Instituto de Auditores Internos de España

RiesgosClave

esfera consejeros

Ciberseguridad, un riesgo sistémico a vigilar

Bien gestionado y supervisado, el riesgo se convierte en una ventaja competitiva

ÍNDICE

Sobre Esfera Consejeros

Esfera Consejeros es una iniciativa dirigida a los consejeros miembros de la **Comisión de Auditoría**.

Es un servicio de análisis, síntesis y conocimiento. Siempre desde la perspectiva de **rigor, calidad** e **independencia** del Auditor Interno.

Nuestro objetivo es aportar el **conocimiento** y la **visión transversal** propia de los auditores internos y contribuir a que los consejeros puedan supervisar la compleja realidad empresarial y su entramado de riesgos.

El servicio se nutre de diferentes publicaciones, **RiesgosClave, EnFoco y EnRuta**, que abordarán con distinta profundidad y enfoque temas relevantes en la vida empresarial.

Un valor diferencial es **la mirada del Auditor Interno** respecto el tema analizado: ¿Cuáles son las preguntas clave que hay que hacerse? ¿Qué inquieta al Auditor Interno y dónde y cómo actúa para proporcionar aseguramiento y confort? Cuestiones todas ellas relevantes para la Comisión de Auditoría en sus labores de supervisión y control.

Confiamos en que **Esfera Consejeros** le sea de utilidad.

Julio 2021

De un vistazo

Ciberseguridad, un riesgo sistémico a vigilar. Este informe aporta una mirada global para ayudar a los miembros de la Comisión de Auditoría a priorizar y supervisar adecuadamente uno de los mayores riesgos empresariales. Apuntamos preguntas y claves para comprender por qué se ha ampliado el perímetro de ciberseguridad, su conexión con otros riesgos, las mayores amenazas, los costes que genera un ciberataque y qué ayuda a mitigarlo. La pregunta ya no es si habrá o no ataques, sino cuándo. Hay que estar preparado.

El riesgo de ciberseguridad en datos

300 % han aumentado los ciberataques con el COVID-19, según el FBI

x5 se multiplicaron los ataques de malware y ransomware en 2020, según Deep Instinc

18 millones de emails tentativos de phishing bloqueó cada día Google al inicio del COVID-19

364 ciberincidentes al día (1 cada 30 minutos) gestionó el INCIBE en 2020 (133155 en total)

3,86 millones de dólares es el coste medio que genera una brecha de seguridad

280 días de media se tarda en detectar (207 días) y contener (73) un ciberataque

1 billón de dólares es el coste global del cibercrimen, el doble que el 2018, según McAfee

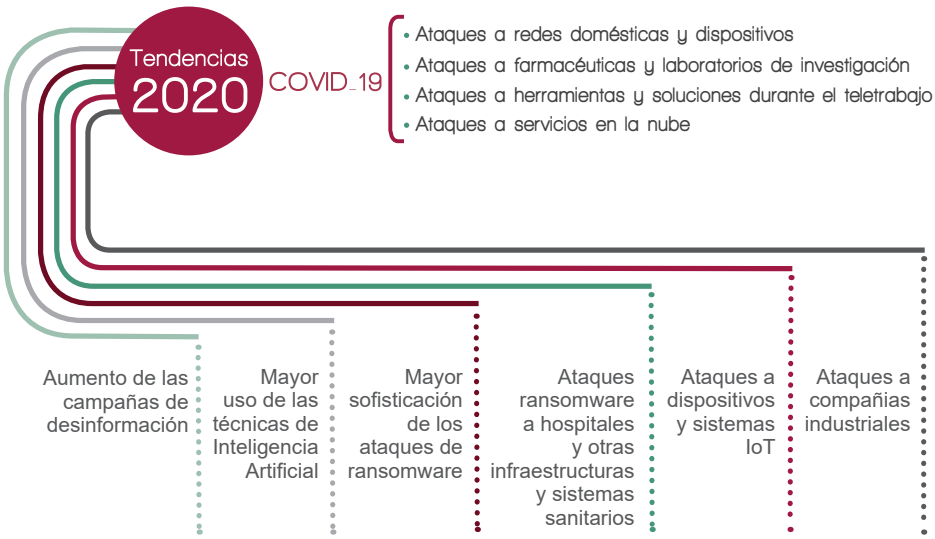
23 % de las brechas de seguridad se debe a errores humanos

Fuente: *IBM Security, Cost of a Data Breach Report 2021, salvo que se precise otra fuente en el texto.*

De un vistazo

- Con la pandemia, los ciberataques se han multiplicado por cuatro y los ataques ransomware, por cinco.
- El 23% de las grandes compañías españolas sufrió algún tipo de ciberincidente en 2020.
- Se estima que se tarda una media de 280 días en detectar un ciberataque.
- La formación y concienciación del personal es clave para mitigar riesgos de ciberseguridad.

2020: el año de la COVID y la ciberseguridad

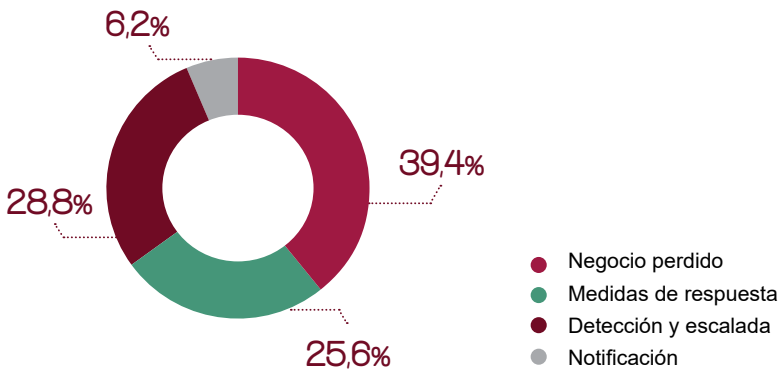


Fuente: *Centro Criptológico Nacional (CCN)*

De un vistazo

- El mayor coste (40%) de un ciberataque corresponde al negocio perdido.
- La regulación exige a las empresas analizar y vigilar los ciber-riesgos de la cadena de suministro.
- Los tests de resistencia a ciberincidentes es lo que más ayuda a mitigar el riesgo.
- La demanda de ciberseguros se ha disparado y ronda un volumen de 5.500 millones de dólares.

Ciberataques: el mayor coste corresponde al negocio perdido (% sobre el total)

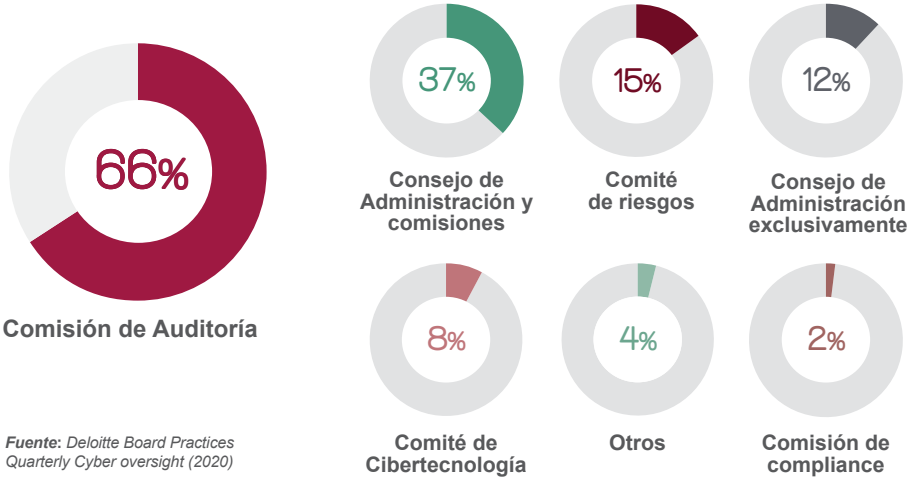


Fuente: *IBM Security, Cost of a Data Breach Report 2021*

De un vistazo

- La ciberseguridad debe integrarse en la estrategia y estar alineada con los objetivos de negocio.
- Se debate la necesidad de tener a nivel de consejo un experto en ciberseguridad o una comisión específica.
- Al consejo se informa sobre todo de vulnerabilidades y tendencias una vez al año. ¿Es suficiente?.
- Si DORA funciona en el sector financiero, la UE creará normas específicas de ciberseguridad por sectores.

Quién supervisa el riesgo de ciberseguridad



***Fuente**: Deloitte Board Practices Quarterly Cyber oversight (2020)*

Conectividad y ciberseguridad

Era un riesgo relevante. Con la creciente digitalización se ha convertido en prioritario. Es el primer riesgo que apuntaba los auditores internos en el informe Risk in Focus 2021[1]. Y figura en el top10 de los más relevantes del 2021 *Global Risks Report del World Economic Forum* (WEF)[2], que destaca la creciente desigualdad digital y el riesgo de una caída global de infraestructuras clave de Internet, de lo que ya hemos visto algunos intentos[3].

