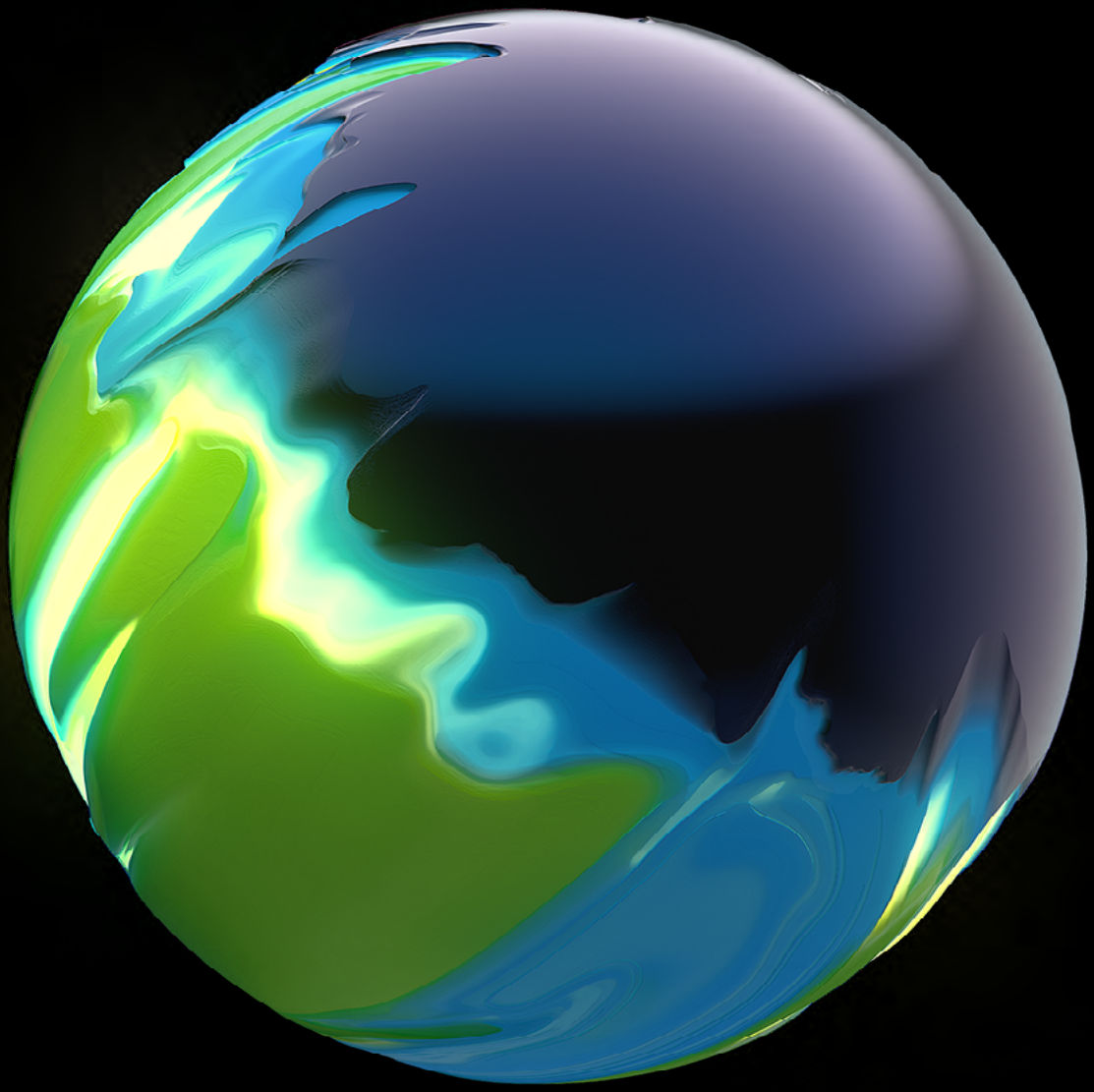
Deloitte.



