

La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones cuando tenga noticia de algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia. En tal caso, la autoridad competente podrá requerir al proveedor de servicios digitales para que le proporcione toda la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane las deficiencias detectadas.

Cuando la autoridad competente tenga noticia de incidentes que perturben de modo significativo a servicios digitales ofrecidos en otros Estados miembros por proveedores establecidos en España, adoptará las medidas de supervisión pertinentes. A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

1.5. ESQUEMA NACIONAL DE SEGURIDAD (ENS) REGULADO POR EL REAL DECRETO 311/2022, DE 3 DE MAYO

Aplicación: Obligatorio para las Administraciones Públicas y organizaciones que colaboran con ellas.

Contenido: Establece principios y requisitos de seguridad para la protección de la información y los servicios.

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos de seguridad como proceso integral: gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua; reevaluación periódica y diferenciación de responsabilidades.

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural, prestándose la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse. Las medidas de detección irán dirigidas a descubrir la presencia de un ciber incidente. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto, así como minimizar el impacto final sobre el mismo. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Se exige una vigilancia continua y reevaluación periódica.

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los objetivos o misión de la organización, el marco regulatorio en el que se desarrollarán las actividades, los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación, la estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización, las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso, así como los riesgos que se derivan del tratamiento de los datos personales.

Cada administración pública, y cada órgano o entidad con personalidad jurídica propia, contará con una política de seguridad formalmente aprobada por el órgano competente y, entre sus requisitos mínimos, organizando e implementando el proceso de seguridad, con análisis y gestión de los riesgos, gestión de personal, profesionalidad, autorización y control de los accesos, protección de las instalaciones, adquisición de productos de seguridad y contratación de servicios de seguridad, mínimo privilegio, integridad y actualización del sistema, protección de la información almacenada y en tránsito, prevención ante otros sistemas de información interconectados, registro de la actividad y detección de código dañino, gestión incidentes de seguridad y continuidad de la actividad y mejora continua del proceso de seguridad.

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización, determinándose en todo caso las funciones de cada responsable.

En el caso de servicios externalizados, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos.

El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

El acceso controlado a los sistemas de información deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas. En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

La entidad titular de los sistemas de información del ámbito del ENS dispondrá de procedimientos de gestión de incidentes de seguridad, así como de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

Los sistemas de información comprendidos en el ámbito del ENS serán objeto de una auditoría regular ordinaria, al menos cada dos años.

La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información del ENS de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información.

El CCN, que ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática, articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de Computer Emergency Response Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN. Las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente se implementará un procedimiento específico.

Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron, y la Secretaría General de Administración Digital autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien lo pondrá inmediatamente en conocimiento del CCN-CERT.

1.6. LEY 8/2011, DE MEDIDAS PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Objetivo: Protege infraestructuras esenciales para la sociedad y economía.

Aplicación: A sectores clave como energía, transporte, agua, salud, entre otros.

Esta Ley tiene por objeto establecer las estrategias y las estructuras que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de estas, con la intención de mejorar la prevención, preparación y respuesta del Estado español frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello determina que se impulse la colaboración e implicación de los organismos gestores y propietarios de tales infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.

Asimismo, esta Ley regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

1.7. LEGISLACIÓN SECTORIAL ESPECÍFICA

1.7.1. Sector financiero

Reglamento Delegado (UE) 2018/389 (PSD2). Requiere autenticación reforzada del cliente y establece normas para la comunicación segura en servicios de pago.

Este Reglamento asume que los servicios de pago ofrecidos electrónicamente deben prestarse con la adecuada protección, mediante la adopción de tecnologías que permitan garantizar una autenticación segura del usuario y minimizar el riesgo de fraude. El procedimiento de autenticación debe incluir, en general, mecanismos de supervisión de las operaciones para detectar los intentos de utilizar las credenciales de seguridad personalizadas del usuario de un servicio de pago que hayan sido objeto de extravío, robo o apropiación indebida, y debe también asegurar que quien hace uso del servicio de pago es el usuario legítimo y está por lo tanto dando consentimiento a la transferencia de fondos y acceso a su información de cuenta mediante un uso normal de sus credenciales de seguridad personalizadas. Por otra parte, precisa los requisitos de autenticación reforzada de clientes que deben aplicarse cada vez que un ordenante acceda a su cuenta de pago en línea, inicie una operación de pago electrónico o lleve a cabo mediante un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos; exige la generación de un código de autenticación que no corra el riesgo de ser falsificado en su totalidad o mediante la revelación de cualquiera de los elementos sobre cuya base se haya generado.