Con la pandemia y la digitalización acelerada, el riesgo de ciberseguridad ha desbordado sus propios límites, saliendo del perímetro al que tradicionalmente estaba confinado. Ha saltado desde un lugar físico (infraestructuras IT en la oficina) a un lugar ubicuo (la nube permite conectarse desde cualquier punto) cuyo uso, además, se ha disparado con el teletrabajo masivo. Ahora hay que controlar y proteger tres frentes: usuarios, accesos e información. Y todo ello en un entorno nuevo (distribuido) en el que el enfoque tradicional no es suficiente.

La pandemia aceleró la digitalización. Y la mayor conectividad de las personas (teletrabajo) y de las máquinas (IoT) ha cuadruplicado los ciberataques. Hay que prevenir, gestionar y mitigar el riesgo antes, durante y después para estar preparado.

[1] ***Instituto de Auditores Internos.*** *2021 Risk in Focus (2020)*

[2] ***World Economic Forum (WEF).*** *2021 Global Risks Report. (2021)*

[3] ***El País.*** *La caída global de miles de páginas alerta sobre la fragilidad de Internet (9 junio 2021). Webs de compañías como Amazon, Twitch, New York Times, HBO Max, Hulu, la web del Gobierno de Reino Unido, Spotify, Reddit estuvieron paradas o con problemas de acceso durante más de una hora*

Top10 desafíos según ENISA

1. Carácter sistémico. El riesgo de ciberseguridad se propaga rápida y ampliamente. Es difícil de evaluar y mitigar.

2. Tecnología preventiva. El uso de Inteligencia Artificial en ciberataques hará mucho más difícil la detección.

3. Errores involuntarios. Aumentan con el uso creciente de aparatos y sistemas conectados.

4. Cadena de suministro. Los hackers aprovechan cualquier debilidad de los ecosistemas empresariales, sean socios, proveedores o de cualquier otro tipo.

5. Automatización. La analítica de datos y la Inteligencia Artificial ayudarán a diseñar estrategias de ciberseguridad más robustas.

6. Falsos positivos. Reducirlos es clave para optimizar los esfuerzos y eliminar alarmas innecesarias.

7. Modelo Zero-Trust. En cada solicitud de acceso a un recurso corporativo, hay que verificar usuarios, dispositivos y aplicaciones[4]. Para muchos, el modelo Zero-Trust es la clave de la seguridad futura.

8. Migración al cloud. Un fallo en la configuración de la nube puede dejar expuestos los datos. Se están diseñando sistemas que identifican automáticamente estos errores.

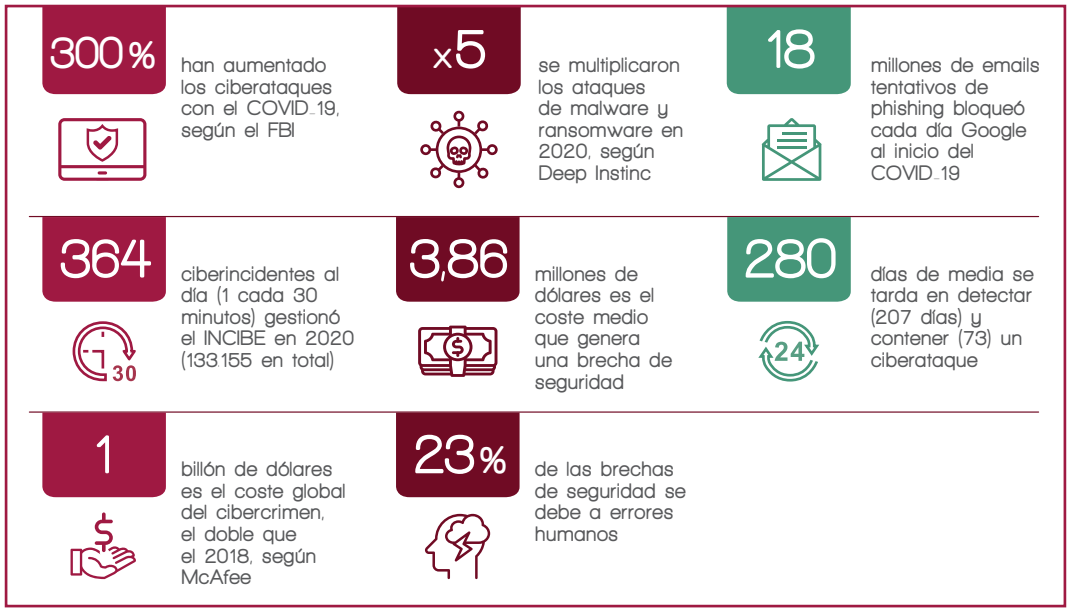
9. Amenazas híbridas. Combinan el mundo digital y el físico para aparecer más reales. La desinformación y las *fake news* son un grave peligro.

10. El cloud como objetivo. La creciente dependencia de las infraestructuras cloud aumentará los ataques no solo a las empresas que las usan, sino también a los proveedores del servicio.

Fuente: *Agencia de ciberseguridad de la Unión Europea (ENISA). Threat Landscape: The year in review (2020)*

[4] ***Mundo Hacker 2021.*** *Presentación sobre Zero Trust de Asier Ortega Peciña, Senior Sales Engineer Forcepoint Iberia.*

El riesgo de ciberseguridad en datos



Fuente: *IBM Security, Cost of a Data Breach Report 2021, salvo que se precise otra fuente en el texto.*

La UE marca la pauta: regulaciones en marcha

Ya en 2018 la UE se posicionó internacionalmente en seguridad y protección de datos con el Reglamento Europeo de Protección de Datos (RGPD). Ahora tiene en marcha una batería de ciber-regulaciones[5], que arranca con su estrategia de seguridad física y digital y sigue con la Directiva NIS 2 para sectores sensibles, la Directiva de Resiliencia, la regulación sobre identificación digital (eIDAS2) y la Ley de Resiliencia de Operativa Digital para el sector financiero, más conocida como DORA. El enfoque de la UE es actuar en los tres frentes clave: tecnología, procesos y personas

[5] *Datos recogidos por* ***Mckinsey****: Cybersecurity in Iberia: Aligning business and the board (Abril 2021)*

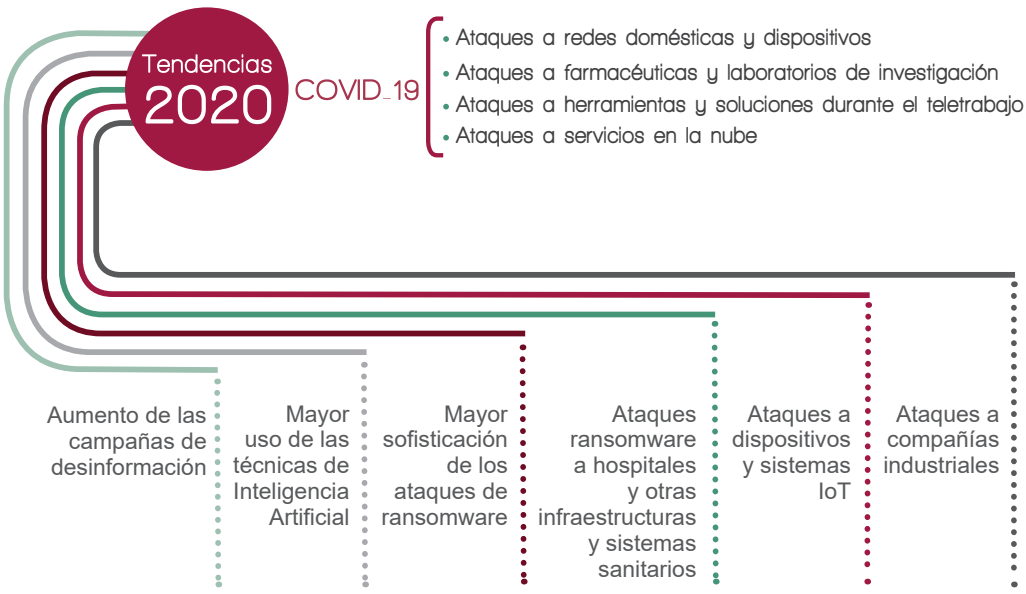
Ataques tipo ransomware

Los ciberataques se han cuadruplicado desde que arrancó la COVID-19, según datos del FBI. Los ataques tipo *ransomware* como WannaCry (2017) -se pide un rescate para desbloquear los datos *hackeados* - se han multiplicado por cinco. Son cada vez más sofisticados y atacan sectores sensibles, las llamadas infraestructuras críticas. Hospitales y farmacéuticas están siendo muy atacados.