El estado de la ciberseguridad en España

"Post pandemia: un camino inexplorado"

2022

DELOITTE CYBER STRATEGY | EMPOWERING YOUR PEOPLE FOR THE FUTURE

Índice

Introducción

El presente estudio, *El Estado de la Ciberseguridad en España 2021,* muestra por **tercer año consecutivo** los resultados del análisis realizado a las empresas españolas con el fin de medir cómo se encuentran las mismas en materia de ciberseguridad y analizar su evolución estos años.

Este estudio se ha convertido en todo un referente nacional que satisface la necesidad de disponer de información actualizada, útil y detallada sobre el estado en el que se encuentran las empresas españolas con respecto a la seguridad de sus sistemas de información. El estudio nació para cubrir el gap existente entre los estudios nacionales, que no arrojaban información comparativa sectorial detallada, y otros informes de analistas consagrados que ofrecían una información similar al presente, pero con un alcance internacional y no nacional.

Esta edición, "Post pandemia: un camino inexplorado", presenta los resultados del análisis realizado en un momento de gran incertidumbre para las organizaciones. A raíz de las medidas de teletrabajo impuestas por los confinamientos a nivel mundial, el número de ciberataques se ha incrementado considerablemente. Estas medidas han acelerado al mismo tiempo los planes de digitalización de las compañías, en las que los procesos críticos de negocio se están transformando y empiezan a depender fuertemente de la tecnología.

A esto se suma una mayor demanda de servicios de ciberseguridad, para los cuales se necesita un talento formado y con experiencia, que es escaso en la industria y que no parece que vaya a aumentar en el corto-medio plazo.

Asimismo, las políticas monetarias expansivas han provocado una inflación, la cual no se sabe si será transitoria o no, y que está generando un aumento de precios y agravando la escasez de semiconductores.

Todos estos cambios que se están produciendo tan rápidamente obligan a los CISO y responsables de ciberseguridad a plantear una estrategia de ciberseguridad en lo que denominados "un camino inexplorado".

Este año agradecemos la masiva respuesta, puesto que se ha superado las 100 empresas que han participado en el estudio. También se quiere agradecer el interés y entusiasmo crecientes que despierta el presente informe año tras año.

Adicionalmente, para esta edición, se ha realizado un trabajo previo de análisis de qué indicadores son relevantes y de mayor utilidad para la comunidad. Este análisis sobre la idoneidad de los indicadores clave a recopilar en el estudio ha sido realizado en varias sesiones de trabajo con más de 20 CISO, junto a los responsables del área de Cyber Strategy de Deloitte.

El Estado de la Ciberseguridad en España 2021 cuenta con el análisis de más de **40 indicadores agrupados en 10 dominios,** facilitando la lectura de las principales conclusiones de una forma más ordenada.

Cyber Strategy, ¿quiénes somos?

El área de Cyber Risk Advisory de Deloitte cuenta con una línea de servicio especializada en estrategia de ciberseguridad, denominada **Cyber Strategy,** la cual es la autora de este estudio.

Cyber Strategy es una línea de servicios que requiere para su día a día información actualizada y sectorial para ayudar a las empresas a definir sus estrategias y tomar las decisiones correctas en materia de gobierno de la seguridad en base a comparables.

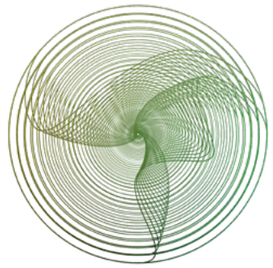
Cyber Strategy ya dispone de información útil en esta materia, gracias a la experiencia obtenida en los cientos de proyectos ejecutados estos años, la cual permite a Deloitte realizar *benchmarks* sectoriales sobre ciberseguridad al detalle, entre otros. A pesar de ello, tradicionalmente se ha observado la falta de información sectorial disponible públicamente y que pudiera ser de utilidad para toda la industria, especialmente para los CISO y otros responsables de ciberseguridad en España.

De esta necesidad nace este estudio hace 3 años, contribuyendo y fomentando la compartición de información relevante, que beneficia especialmente a la ciberresiliencia de las empresas españolas.