1.7.2. Sector de Telecomunicaciones

Ley 9/2014, General de Telecomunicaciones. Garantizar la seguridad e integridad de las redes y servicios.

Esta Ley determina que los operadores de redes y de servicios de comunicaciones electrónicas disponibles al público gestionarán los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en las redes interconectadas. Asimismo, los operadores de redes públicas de comunicaciones electrónicas garantizarán la integridad de las mismas a fin de asegurar la continuidad en la prestación de los servicios que utilizan dichas redes.

Los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público notificarán al Ministerio de Industria, Energía y Turismo las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios. Cuando proceda, el Ministerio informará a las autoridades nacionales competentes de otros Estados miembros y a la Agencia Europea de Seguridad en las Redes y la Información (ENISA). Asimismo, podrá informar al público o exigir a las empresas que lo hagan, en caso de estimar que la divulgación de la violación reviste interés público. Una vez al año, el Ministerio presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este apartado.

Del mismo modo, el Ministerio comunicará a la Secretaría de Estado de Seguridad del Ministerio del Interior aquellos incidentes que afectando a los operadores estratégicos nacionales sean de interés para la mejora de la protección de infraestructuras críticas. También el Ministerio comunicará a la Comisión Nacional de los Mercados y la Competencia las violaciones de la seguridad o pérdidas de integridad a que se refiere este apartado que afecten o puedan afectar a las obligaciones específicas impuestas por dicha Comisión en los mercados de referencia. El Ministerio de Industria, Energía y Turismo establecerá los mecanismos para supervisar el cumplimiento de las obligaciones anteriores y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para los operadores, incluidas las relativas a las fechas límite de aplicación, para que adopten determinadas medidas relativas a la integridad y seguridad de redes y servicios de comunicaciones electrónicas.

1. LEGISLACIÓN NACIONAL Y SECTORIAL

Entre ellas, podrá imponer:

a) La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad.

b) La obligación de someterse a una auditoría de seguridad realizada por un organismo independiente o por una autoridad competente, y de poner el resultado a disposición del Ministerio de Industria, Energía y Turismo. El coste de la auditoría será sufragado por el operador.

Los operadores garantizarán la mayor disponibilidad posible de los servicios telefónicos disponibles al público a través de las redes públicas de comunicaciones en caso de fallo catastrófico de la red o en casos de fuerza mayor, y adoptarán todas las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia.

1.7.3. Sector Energético

Real Decreto 43/2021, de 26 de enero. Establece medidas específicas de seguridad para las redes y sistemas de información del sector energético.

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios, tanto si se trata de redes y sistemas propios, como de proveedores externos. En el caso de los operadores de servicios esenciales, deberán aprobar unas políticas de seguridad de las redes y sistemas de información, atendiendo a los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas. Las medidas de seguridad que se adopten por los operadores de servicios esenciales deberán tener en cuenta, en particular, la dependencia de las redes y sistemas de información y la continuidad de servicios o suministros contratados por el operador, así como las interacciones que presenten con redes y sistemas de información de terceros.

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán gestionar (comunicándolo, en todo caso, a la autoridad competente) y resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios. En el caso de redes y sistemas que no sean propios los operadores deberán tomar las medidas necesarias para garantizar que dichas acciones se lleven a cabo por los proveedores externos.

1.7.4. Sector Sanitario

Ley 41/2002, Básica Reguladora de la Autonomía del Paciente. Protección de datos sanitarios y confidencialidad de la información clínica.

Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal

2. LEGISLACIÓN EUROPEA

La Directiva NIS2 y el Reglamento DORA son marcos regulatorios recientes en la Unión Europea que tienen un gran impacto en la ciberseguridad de las empresas, especialmente en sectores críticos y financieros. Estos marcos están diseñados para mejorar la resiliencia de las infraestructuras digitales y proteger los servicios esenciales frente a ciberamenazas, con un enfoque en la gestión de riesgos y la ciberresiliencia.