En España, durante el 2020 el INCIBE gestionó un total de 133.155 ciberincidentes, lo que supone 364 al día, es decir, uno cada 25/30 minutos. Los datos del Centro Criptológico Nacional (CCN) revelan que el 23% de las grandes compañías españolas sufrió algún tipo de ciberincidente en 2020, porcentaje que baja al 12% para las pymes, menos digitalizadas, y sube al 28% para los ciudadanos[6]. Nunca antes se vio algo igual.

La pregunta ya no es si una empresa sufrirá o no un ciberataque, sino cuándo. El cibercrimen se ha profesionalizado y han surgido actores nuevos amparados por los estados.

2020: el año de la COVID y la ciberseguridad



Fuente: *Centro Criptológico Nacional (CCN)*

[6] *Datos recogidos por* ***Mckinsey****: Cybersecurity in Iberia: Aligning business and the board (Abril 2021)*

De TI a la estrategia

Desde el punto de vista empresarial, la ciberseguridad vive un cambio de paradigma total. Ha dejado de ser un problema de TI para convertirse en cuestión estratégica, que implica a toda la organización y que, de no gestionarse bien, puede ocasionar un grave impacto económico, regulatorio, reputacional y hasta llevarse a la compañía por delante[7]. La ciberseguridad no se puede afrontar desde la respuesta, sino de forma proactiva, anticipándose.

Hay que proteger usuarios, accesos e información en un entorno donde el enfoque clásico no es suficiente.

Con la pandemia, el riesgo de ciberseguridad ha desbordado sus propios límites.

El mapa de la ciberseguridad

Principales riesgos

- Fraude dinerario
- Robo de información
- Indisponibilidad de servicios
- Sabotaje de infraestructuras
- Pérdida de reputación

Principales amenazas

- Contra la información
- Contra la infraestructura TIC

Perfil de los atacantes

- Hacking
- Cibercrimen
- Hacktivismo
- Ciberespionaje y ciberterrorismo
- Insider

Principales técnicas de ataque

- Ingeniería social
- Fingerprinting
- Enumeración y escaneo
- Ataques de días cero (0_Day)
- Spam y Phishing
- Hijacking
- Denegación de Servicios (DoS)
- SQL Injection
- Cross_site scripting (XSS)
- Virus, malware, gusanos y troyanos
- Botnet (redes zombis)
- Rootkits
- Ransomware
- APT (Amenaza Persistente Avanzada)

Fuente: *La Fábrica de Pensamiento. Ciberseguridad: Una guía de supervisión.*

[7] ***El País.*** *Ciberataques que matan a las empresas. (2020)*

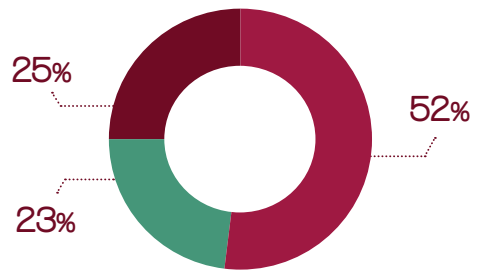
Responsabilidad del consejo

Reguladores y supervisores, conscientes de este creciente riesgo, piden a las empresas que estén preparadas. ¿Cómo? Con diferentes medidas. Uno, atribuyendo la responsabilidad (y exigiendo conocimientos técnicos) a lo más alto: el Consejo de Administración y sus comisiones de apoyo. Dos, con severas regulaciones y sanciones (el RGDP es un buen ejemplo). Tres, exigiendo planes de continuidad de negocio y, en el caso del sector financiero, incluso haciendo test de estrés a bancos, plataformas de negociación y sistemas de liquidación y compensación de pagos[8]. Cuatro, ampliando el perímetro de control a la cadena de suministro y cualquier otra relación con proveedores o terceros, un histórico punto débil por el que se han colado ciberataques. Y cinco, reclamando un modelo de gobernanza de la ciberseguridad y más y mejor supervisión.

El sector financiero está siendo sometido a test de estrés para calibrar su ciber_resiliencia

La Comisión de Auditoría, al igual que Auditoría Interna, juegan un papel muy relevante para supervisar este riesgo y asegurarse de que la organización promueve una adecuada cultura de ciberseguridad. Y esa adecuada cultura, hoy más que nunca por el teletrabajo, pasa por la formación y concienciación de la plantilla. Es uno de los grandes retos.

Fallos del sistema y errores humanos generan la mitad de las brechas (En %)



La Comisión de Auditoría debe asegurarse de que se promueve una adecuada cultura de ciberseguridad

Fuente: *IBM Security, Cost of a Data Breach Report 2021*

[8]***Autoridad Bancaria Europea (EBA).*** *EU-wide stress testing (Enero 2021).* ***Banco Central Europeo (BCE).*** *What is cyber resilience?*

El cibercrimen cuesta 1 billón de dólares

Los ciberataques son cada día más numerosos y sofisticados. El cibercrimen no es una actividad individual, como hace años, sino de grupos organizados con profundos conocimientos informáticos, diferentes motivaciones, un modelo empresarial claro y hasta sus propios departamentos de I+D+i[9]. En la Internet profunda o *Dark Web* se pueden comprar todo tipo de recursos, herramientas y malware para llevar a cabo ataques. Hay hasta foros donde los hackers se cursan preguntas y desafíos. Es lo que muchos llaman Ciberdelincuencia como Servicio *(Crime as a Service)*. McAfee cifra en un billón de dólares el coste global del cibercrimen, el doble que en 2018[10].

Se tarda una media de 280 días en detectar un ciberataque.

El cibercrimen se ha profesionalizado y cuenta con departamentos de I+D+i

DORA abre la puerta a ciber-regulaciones por sectores

La Ley de Resiliencia Operativa Digital, más conocida como DORA, es una regulación europea sobre ciberseguridad específica para el sector financiero. Apunten ese nombre, porque hay un antes y un después de DORA, un reglamento europeo que se aplicará directamente a todos los países miembros sin necesidad de trasposición interna. Dora, aplicable al sector financiero, es un patrón que, si funciona, será replicado por la UE con normas específicas para otros sectores como energía, agua o telecomunicaciones.

[9] ***KPMG Tendencias.*** *El modelo empresarial del Cibercrimen; Consideraciones clave para la gestión de ciberincidentes (2020); Vídeo: Cinco respuestas: Cómo evitar los ciberataques y el bloqueo de sistemas (marzo 2021)*

[10] ***McAfee:*** *The Hidden Costs of Cybercrime (2020)*

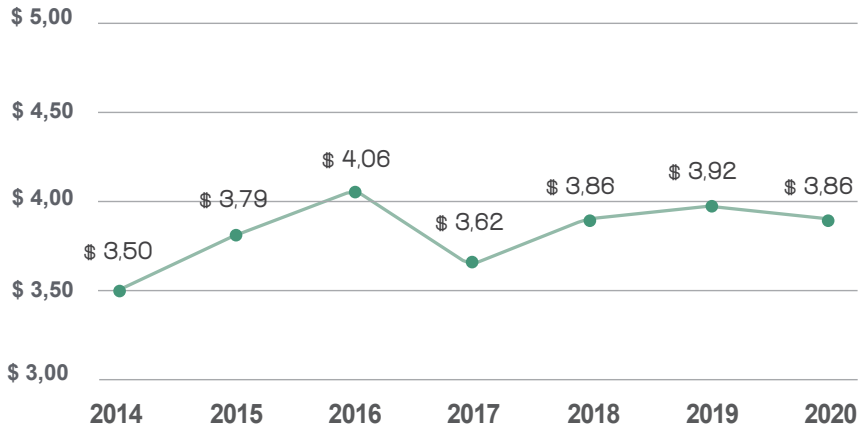
Valorar todos los impactos

Un ciberataque puede tener un coste enorme para una compañía. Puede incluso hacer peligrar su supervivencia.

Además del daño reputacional, el mayor coste corresponde a la pérdida de negocio ocasionado por la fuga de clientes o la propia la paralización de la compañía, como ocurre con los ataques de denegación de servicio DoS y en los de *ransomware*: se secuestra información clave para operar y se pide un rescate para liberarla. Este tipo de ciberataques se han disparado con la pandemia: los DoS se han duplicado y los de *ransomware,* quintuplicado, según datos de IBM.

El riesgo de ciberseguridad desata otros riesgos asociados legales, financieros, reputacionales... El mayor impacto de un ciberataque viene por la pérdida de negocio. Hay medidas que ayudan a mitigarlo como son los planes de continuidad, las pruebas de resistencia y los ciberseguros.

Coste medio por brecha de datos (Mill $)



Fuente: *IBM Security, Cost of a Data Breach Report 2021*

Proveedores y socios, el punto débil

Los *hackers* saben que proveedores, *partners* o socios de las compañías son un punto débil y lo intentan explotar. Máxime ahora que cualquier cosa conectada –impresora, móvil, sistema domótico, aire acondicionado…– puede ser una puerta de entrada para los *hackers*. En 2013, los almacenes Target sufrieron un robo de datos (40 millones de tarjetas de clientes) y el modus operandi de los *hackers* fue aprovechar la conexión del proveedor de refrigeración para entrar en los sistemas[11]. Según recoge COSO ERM, el 59% de las compañías ha sufrido brechas de seguridad a través de un tercero[12]. Las regulaciones en marcha –Directiva NIS 2.0, DORA etc.– incluyen la obligación de analizar la ciberseguridad de los proveedores. En fusiones y adquisiciones, también es habitual incluir un análisis ciber en la *due diligence*.