Los servicios de consultoría ofrecidos por esta línea de Deloitte destacan por la definición de planes estratégicos y directores de ciberseguridad, la definición de los modelos operativos y de gobierno, además de la evolución de los SOC y CSIRT de las empresas a través de la mejora de estos servicios, orientando los mismos a la cobertura real de amenazas.

Dado que Cyber Strategy ayuda a los principales CISO y responsables de ciberseguridad en España, a través de servicios como los mencionados, el análisis realizado en el presente estudio tiene como objetivo y foco facilitar a la dirección de las compañías la toma de decisiones estratégicas.

Contexto: otras iniciativas



The CISO Program

Los **Executive Programs** de Deloitte se han desarrollado con el objetivo de ayudar a los líderes empresariales a lo largo de su carrera para asegurar su éxito personal y profesional, focalizándonos en sus prioridades y aspectos clave que les preocupan, a la vez que fomentamos el establecimiento de relaciones de confianza.

Entre estos programas se encuadra el **CISO Program.** Este nuevo modelo nace con el objetivo de ayudar a los principales líderes de seguridad de la información a mantenerse por delante de los crecientes desafíos y demandas del mercado. Surge en un momento en el que la figura del CISO se ha convertido en una pieza fundamental e imprescindible para conseguir alinear la estrategia de ciberseguridad con el negocio.

¿Por qué un CISO Program?
El papel del CISO está evolucionando:

- La ciberseguridad se ha convertido en una **necesidad primordial** para cualquier empresa.
- **Reorientación del rol del CISO** con el desafío de diseñar una estructura de reporte para los programas de seguridad de la información que equilibre los requerimientos de cada una de las partes implicadas a nivel empresarial.
- Elevada **presión para responder a las expectativas de negocio.** Revisiones de seguridad, entornos *Cloud* y nuevas tendencias tecnológicas que conllevan una alta concienciación de la importancia de realizar revisiones periódicas sobre las aplicaciones imprescindibles para cada modelo de negocio.
- Mayor **relevancia de las tecnologías** Blockchain, IA, Machine Learning y Algoritmos Predictivos que se implantan como herramientas clave en la ciberseguridad de las empresas.

El Estado de la Ciberseguridad en España 2021. Post pandemia: un camino inexplorado es la tercera edición del análisis nacional de las tendencias del sector, elaborado con resultados obtenidos del feedback de más de 100 CISO.

Este estudio se encuentra enmarcado como iniciativa principal dentro del CISO Program, con el objetivo de generar eminencia y servir como documento de referencia para industria.

Para obtener más información sobre los Executive & Board Programs de Deloitte, escribe al correo executiveprograms@deloitte.es.

En caso de estar interesado en el CISO Program de la Firma, contacta con el responsable de la iniciativa, Rubén Frieiro, Socio de Risk Advisory Cyber de Deloitte a través de su email: rfrieiro@deloitte.es

Future of Cyber 2021

Deloitte ha realizado un estudio internacional denominado ***Future of Cyber***[1] **en el 2021** durante el 6 de junio y el 24 de agosto, a través del cual se encuestó de manera online a casi **600 ejecutivos C-Level,** incluidos casi 200 CISO, 100 CIO, 100 CEO, 100 CFO y 100 CMO **de empresas con unos ingresos anuales de al menos 500 millones de dólares.**

Future of Cyber ha puesto el foco en los procesos de transformación digital de las compañías desde la perspectiva de ciberseguridad, de tal manera que se ahonda en conceptos como el paradigma Zero Trust, la identidad digital y cómo se deben recoger los datos de los usuarios, así como las tecnologías emergentes como el IoT, entre otras cuestiones.