1.1. DIRECTIVA NIS2 (SEGURIDAD DE REDES Y SISTEMAS DE INFORMACIÓN)

La Directiva NIS2 (Directiva (UE) 2022/2555) es una actualización de la Directiva NIS original (2016), con el objetivo de reforzar la seguridad de las redes y sistemas de información en la Unión Europea. Esta nueva directiva amplía el alcance de los requisitos y mejora las obligaciones de seguridad para las empresas en sectores clave como el sector digital, salud pública, gestión de residuos, fabricación, y administración pública.

Las organizaciones deberán implementar medidas técnicas y organizativas más estrictas para gestionar los riesgos de ciberseguridad. Esto incluye medidas de protección frente a ciberamenazas y la mitigación de riesgos.

También se espera que las empresas adopten estrategias de gestión de riesgos basadas en el análisis de amenazas, identificando y respondiendo a vulnerabilidades.

NIS2 impone plazos más ajustados para notificar incidentes de ciberseguridad significativos a las autoridades nacionales. Se requiere una notificación preliminar dentro de las 24 horas después de detectar un incidente y un informe más detallado en las siguientes 72 horas.

La directiva hace que la alta dirección de las empresas sea responsable de las políticas de ciberseguridad. Esto significa que los directivos podrían enfrentarse a sanciones en caso de que la empresa no cumpla con las normas de seguridad, aumentando la responsabilidad a nivel ejecutivo. Las sanciones por incumplimiento de la NIS2 pueden ser significativas, con multas que pueden llegar hasta el 2% del volumen de negocios global de la empresa o una multa máxima de 10 millones de euros, lo que sea mayor.

1.2. DORA (REGLAMENTO SOBRE RESILIENCIA OPERATIVA DIGITAL)

El Reglamento DORA (Digital Operational Resilience Act, Reglamento (UE) 2022/2554) es una normativa específica para el sector financiero que establece requisitos para garantizar la resiliencia operativa digital de las entidades financieras. El objetivo es asegurar que las entidades puedan resistir, responder y recuperarse de cualquier tipo de interrupción operativa, especialmente las relacionadas con ciberataques.

Las organizaciones deben gestionar los riesgos derivados de la externalización de servicios tecnológicos a proveedores críticos (como proveedores de la nube o de servicios de ciberseguridad).

DORA introduce un régimen de supervisión directa de terceros proveedores críticos por parte de las autoridades financieras, como los proveedores de servicios en la nube. Esto garantiza que los terceros cumplan con las mismas normas de resiliencia digital que las entidades financieras.

ESTRATEGIAS Y MEJORES PRÁCTICAS EN CIBERSEGURIDAD

1. IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es un proceso estructurado y estratégico, necesita el compromiso de la alta dirección, que sigue una serie de fases bien definidas, cuyo objetivo es garantizar la protección de los activos de información de una organización mediante la creación de un marco normativo y procedimental conforme a estándares como la ISO/IEC 27001.

Un SGSI no se limita a la mera adopción de herramientas tecnológicas o a la implantación de políticas reactivas, sino que involucra un enfoque integral de gestión que articula procesos, personas y tecnología para garantizar la confidencialidad, integridad y disponibilidad de la información en todos los niveles de la organización, así como la evaluación y auditoría periódica de su eficacia.

Uno de los aspectos más desafiantes en la implementación de un SGSI es la necesidad de alinear las políticas de seguridad con los objetivos estratégicos del negocio, lo que implica comprender profundamente los riesgos que enfrenta la empresa y el valor intrínseco de la información. Así cómo definir el alcance del SGSI, identificando qué parte de la organización está cubierta por el sistema.

De manera resumida los pasos que facilitarán una gestión adecuada de la seguridad podrían resumirse en:

a) Compromiso de la alta dirección y establecimiento del alcance. Integrar la seguridad en la cultura empresarial.

b) Evaluación Inicial y Análisis de Riesgos. Apalancarse en estándares conocidos como la ISO/IEC 27001

c) Definición de Políticas de Seguridad de la Información. Asignar responsables.

d) Implementación de Controles de Seguridad

e) Formación y Concienciación del Personal.

f) Monitorización y Revisión del SGSI. Mejora continua y visión a largo plazo.