[11] ***Reuters.*** *Target cyber breach hits 40 million payment cards at holiday peak (2013)*

[12] ***COSO.*** *Managing Cyber Risk in a Digital Age (2019)*

Coste legal

El coste legal también puede ser alto: recordemos que el reglamento europeo RGPD contempla multas de hasta el 4% de la facturación del grupo por incumplir la obligación de protección de los datos personales. Regulaciones europeas en marcha elevarán este coste legal.

IBM calcula que el coste total medio para una empresa que sufra una brecha de datos ronda los 3,86 millones de dólares. Pero detectar un ciberataque no es algo fácil ni rápido: se tarda una media de 280 días en detectarlo, es decir, más de nueve meses. Cada vez más compañías invierten en sistemas de ciberinteligencia y ciberdefensa que permiten explorar la *Deep Web* (web profunda) para detectar allí señales de alerta temprana que ayuden a actuar antes.

Estar preparados reducirá el coste después. El gráfico de la siguiente página muestra al detalle los factores que ayudan a mitigar el coste de un ciberataque, como son los test o pruebas de respuesta a incidentes (el *hacking* ético es habitual para detectar posibles vulnerabilidades), los planes de continuidad de negocio o la formación de la plantilla. Pese a la relevancia de estos aspectos, pocas compañías se preparan con antelación. Según un artículo de *Harvard Business Review,* el 47% de las organizaciones no ha evaluado la preparación de sus equipos de respuesta ante ciberincidentes, lo que significa que la primera vez que lo hagan será en medio de un ciberataque, el peor escenario posible[13].

> Los tests y pruebas de resistencia a ciberincidentes es lo que más ayuda a mitigar el riesgo

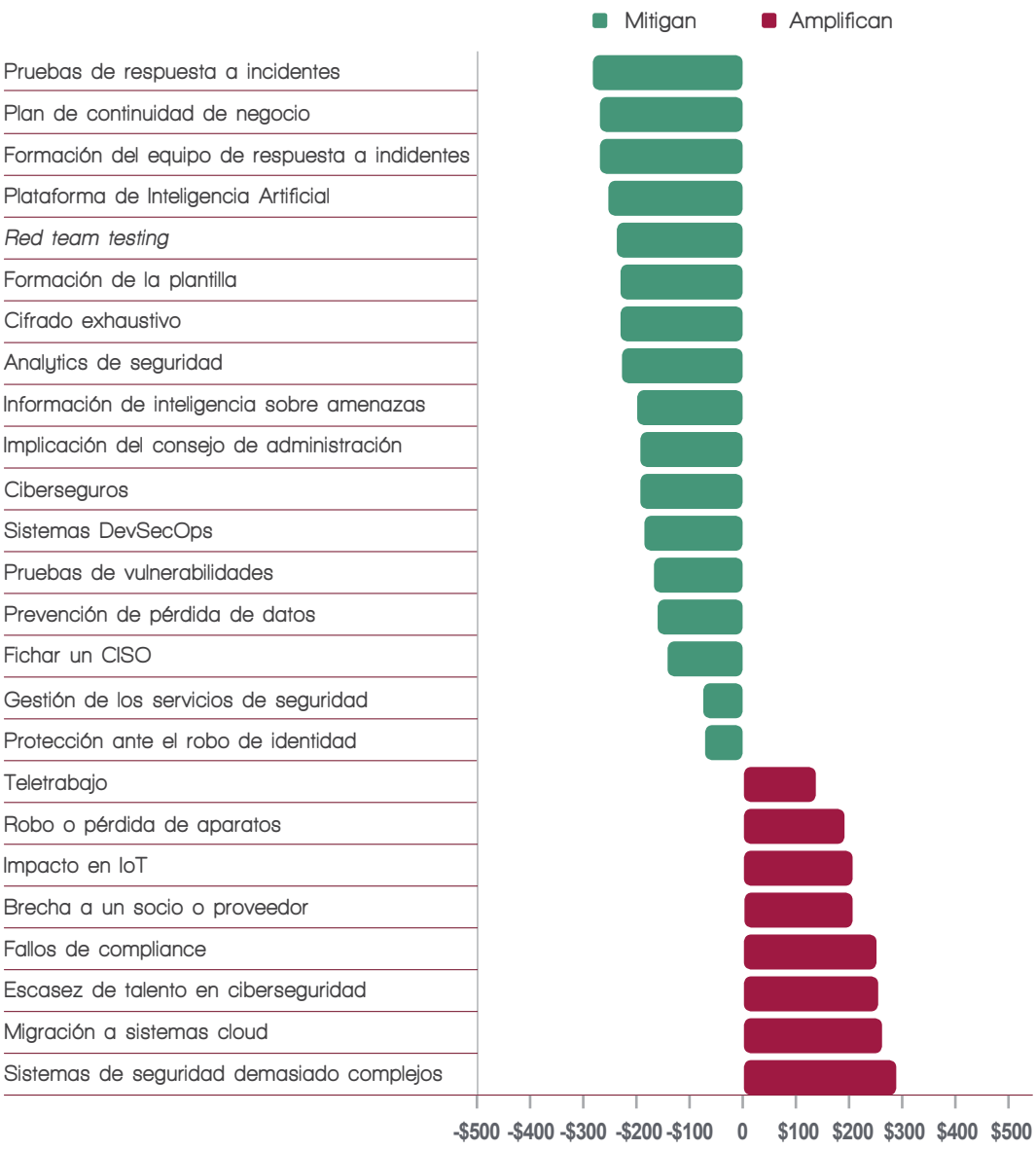
Entre los factores que amplifican el coste de un ciberataque figuran, entre otros, el teletrabajo, por la vulnerabilidad que supone la conexión en remoto, el robo o pérdida de aparatos electrónicos corporativos (portátil, móvil etc.) o los errores en la migración a sistemas cloud.

> El mayor coste (40%) de un ciberataque corresponde al negocio perdido… si la compañía sobrevive

> La demanda de ciberseguros se ha disparado y ronda un volumen de 5.500 millones de dólares

[13] ***Harvard Business Review.*** *Cyberattacks Are Inevitable. Is Your Company Prepared? (Marzo 2021)*

Factores que mitigan el coste y que lo amplifican (Datos en miles $)



Fuente: *IBM Security, Cost of a Data Breach Report 2021*

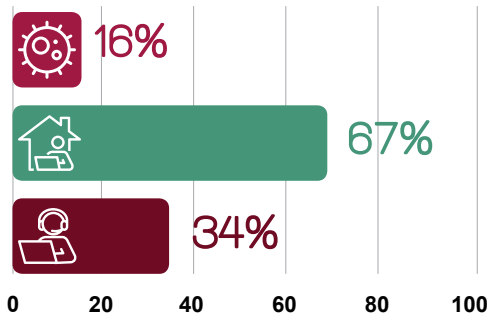
Trabajar en remoto

El teletrabajo masivo ha abierto importantes desafíos para la ciberseguridad que deben atajarse con herramientas para controlar los accesos y con formación para concienciar al personal para que, entre otras, siga las siguientes prácticas: utilizar contraseñas potentes y no siempre la misma; tener el software siempre actualizado; no abrir (ni hacer click) emails y links extraños o sospechosos y utilizar las VPNs de acceso seguro.

El mayor problema viene de utilizar aparatos y redes personales para uso corporativo: ni el wifi del hogar ni el móvil personal tienen los mismos niveles de ciberseguridad que los corporativos. Por ejemplo, un móvil corporativo seguro no permite al usuario bajarse cualquier app: están bloqueadas.

El 47% de las empresas europeas consultadas por Cisco[14] no había preparado antes de la pandemia sus sistemas para este teletrabajo masivo, que requiere de videoconferencias constantes y herramientas colaborativas. ¿Resultado? El 93% tuvo que actualizar sus políticas de ciberseguridad, adoptando sobre todo tres medidas: aumento de la capacidad del VPN, implementación de la autenticación multifactor (MFA), mayor control de la web y políticas de uso aceptable más restrictivas.