El presente estudio, ***El Estado de la Ciberseguridad en España 2021,*** **muestra diferencias significativas** por las que no solo resulta necesario que ambos estudios convivan, sino que ambos se complementan perfectamente:

- En primer lugar, el presente estudio tiene **foco exclusivamente en España,** lo cual nos sirve como termómetro del estado la ciberseguridad en el país.
- **Este análisis busca conocer la realidad de la ciberseguridad en el país a través de la visión de los responsables de ciberseguridad y los CISO,** puesto que estos son los que lidian en primera instancia con la ciberseguridad en sus empresas y tiene información más detallada. Gracias a esto se puede profundizar en cuestiones que otros responsables fuera del área de ciberseguridad probablemente desconozcan.
- Y, finalmente, **el objetivo último de este informe es poder ayudar a la sociedad y las empresas del país a través de información útil, comparable y específica que pueda ayudar a definir sus estrategias de ciberseguridad.** Por esta razón, se analizan cuestiones como el modelo operativo, los incidentes sufridos, los marcos de referencia o la percepción del CISO y sus preocupaciones, entre otras.

Como se puede apreciar, estos estudios son herramientas de gran utilidad para los responsables de ciberseguridad. Ambos se complementan y proveen información pública que permite a las empresas mejorar su gobierno de la ciberseguridad, pudiendo al mismo tiempo conocer las tendencias y analizar el estado general del sector.

Adicionalmente, nótese que a lo largo del presente estudio se hace referencia al estudio *Future of Cyber* para complementar los hallazgos realizados.

1. https://www2.deloitte.com/global/en/pages/risk/articles/future-of-cyber.html

Muestra del estudio

En primer lugar, se quiere **agradecer en esta edición a ISMS Forum su participación en el estudio en la fase de recolección de información, la cual ha ayudado a que este año se haya alcanzado la cifra de más de 100 CISO y responsables de ciberseguridad que han participado.** Se trata de la muestra más alta obtenida hasta la fecha en este estudio.

Se quiere destacar que todas las empresas analizadas son empresas españolas o cuyo centro de operaciones de ciberseguridad reside en España.

Toda la información obtenida se ha anonimizado, manteniéndose en todo momento la confidencialidad y privacidad de las empresas participantes.

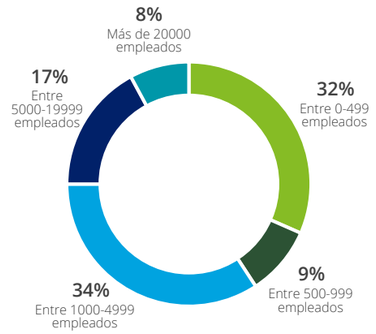
A continuación, se analiza el perfil de las empresas del estudio a través de dos variables: el número de empleados y sector al que pertenece la organización.

Como se puede apreciar, **la mayoría de las empresas participantes tienen entre 1.000 y 5.000 empleados en España,** seguidas de las más pequeñas, que tienen menos de 500.

Las organizaciones más grandes, las que cuentan con más de 20.000 empleados en España, representan el 8%, mientras que el 17% disponen entre 5.000 y 20.000 empleados.

Respecto al análisis por sectores de mayor a menor participación, podemos destacar que la Banca, con un 20%, ha sido el sector que más ha participado. Esto no solo es reflejo del alto nivel de madurez de este sector, sino de su concienciación con las buenas prácticas en la compartir información que sea de utilidad a la industria.

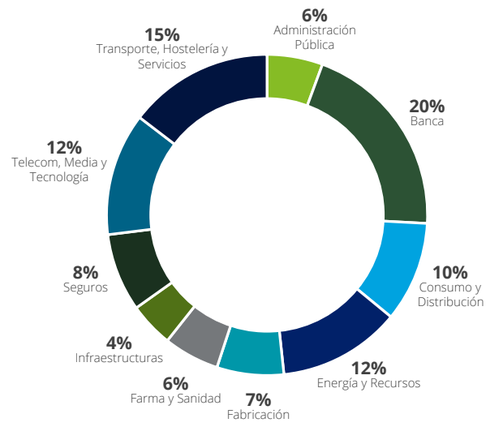
Gráfico muestra 1: Volumen de empleados



En segundo lugar, también son destacables las empresas de transporte, hostelería y servicios, con un 15%, y energía y recursos, además de telecomunicaciones, media y tecnología, con un 12% en ambos casos. El resto de los sectores solo representan el 41%.