2. CONCIENCIACIÓN, CAPACITACIÓN Y FORMACIÓN DEL PERSONAL. ESCASEZ DE TALENTO

La concienciación, capacitación y formación del personal son pilares fundamentales en cualquier estrategia de ciberseguridad, ya que, a menudo, los empleados representan el eslabón más débil en la cadena de defensa de una organización. La mayoría de los incidentes de seguridad se producen como consecuencia de errores humanos, bien por desconocimiento o por falta de atención a las políticas de seguridad.

Ante este panorama, el enfoque en la formación del personal no debe verse como una medida secundaria, sino como un componente central y estratégico dentro de un programa de gestión de seguridad. Crear una cultura de concienciación implica ir más allá de simples charlas o formaciones puntuales; se trata de transformar la forma en que los empleados perciben y actúan frente a las amenazas cotidianas.

Esto requiere la creación de un entorno donde la seguridad sea una responsabilidad compartida, lo que implica que cada miembro de la organización, independientemente de su rol, esté al tanto de los riesgos a los que está expuesto y de cómo puede contribuir a mitigarlos.

La capacitación en ciberseguridad debe ser vista como un proceso continuo y dinámico, en el que los programas de formación se actualicen regularmente para reflejar la evolución de las amenazas y las vulnerabilidades emergentes. Una simple formación inicial al comenzar en la empresa es insuficiente, especialmente considerando la rapidez con la que el panorama de la ciberseguridad cambia. La introducción de phishing más sofisticado, ransomware, amenazas internas y la utilización de técnicas de ingeniería social implica que los empleados deben estar equipados no solo con conocimientos básicos, sino también con habilidades para reconocer y actuar frente a estas amenazas en tiempo real.

Aquí es donde las simulaciones, como los ataques de phishing internos o las pruebas de respuesta a incidentes, juegan un papel esencial, ya que proporcionan una experiencia práctica que es mucho más eficaz que la simple teoría.

Aun así, la implantación de estos programas de formación enfrenta un desafío significativo: la escasez global de talento[35] en el mundo de la ciberseguridad.

En los últimos años, la creciente sofisticación de los ciberataques y la dependencia cada vez mayor de las tecnologías digitales han creado una demanda masiva de profesionales en este ámbito, que las instituciones educativas y los programas de formación no han sido capaces de cubrir a tiempo. La falta de personal cualificado no solo ralentiza la capacidad de las organizaciones para implementar defensas robustas, sino que también aumenta la carga de trabajo de los equipos de ciberseguridad existentes, lo que puede llevar a errores humanos, fatiga y, eventualmente, a incidentes de seguridad no detectados o mal gestionados.

Esta escasez no es solo un problema técnico, sino que también tiene profundas implicaciones estratégicas para la gestión del riesgo empresarial. En muchos casos, las organizaciones compiten agresivamente por el mismo grupo limitado de expertos en ciberseguridad, lo que no solo incrementa, o debería, los costos de contratación, sino que también obliga a las empresas a ser más creativas en su enfoque. Algunas han comenzado a implementar programas internos de desarrollo de talento, invirtiendo en la formación de empleados existentes para reconvertirlos en roles relacionados con la ciberseguridad. Esta estrategia, aunque efectiva a largo plazo, requiere tiempo y recursos considerables, algo que muchas organizaciones, especialmente las más pequeñas, pueden no tener.

Además, la brecha entre las necesidades de seguridad y el talento disponible también resalta una cuestión crítica sobre las habilidades requeridas en el sector de la ciberseguridad. La formación técnica en herramientas y metodologías es crucial, pero también lo es la capacidad de analizar riesgos, prever nuevas tendencias en ataques y tomar decisiones estratégicas que alineen la seguridad con los objetivos del negocio.

[35] La implementación de herramientas de detección de intrusiones (IDS/IPS), los sistemas de gestión de información y eventos de seguridad (SIEM) y las políticas de monetización continua le ayudarán en este objetivo.