Empresas europeas con más del 50% de la plantilla teletrabajando



El 93% de las empresas tuvo que actualizar su ciberseguridad con la llegada de la pandemia y el teletrabajo masivo

Fuente: *Cisco, Future of Secure Remote Work Report (2021)*

[14] ***Cisco.*** *Future of Secure Remote Work Report (2021) Security Outcomes Study - Proven Factors for Your Security Program (2021) Simplify to Secure Cybersecurity Report (2021)*

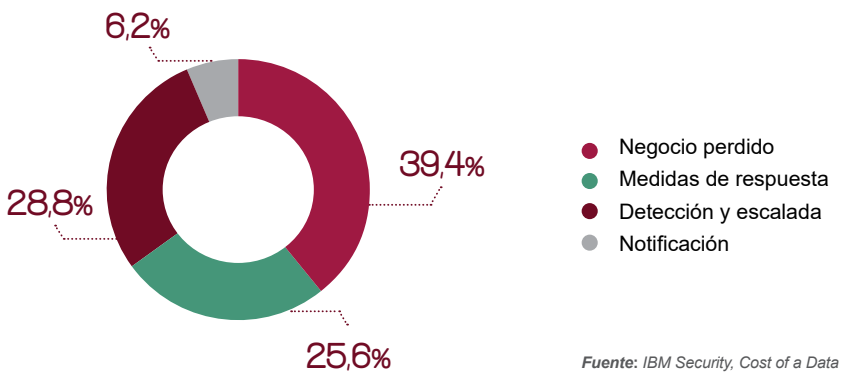
Ingeniería social

Las personas son el eslabón más débil de la cadena de ciberseguridad. Por eso son objetivo de los *mailings* maliciosos, que apelan directamente a las debilidades del ser humano. Es la llamada ingeniería social, con múltiples formas de expresión como el *phishing* o suplantación de identidad. Al principio de la pandemia, Google bloqueaba cada día más de 18 millones de emails sospechosos de malware o *phishing*. El fraude del CEO, conocido porque el objetivo del ciberataque es hacerse pasar (vía email) por un alto directivo para que los empleados acaten rápidamente las órdenes (falsas) del jefe. ¿El objetivo? Solicitar pagos o transferencias para hacerse con dinero de la compañía. Hay que estar muy alerta para detectar y reaccionar ante cualquier tipo de email sospechoso y establecer canales para que los empleados que los detecten puedan comunicarlo rápidamente.

Las fusiones y adquisiciones incluyen el análisis de ciberseguridad en la *'due diligence'*

Cada vez más compañías invierten en ciberinteligencia para detectar alertas en la *Deep Web*

Ciberataques: el mayor coste corresponde al negocio perdido (% sobre el total)

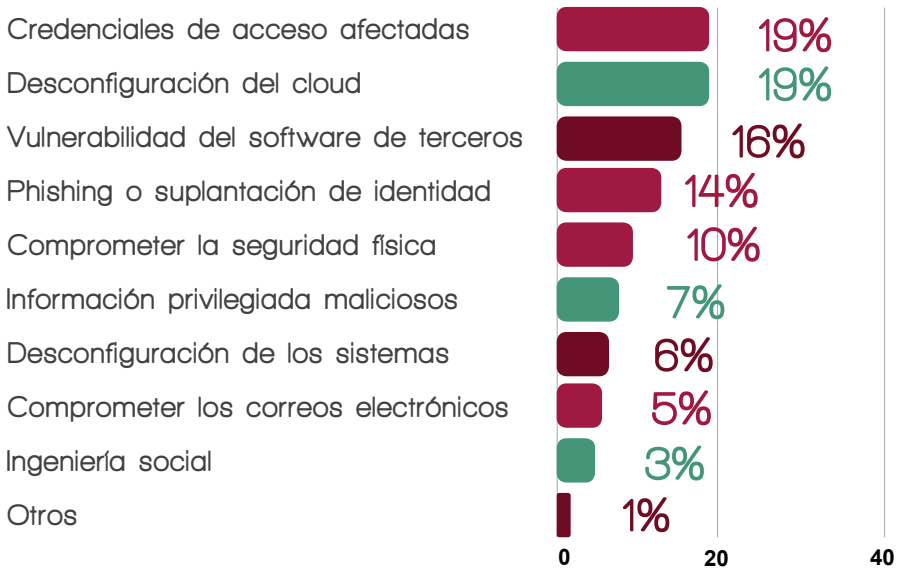


Fuente: *IBM Security, Cost of a Data Breach Report 2021*

Ciberseguros: ojo el grado de cobertura

Los ciberseguros son una práctica cada día más habitual en las empresas, especialmente entre las grandes. No tanto para las pymes y el sector público debido a la complejidad de estas pólizas. Se calcula que el mercado mundial de ciberseguros mueve primas por volumen de 5.500 millones de dólares, según McAfee[15]. Son contratos complejos: hay que mirar bien la letra pequeña y los términos y, seguramente, pelear en los tribunales: de las reclamaciones planteadas en 2017 en EEUU, sólo se abonó el 28%, con una media de 188.525 dólares, cifra que apenas supone en torno a un tercio del coste medio estimado por ciberataque.

Tipos de ataques maliciosos según tipo de amenaza (En % sobre el total)



Fuente: *IBM Security, Cost of a Data Breach Report 2021*

[15] ***McAfee:*** *The Hidden Costs of Cybercrime (2020)*

Marco de gobierno

Países y empresas están adaptando sus políticas, estrategias y marcos de ciberseguridad al entorno digital. Los consejeros deben comprender el riesgo y asegurar los controles adecuados. Se debate la necesidad de contar en el consejo con un experto en ciberseguridad o una comisión específica.

Los países están actualizando sus políticas y estrategias de seguridad nacional desde un enfoque físico a un entorno digital, a estrategias de ciberseguridad. En España, la última revisión data de 2019[16]. Para el estatus especial que tienen las llamadas infraestructuras críticas, existe una regulación y un organismo específico: el Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC).

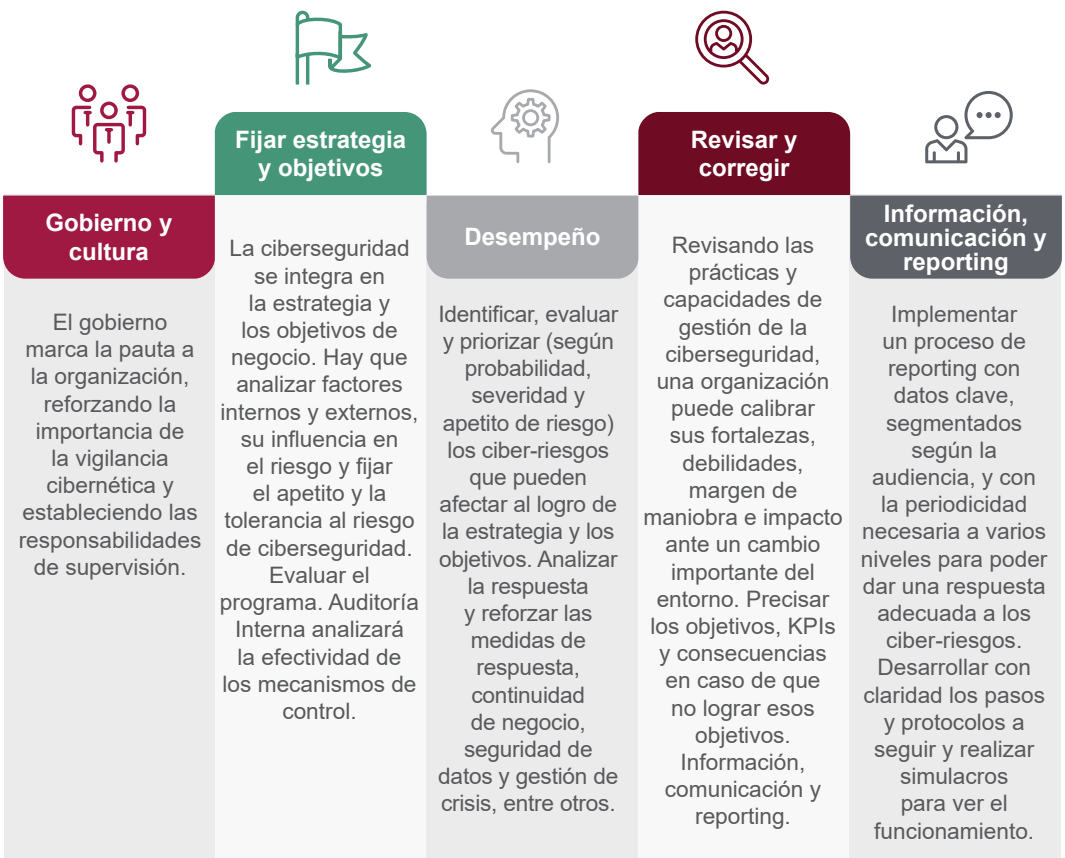
También las empresas deben actualizar sus marcos de control al nuevo contexto. Existe un buen número de marcos de control sobre ciberseguridad. Destacamos abajo[16] algunas instituciones nacionales e internacionales de referencia que periódicamente ofrecen alertas, marcos, formaciones, recomendaciones y buenas prácticas.

[16] ***IBOE.*** *Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.*

[17] ***INCIBE; ENISA;*** *Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC); National Institute of Standards and Technology (NIST): Cybersecurity Framework (2018) y Cybersecurity Guidelines (Marzo 2021); Center for Internet Security (CIS); National Cyber Security Centre (NCSC) e Information Systems Audit and Control Asso- ciation (ISACA). Securities and Exchange Commission (SEC): Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2018) Cybersecurity and Resiliency Observations (2020)*

COSO también desarrolló recientemente (diciembre 2019) una nueva guía: *Managing Cyber Risk in a Digital Age*. El documento subraya el papel del consejo de administración y sus comisiones de apoyo, como la Comisión de Auditoría, en la supervisión de un riesgo tan relevante. Hay que contar con un marco claro, alineado con los objetivos, la estrategia, el apetito de riesgo y la tolerancia al mismo[18].

El marco COSO ERM



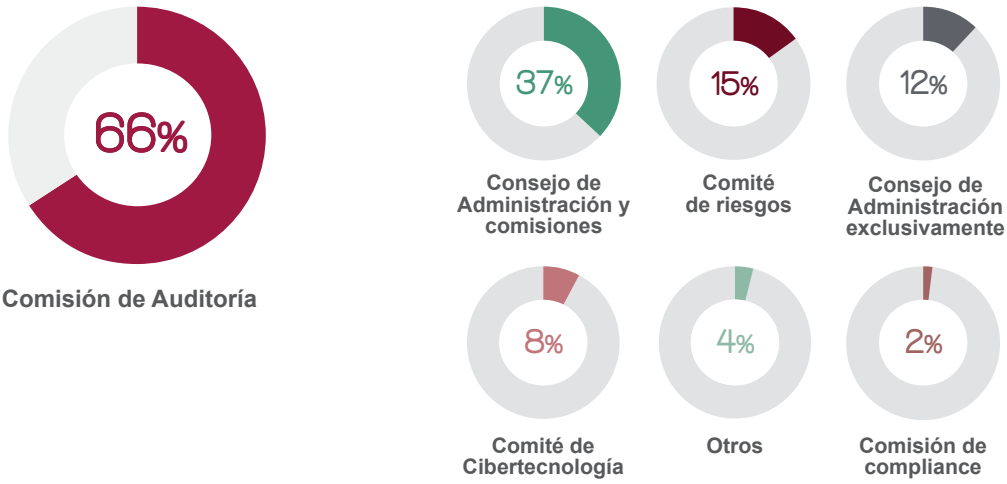
Fuente: *COSO ERM. Managing Cyber risk in a digital age.*

[18] ***COSO.*** *Managing Cyber Risk in a Digital Age (diciembre 2019)*

SEC: informar sobre cómo se supervisa el riesgo

Una de las referencias internacionales es la Guía de la SEC de 2018[19] sobre divulgación de información en materia de ciberseguridad, que concreta múltiples aspectos, entre ellos, cómo y cuándo se debe informar sobre la supervisión por parte del consejo de administración y sus comisiones. ¿Cuándo? Cuando los riesgos de ciberseguridad son importantes (materiales) para el negocio de la compañía. ¿Cómo? Informando sobre con quién (y cómo) trata las cuestiones de ciberseguridad el consejo y cómo cumple con su obligación de supervisar este riesgo y sobre los sistemas, controles y procesos implantados. La SEC, como otros reguladores, exige al consejo estar vigilante y comprender las cuestiones sobre tecnología y seguridad y la forma en la que los riesgos de ciberseguridad son gestionados en la organización. Se debate que haya un experto o comisión específica de ciberseguridad a nivel de consejo.

Quién supervisa el riesgo de ciberseguridad



Fuente: *Deloitte Board Practices Quarterly Cyber oversight (2020)*

[19] ***Securities and Exchange Commission (SEC):*** *Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2018) Cybersecurity and Resiliency Observations (2020)*

Los consejeros no necesitan ser ingenieros informáticos, pero deben conocer y comprender el riesgo de ciberseguridad. Algunas compañías están designando a un experto responsable de ciberseguridad dentro del consejo. Ése es el debate ahora mismo. Otras están creando una comisión específica de ciberseguridad: aunque este segmento apenas representa el 10% a nivel internacional, Gartner cree que será del 40% en el horizonte de 2025[20].

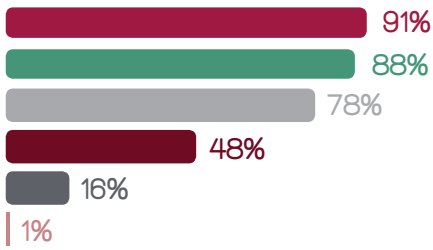
Con el valor creciente de los datos, todos los sectores son susceptibles de ser atacados. Hay que pensar en términos de ciberseguridad al arrancar cualquier proyecto, producto o servicio, desde el momento cero.

Al consejo y las comisiones se informa de vulnerabilidades y tendencias una vez al año: ¿Es suficiente?

Gartner: en 2025, el 40% de las grandes empresas tendrá una Comisión de Ciberseguridad (10% actualmente)

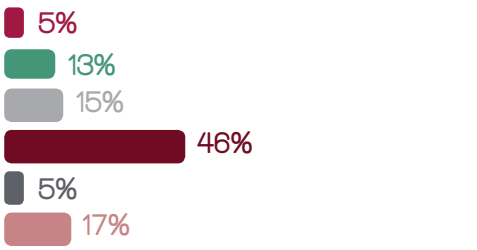
La información sobre ciberseguridad que llega al consejo y sus comisiones

De qué se le informa



- Vulnerabilidades
- Tendencias
- Métricas
- Medidas de detección y prevención
- Otros
- Nada

Cuándo se le informa



- En cada reunión
- Trimestralmente
- Bianualmente
- Anualmente
- Nunca
- Otros

Fuente: *Deloitte Board Practices Quarterly Cyber oversight (2020)*

[20] ***Gartner:*** *Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025 (Enero 2021)*

Ataques a infraestructuras críticas y servicios esenciales

Los ciberataques a infraestructuras críticas o servicios esenciales son cada día más frecuentes[21]. Desde el inicio de la pandemia, ha sido atacadas instalaciones de petróleo y gas (Estados Unidos, Arabia Saudí y Taiwán), redes eléctricas (India), saneamientos (Israel), agencias gubernamentales (Australia, España (SEPE), universidades (Oxford), hospitales (Alemania, Francia, Reino Unido, Irlanda, España), bancos centrales y bolsas de valores (Nueva Zelanda)... La lista no para de crecer[22], lo que ha llevado al presidente de EEUU, Joe Biden[23], a ampliar la lista de sectores esenciales. Europa ha hecho lo mismo con la Directiva NIS 2.0, que subraya también la obligación de vigilar la ciberseguridad de la cadena de suministro. Todo integra la nueva Estrategia de Ciberseguridad de la UE[24].

Seis principios para una organización ciber-resiliente

1 La ciberseguridad es un facilitador de la estrategia de negocio

La ciberseguridad es un facilitador de la estrategia de negocio 2

3 Alinear la gestión de la ciberseguridad con las necesidades del negocio

Asegurarse de que el diseño organizacional mira por la ciberseguridad 4

5 Incorporar conocimiento y experiencia sobre ciberseguridad al consejo

Impulsar la resiliencia sistémica y la colaboración 6

Fuente: *World Economic Forum (WEF), National Association of Corporate Directors (NACD) y Internet Security Alliance (ISA): Principles for Board Governance of Cyber Risk (marzo 2021)*

[21] ***Deloitte.*** *The impact of Cyber on "critical infrastructure" in the Next Normal (2020)*

[22] ***Reuters.*** *Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed (9 mayo 2021)*

[23] ***Reuters.*** *Biden administration eyes cybersecurity funding after hacks (18 mayo 2021)*

[24] ***Comisión Europea****. Nueva Estrategia de Ciberseguridad de la UE y nuevas normas para aumentar la resiliencia de las entidades críticas físicas y digitales.*

Seis recomendaciones clave para consejeros

Para terminar, recogemos un resumen de los seis principios y recomendaciones clave para convertirse en una organización ciber-resilientes, con un gobierno y una supervisión de la ciberseguridad adecuada por parte del consejo, que recogía recientemente el World Economic Forum (WEF) en un informe elaborado en colaboración con National Association of Corporate Directors (NACD) y Internet Security Alliance (ISA)[25].

1. **No quitarse nunca las lentes de ciberseguridad.** La ciberseguridad debe estar en la estrategia y en la agenda del consejo. Requiere de liderazgo comprometido y cultura de ciberseguridad. Todo hay que mirarlo sin quitarse las lentes de ciberseguridad: innovación, transformación digital, estrategia comercial, fusiones y adquisiciones, desarrollo de productos, expansión comercial, etc.