2. CONCIENCIACIÓN, CAPACITACIÓN Y FORMACIÓN DEL PERSONAL. ESCASEZ DE TALENTO

La ciberseguridad no puede considerarse una función puramente técnica; es una disciplina transversal que requiere una comprensión profunda del entorno de negocio, lo que hace que el desarrollo de líderes en ciberseguridad sea una prioridad igual de importante que la formación técnica.

En definitiva, la solución a largo plazo para este desequilibrio entre oferta y demanda en el ámbito de la ciberseguridad no pasa solo por la formación técnica de profesionales, sino también por un replanteamiento estructural de cómo se concibe la ciberseguridad dentro de las organizaciones. La integración de la seguridad en la cultura corporativa, apoyada por una formación continua y una mayor diversificación del talento, permitirá no solo mitigar el impacto de la escasez de profesionales cualificados, sino también crear una postura de seguridad más robusta y resiliente frente a las amenazas futuras.

3. EVALUACIÓN Y GESTIÓN DE RIESGOS. PLANES DE RESPUESTA A INCIDENTES Y CONTINUIDAD DE NEGOCIO

La evaluación y gestión de riesgos es el proceso fundamental para identificar y priorizar las amenazas cibernéticas que pueden comprometer la seguridad de una organización, lo que permite implementar controles adecuados para mitigar su impacto. A partir de esta evaluación, se desarrollan los planes de respuesta a incidentes, que establecen protocolos claros y eficientes para detectar y reaccionar ante ciberataques, minimizando el daño y permitiendo una rápida contención.

Estos planes están intrínsecamente ligados a la continuidad de negocio, ya que, tras un incidente, la prioridad es asegurar que las operaciones críticas puedan seguir funcionando sin interrupciones, apoyándose en estrategias de recuperación y resiliencia operativa. Así, la gestión proactiva del riesgo, la respuesta ante incidentes y la continuidad de negocio forman un ciclo integrado que protege tanto los activos de la organización como su capacidad para seguir operando de manera eficiente frente a ciberamenazas.

Las recomendaciones que seguir para este objetivo son:

a) Realizar una evaluación de riesgos exhaustiva. Identificar y clasificar los activos críticos, así como las vulnerabilidades y amenazas que podrían afectarlo. Esto es un proceso continuo y requiere procesos de evaluación y auditoría de seguridad periódicos, con recursos internos y externos (proveedores).

b) Establecer un marco de gestión de riesgos: Implementar un enfoque sistemático, como el basado en ISO/IEC 27005 o el marco NIST, que permita gestionar los riesgos de manera continua, mediante la identificación, análisis, tratamiento y monitorización de las amenazas.

c) Implementar controles de seguridad adaptados a los riesgos. Monitorización y revisión continua. Esto puede incluir medidas como cifrado, autenticación multifactorial, segmentación de red, etc.

d) Desarrollar, evaluar y actualizar planes de respuesta. Para ello necesitará detectar el incidente[36], clasificarlo en función de su impacto, asignarlo a un responsable/equipo con capacidad de respuesta, contenerlo/erradicarlo, comunicar el estado del ciclo de vida de este y, finalmente, aprender del incidente y generar nuevas buenas prácticas defensivas.

e) Implementar un plan de continuidad de negocio donde una vez identificado y clasificado los procesos y sistemas críticos se defina un plan de recuperación ante desastres (DRP). Habitualmente centrados en restaurar sistemas y datos con mecanismos redundantes, copias de seguridad, etc.

[36] La implementación de herramientas de detección de intrusiones (IDS/IPS), los sistemas de gestión de información y eventos de seguridad (SIEM) y las políticas de monetización continua le ayudarán en este objetivo.

4. INVERSIÓN EN CIBERSEGURIDAD

En España la mayor parte de los ataques cibernéticos van destinados a las pequeñas y medianas empresas al constituir estas la casi totalidad de nuestro tejido empresarial. Diferentes fuentes, en función de la visibilidad de las empresas que analizan el impacto y criticidad de los ataques, indican que en un rango del 60% al 80% de los ataques en España van dirigidos a pymes, siendo los costes habituales en pequeñas empresas por ataque de 30.000 a 80.000 euros. Sin embargo, estos datos pueden resultar engañosos porque el impacto depende mucho del ámbito de acción y los datos manejados por la empresa y que, por desgracia, muchos de los incidentes se mantienen en secreto para evitar represalias legales o de reputación de marca. Para empresas de tamaño mayor es más habitual observar estos ciber incidentes en la prensa[37].