2. **Apetito, indicadores, marco de gobierno.** Hay que medir el riesgo de ciberseguridad frente a los objetivos estratégicos, regulatorios, legales y comerciales. Determinar y revisar el apetito de riesgo ciber y el nivel de tolerancia, establecer ciberescenarios, indicadores (KPIs) y un marco de gobierno robusto, con modelos sólidos de cuantificación.

3. **Perfil de seguridad alineado a las necesidades del negocio.** Un buen gobierno requiere de alineación entre la gestión de la ciberseguridad y los objetivos de negocio. Hay que analizar el riesgo ciber de cualquier decisión: nuevo producto, una app… Una buena gestión el riesgo ciber abre oportunidades y mitiga riesgos.

4. **Security by Design o, desde el momento cero.** La seguridad forma parte del proceso de desarrollo de una compañía: no se deja para después el análisis de seguridad, sino que se contempla desde el principio, cuando empieza a diseñar el producto. Hay que revisar la estructura organizativa para asegurarse de que la función de ciberseguridad está presente en toda la empresa, grupos, áreas y líderes.

5. **Conocimiento y experiencia.** Los consejeros deben asegurarse directa o indirectamente -con la ayuda de la Alta Dirección, Auditoría Interna y expertos externos- el conocimiento actualizado y necesario para supervisar adecuadamente este complejo y técnico riesgo. Además de hacer auditorías periódicas, conviene repasar tendencias, vulnerabilidades y ciberincidentes reseñables. Como comentamos antes, está el debate de que, a nivel consejo, haya un experto responsable de ciberseguridad o una comisión específica.

6. **Colaboración para ganar ciber-resiliencia.** El riesgo de ciberseguridad corre como la pólvora en un mundo interconectado. Gestionarlo adecuadamente exige altas dosis de colaboración interna y externa. Interna, entre los diferentes departamentos empresariales, incluyendo proveedores. Y externa, con el propio sector y otros sectores, contemplando también la colaboración público-privada.

[25] *Recomendaciones recogidas en el reciente informe elaborado por el World Economic Forum (WEF), la National Association of Corporate Directors (NACD) y Internet Security Alliance (ISA).*

Ciberseguridad como ventaja competitiva

Bien gestionado, el riesgo de ciberseguridad puede convertirse en una ventaja competitiva de la compañía. Los clientes están cada vez más vigilantes de la seguridad de sus datos. Y no dudan en huir si algo les infunde desconfianza. Y, al contrario, la confianza digital genera fidelidad y permite más y nuevos ingresos.

Una adecuada gestión y supervisión de la ciberseguridad protege a la empresa del riesgo cibernético al tiempo que impulsa la confianza en la marca. Hay buscar un difícil equilibrio entre seguridad y experiencia de cliente, gestionando su privacidad y sus accesos, sin poner demasiadas barreras o fricciones[26]. Formar y cuidar al cliente interno (empleados) revierte rápidamente en mejor percepción y satisfacción del cliente externo.

La ciberseguridad, antes acotada al departamento de TI, se ha convertido en un elemento transversal y clave dentro de cualquier organización. Correctamente gestionada, es un 'driver' del crecimiento empresarial. La confianza digital genera fidelidad del cliente y más ingresos.

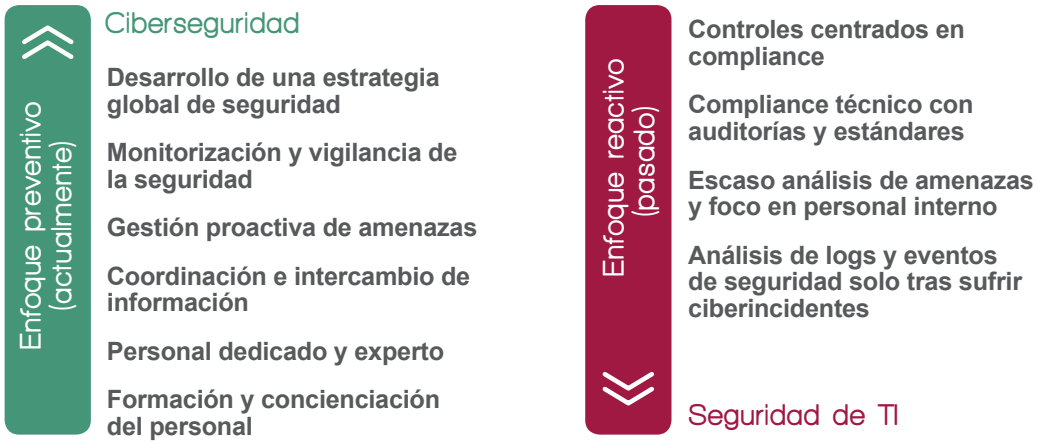
[26] ***Mckinsey.*** *Building security into the customer experience (2020)*

Driver de crecimiento

La clave es entender la ciberseguridad como un elemento facilitador de la estrategia. Solo con una ciberseguridad robusta se podrá abordar el crecimiento. Esta visión debe arrancar desde arriba, desde el CEO, que integrará la ciberseguridad en la estrategia y en los objetivos de negocio. Esto permite alinear las estrategias a corto y largo plazo, agregar valor en las ofertas comerciales utilizando la ciberseguridad como elemento diferenciador y aprovechar el liderazgo para construir una sólida ciber cultura, subraya Mckinsey.

Esta visión tiene mucho que ver con el cambio de enfoque que se ha dado estos años al abordar la ciberseguridad: desde un enfoque reactivo a otro proactivo, para anticiparse y estar preparado. Las nuevas tecnologías como Data Analytics e Inteligencia Artificial permiten afinar más este enfoque preventivo, sin dejar de ofrecer un servicio personalizado a millones de clientes, mejorando su experiencia y generando nuevos productos y más ingresos. Los empresarios creen ampliamente que la ciberseguridad facilitará más aún la innovación empresarial, según una encuesta recogida en el informe de Wall Street Journal Intelligence y Forcepoint , que subraya que el 41% de los líderes empresariales cree que la ciberseguridad aporta ventaja competitiva.

Un cambio de enfoque muy reseñable



Fuente: *La Fábrica de Pensamiento. Ciberseguridad: Una guía de supervisión.*

[27] ***Mckinsey.*** *Transition to the next normal: Enhancing cybersecurity in the Iberian Peninsula. (Julio 2020)*

[28] ***Wall Street Journal Intelligence y Forcepoint.*** *The C-Suite Report: Business and Security Strategies for Today's Unbound Enterprise. (Mayo 2021)*

Muchas empresas contemplan adoptar nuevas arquitecturas de seguridad como *Zero Trust y Secure Access Service Edge (SASE).* Tomen nota porque, aunque suena técnico, los ingenieros de ciberseguridad ven su adopción como un paso clave para responder a los desafíos de la transformación digital, la computación perimetral y la ubicuidad de los empleados.

La ciberseguridad es un elemento transversal clave dentro de cualquier organización

Refuerzo del CISO: el equipo como primera defensa

En el mundo anglosajón se le conoce como CISO – *Chief Information Security Officer*–. En España será más bien el ISO o RSI, como Responsable de Seguridad de la Información. Todas las empresas deberán contar con uno, según el Real Decreto Ley que aprobó el gobierno en enero[29]. El responsable de seguridad digital ostentará las competencias para elaborar y supervisar las políticas de seguridad y las medidas técnicas y organizativas a implantar en la organización. Al margen del detalle anecdótico de las siglas, lo cierto es que contar con un equipo técnico de calidad es la primera línea de defensa de la organización en lo que a ciberseguridad se refiere. La segunda sería una dirección de riesgos importante y la tercera, sin duda, Auditoría Interna, que cada vez tiene más que decir sobre este riesgo.

La confianza digital genera fidelidad de clientes y permite más ingresos

Los clientes reclaman seguridad y transparencia: huyen si perciben riesgos

[29] **BOE.** *Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

Los sectores más afectados
(coste medio por brecha de seguridad en millones $)

***Fuente:** IBM Security, Cost of a Data Breach Report 2021*

Impacto en el rating

La ciberseguridad no cotiza en bolsa, pero sí está en los precios de los activos vía el rating crediticio de la organización. Las agencias de rating están teniendo en cuenta el perfil, el gobierno de la ciberseguridad y las medidas que adoptan las compañías antes de asignarlas un rating. Una mala gestión de un ciberataque puede llevar a un recorte del rating como ocurrió con la americana SolarWinds, *hackeada* en 2020[30]. Y con peor rating, todo se encarece, empezando por la financiación. También están surgiendo multitud de agencias que califican la seguridad *(security score)* tras analizar su capacidad de proteger los datos de posibles ciberataques. *Black Kite, BitSight y SecurityScorecard* son algunas de esas agencias, la mayoría americanas[31].

La mirada del Auditor Interno

Preguntas clave

Éstas son las cuestiones más relevantes que, a los ojos del Auditor Interno, hay que hacerse para asegurarse una priorización y supervisión adecuada del riesgo de ciberseguridad.