La recomendación de inversión en ciberseguridad para una pyme o empresa en España en 2025 puede variar considerablemente dependiendo de su tamaño, sector y nivel de madurez digital. Un nivel de seguridad avanzado puede oscilar de 20 a 50 euros/mes[38] por usuario en el que se podría incluir al menos soluciones EDR (defensa de dispositivo de usuario), cortafuegos a nivel de aplicación, sistema de backup, protección contra phishing, software de red privada virtual (VPN), sistemas de monitorización de amenazas gestionado y autenticación multifactor (MFA). Cifras de 10 a 20 euros/mes por usuario ya permiten niveles básicos de ciberseguridad que en la práctica reducen significativamente muchos de los ataques masivos actuales.

No es sencillo definir el retorno de inversión de aplicar ciberseguridad porque depende del escenario de empresa concreto. El histórico indica que por cada euro invertido en ciberseguridad una organización puede ahorrar en el amplio rango de 5 a 20 euros en gastos de mitigación y recuperación ante un incidente (interrupciones operativas), incluyendo posibles multas por fuga de información y la pérdida de reputación que puede afectar directamente al balance económico de la empresa.

De manera general, el presupuesto de ciberseguridad dedicado en PYMES suele situarse entre el 5% al 10% del presupuesto total del departamento de IT. Siendo razonable, si fuera posible, el rango del 10% al 20%. Aunque las cifras indicadas anteriormente, en el rango de 10 a 50 euros/mes/usuario permite trabajar la ciberseguridad poco a poco en función del presupuesto disponible y de manera gradual. Si el presupuesto es limitado, priorizar:

1. **Medidas básicas: Antivirus/EDR, phishing y backups.**
2. **Autenticación multifactor y gestión accesos.**
3. **Cifrado de la información**
4. **VPN**
5. **Concienciación en ciberseguridad para empleados.**

Para contextualizar lo anterior se pueden ver unos pequeños ejemplos considerando una inversión de 10 a 20 euros por usuario/mes. Estos precios estarían destinados a uso de productos tecnológicos de ciberseguridad, los costes del personal para su gestión interna o expertos se gestionarían adicionalmente.

[37] Tendam (Cortefiel) sufre un ataque informático y los ciberdelincuentes reclaman un pago de 800.000 euros https://elxpais.com/economia/2024-09-09/tendam-cortefiel-sufre-un-ataque-informatico-y-los-ciberdelincuentes-reclaman-un-pago-de-800000-euros.html?utm_source=chatgpt.com.

[38] Este precio es orientativo y varía en función de las soluciones tecnológicas concretas seleccionadas y el volumen de usuarios.

4. INVERSIÓN EN CIBERSEGURIDAD

Microempresa:

- Empleados: Menos de 10.
- Facturación anual o balance: ≤ 2 millones de euros.
- Inversión mínima en ciberseguridad – Rango 1200 a 2400 euros/anuales

Pequeña empresa:

- Empleados: Entre 10 y 49.
- Facturación anual o balance: ≤ 10 millones de euros.
- Inversión mínima en ciberseguridad – Rango 6000 a 12000 euros/anuales

Mediana empresa:

- Empleados: Entre 50 y 249.
- Facturación anual o balance: ≤ 50 millones de euros o ≤ 43 millones de euros respectivamente.
- Inversión mínima en ciberseguridad – Rango 30000 a 250000 euros/anuales

Considerando estas cifras de inversión en ciberseguridad puede observarse como minimizar el impacto de ciberataques por costes desde 30.000 a 1.500.000 euros.

ceim
EMPRESARIOS
DE MADRID

Comunidad
de Madrid

Calle de Diego de León, 50
28006 Madrid
Tel. 914 11 53 17
info@ceim.es

www.ceim.es