1. ¿Se han reforzado con la pandemia la formación y concienciación del personal?
2. ¿Se cuenta con los recursos necesarios para la monitorización, vigilancia y gestión preventiva de la ciberseguridad?
3. ¿Se dispone de procedimientos y protocolos de gestión, respuesta y recuperación ante incidentes de seguridad? ¿Se han hecho simulacros?
4. ¿Se realizan periódicamente ejercicios de intrusión (hacking ético) en los sistemas?
5. ¿Se hacen controles de ciberseguridad a los proveedores externos antes y durante la relación comercial?
6. ¿Hay una cultura de ciberseguridad adecuada y se fomenta la colaboración entre ciberseguridad y las áreas relacionadas como compliance, privacidad, etc.?

Funciones del Auditor Interno

Auditoría Interna proporciona aseguramiento en la evaluación de la eficacia del gobierno de las Tecnologías de la Información, la gestión de los riesgos y los controles internos de esta materia.

Auditoría Interna debería participar o estar informada puntualmente de las actividades de las áreas de seguridad de sistemas. Puede participar en ejercicios de revisión técnica de la seguridad, con el fin de identificar riesgos no identificados en las capas anteriores. Apuntamos los principales aspectos en materia de ciberseguridad que deberían ser preocupación y objeto de revisión por parte de Auditoría Interna.

1. Colaborar con la dirección de la compañía en la creación y desarrollo de una estrategia y política de ciberseguridad.

2. Asegurar que la organización cuenta con un correcto nivel de madurez y capacidad para la identificación y mitigación de los riesgos de ciberseguridad.

3. Verificar los mecanismos para reconocer incidentes de ciberseguridad procedentes de un empleado o proveedor externo.

4. Aprovechar las relaciones con la dirección de la compañía para aumentar el nivel de concienciación con los riesgos de ciberseguridad del Consejo, así como su implicación y compromiso con cuestiones clave en esta materia, como la actualización de la estrategia de ciberseguridad de la compañía.

5. Integración en el plan. La ciberseguridad se encuentra formalmente cubierta e integrada en el Plan de Auditoría Interna.

6. Entender y desarrollar un perfil de riesgo en ciberseguridad de la compañía, teniendo en cuenta las nuevas tecnologías y tendencias emergentes.

7. Evaluar
el programa de ciberseguridad de la compañía con el marco de ciberseguridad de la NIST, y otros estándares tales como ISO 27001 y 27002.

8. Identificar
y evaluar las capacidades preventivas de control de la ciberseguridad en materia de educación, formación y concienciación de usuarios, así como procesos y herramientas de control y vigilancia digital.

9. Asegurar
que la monitorización y gestión de ciberincidentes es considerada una prioridad en la compañía, existiendo un proceso de escalado claro al respecto.

10. Identificar
cualquier carencia o falta de personal de IT y Auditoría Interna que pueda representar un impedimento para alcanzar los objetivos y retos de ciberseguridad de la compañía.

Referencias: normativas y documentos relevantes.

- **Instituto de Auditores Internos de España.** La Fábrica de Pensamiento. Ciberseguridad. Una guía de supervisión. Edición Consejeros; Informe Risk in Focus 2021; Guía Práctica sobre Ciberseguridad y protección de datos. Los lunes del Instituto. Ciberseguridad: regulación europea y el papel de Auditoría Interna. 2021 Risk in Focus (2020)
- **Global Institute of Internal Auditors.** The IIA cibersecurity Resource Exchange. IIA UK-Mind the Gap: Cyber security Risk in the new normal. 2021 Risk Report (2020)
- **National Institute of Standards and Technology (NIST).** Cybersecurity Framework.
- **COSO.** Managign Cyber Risk in a Digital Age (2019)
- **Securities and Exchange Commission (SEC):** Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2018). Cybersecurity and Resiliency Observations (2020)
- **Banco Central Europeo (BCE).** Cyber resilience
- **Banco Internacional de Pagos de Basilea (BIS).** Covid-19 and cyber risk in the financial sector (2021)
- **Comisión Europea.** Nueva Estrategia de Ciberseguridad de la UE y nuevas normas para aumentar la resiliencia de las entidades críticas físicas y digitales.; EU Security Union Strategy 2020-2025; Directive on Security of Network and Information Systems (NIS 2); Directiva sobre resiliencia de entidades críticas y Reglamento Ley de Resiliencia de Operativa Digital.
- **Banco Mundial.** Financial Sector's Cybersecurity: A Regulatory Digest (Mayo 2019)
- **CCN-CERT.** Informe Ciberamenazas y Tendencias (2020)
- **ONTSI.** Dossier de Indicadores sobre Ciberseguridad y Confianza Digital en España y Europa (2020)
- **Agencia de ciberseguridad de la Unión Europea (ENISA):** Cybersecurity Incident Report and Analysis System (2020); Threat Landscape: The year in review (2020)
- **INCIBE.** Balance ciberseguridad 2020. Gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020.
- **BOE.** Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.
- **World Economic Forum (WEF), National Association of Corporate Directors (NACD) y Internet Security Alliance (ISA):** Principles for Board Governance of Cyber Risk (Marzo 2021)
- **Autoridad Bancaria Europea (EBA).** EU-wide stress testing (Enero 2021)
- **Banco Central Europeo (BCE).** What is cyber resilience?

- **Global S&P.** Baja rating de SolarWinds (Abril 2021) Artículo de Simon Ashworth, Head of Analytics and Research, Insurance at S&P Global Ratings. The Increasing Credit Relevance of Cybersecurity (2021)
- **World Economic Forum y University of Oxford.** Cybersecurity, emerging technology and systemic Risk (2021)
- **World Economic Forum.** 2021 Global Risks Report.
- **IBM Security.** Cost of a Data Breach Report 2021. IBM X-Force Threat Intelligence Index.
- **McAfee y Center for Strategic and International Studies (CSIS).** The Hidden Costs of Cybercrime (2020)
- **Cisco** Future of Secure Remote Work Report (2021) Security Outcomes Study - Proven Factors for Your Security Program (2021) Simplify to Secure Cybersecurity Report (2021)
- **Gartner:** Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025 (Enero 2021)
- **Harvard Business Review.** Cyberattacks Are Inevitable. Is Your Company Prepared? (2021)
- **BCG.** Ensuring Online Security in a Quantum Future (2021)
- **Forbes.** Cybersecurity In The New Normal: Good Enough Is No Longer Enough
- **Cybercrime Magazine.** 10 Hot Security Ratings Companies To Watch In 2021 (Enero 2021)
- **Mundo Hacker 2021.** Presentación sobre Zero Trust de Asier Ortega Peciña, Senior Sales Engineer Forcepoint Iberia.
- **El País.** La caída global de miles de páginas alerta sobre la fragilidad de Internet (9 junio 2021). Ciberataques que matan a las empresas. (2020)
- **Reuters.** Target cyber breach hits 40 million payment cards at holiday peak (2013) Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed (9 mayo 2021) Biden administration eyes cybersecurity funding after hacks (18 mayo 2021)
- **Wall Street Journal Intelligence y Forcepoint.** The C-Suite Report: Business and Security Strategies for Today's Unbound Enterprise. (Mayo 2021)
- **Mckinsey.** COVID-19 crisis shifts cybersecurity priorities and budgets (2020). Transition to the next normal: Enhancing cybersecurity in the Iberian Peninsula (2020). Cybersecurity: Emerging challenges and solutions for the boards of financial-services companies (2020). Cybersecurity in Iberia: Aligning business and the board (Abril 2021). Building security into the customer experience (2020)
- **Deloitte.** Board Practices Quarterly: Cyber oversight (Mayo 2021) Impacto del COVID en la ciberseguridad. The impact of Cyber on "critical infrastructure" in the Next Normal (2020)

- **KPMG.** Cinco respuestas: Cómo evitar los ciberataques y el bloqueo de sistemas. El modelo empresarial del Cibercrimen. KPMG Tendencias. El modelo empresarial del Cibercrimen; Consideraciones clave para la gestión de ciberincidentes (2020); Vídeo: Cinco respuestas: Cómo evitar los ciberataques y el bloqueo de sistemas (marzo 2021)
- **PwC.** Ciberseguridad: cómo gestionar el impacto del COVID-19
- **EY.** Technology and information security

Instituto de Auditores Internos de España.
Santa Cruz de Marcenado, 33 - 28015 Madrid
Tel.: 91 593 23 45 - Fax: 91 593 29 32
www.auditoresinternos.es

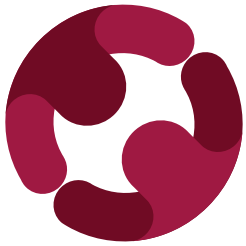
Depósito Legal: M-21197-2021

ISBN: 978-84-122588-5-1

Diseño y maquetación: Blondas de Papel S.L.

Instituto de Auditores Internos de España

RiesgosClave



esfera consejeros

Members of

The Institute of Internal Auditors