Se aprecia una **distribución por sectores equilibrada,** lo cual facilita a que la calidad del dato sea idónea para extrapolar conclusiones significativas para todas las empresas.

Gráfico muestra 2: Distribución sectorial



Dominios del estudio

Para una mejor comprensión de las principales conclusiones del estudio, se ha decidido agrupar las mismas en dominios comunes a cualquier empresa. No obstante, señalamos que se pueden encontrar conclusiones obtenidas del cruce de dos o más dominios diferentes. De esta manera, se ha podido inducir cierta información relevante, que es imposible obtener a través de un simple análisis individualizado de las cuestiones planteadas por separado. Por ello, se puede encontrar información dentro de un dominio que también contenga parte de la información de otro.

01 Headcount[2]

El entorno en constante cambio de amenazas y nuevas tecnologías obliga a las compañías a redimensionar de forma continua el número de personas asignadas a la función de ciberseguridad.

02 Presupuesto y servicios

Sin lugar a duda, el aumento de los ciberataques y la necesidad de mayor ciberseguridad, obligan a los CISO a demandar mayores presupuestos año a año, siendo indispensable a su vez la optimización de dichos recursos. Una estrategia ineludible y no siempre fácil de implementar, es la de concienciar a la alta dirección para que perciban los servicios internos de ciberseguridad como una inversión y futuro ahorro de costes, al evitar y gestionar eficazmente los posibles ciberincidentes y no solo como un puro gasto más para el negocio.

03 Modelo Operativo y políticas

El modelo operativo hace referencia a la organización de las compañías, que principalmente suele reflejarse en la configuración de sus organigramas, roles y responsabilidades. La definición de un modelo operativo eficiente en materia de ciberseguridad, combinado con el cumplimiento de políticas, no solo a nivel nacional, ayudan a los CISO a optimizar la distribución del personal dedicado a seguridad y los presupuestos asignados.

04 Certificaciones, *framework*[3] y formación

Las certificaciones, *frameworks* y acciones de formación y concienciación facilitan a las empresas y profesionales el aprovechamiento de las buenas prácticas de la industria. Estas, a su vez, son una herramienta idónea para medir de forma objetiva la consecución de niveles de madurez por capacidades específicas de ciberseguridad. Qué certificaciones y *frameworks* abordar suele ser objeto de debate y discusión entre los diferentes CISO, al no haber un verdadero consenso sobre cuáles son los más útiles o demandados en el mercado.

05 Revisiones de seguridad

En este dominio se recoge información sobre las revisiones de seguridad realizadas en entornos críticos de las compañías, de manera planificada o no, que cubren los aspectos técnicos y de cumplimiento, de las que se pueden derivar posibles planes de acción a ejecutar.
Las revisiones de seguridad son necesarias para asegurar que los controles están implantados tal cual fueron diseñados y que su rendimiento es el correcto.

2. Número de personal
3. Marco de referencia (i.e: ISO 27.000, NIST, Deloitte CSF...)

06 Entornos Cloud y tendencias tecnológicas

Una de las preocupaciones de los CISO y los responsables de seguridad en los tiempos actuales es el uso que se hace de las infraestructuras en la nube y en cómo se opera y se despliega el *stack* tecnológico sobre estos entornos de terceros.

La nube ya es una realidad para un gran número de empresas, mientras que para otras sigue siendo un reto dentro su plan de transformación digital, los cuales no solo incorporan *Cloud* como una de sus claves estratégicas, sino el uso de tecnologías igualmente "disruptivas" como puede ser el uso masivo del IoT[4].

07 Incidentes de seguridad

Probablemente la mayor preocupación de los CISO es saber cuándo y cómo recibirá el siguiente ciberataque o ciberincidente. Para facilitar información de interés en este contexto, en este estudio se analizan cuáles son las estadísticas de incidentes en los últimos años, también a nivel sectorial.

El incidente de seguridad es el indicador clave que se ha usado en mayor medida para correlacionar información con otros dominios. Por ello, es fácil que se encuentre muchos puntos donde se ahonda en diferentes cuestiones en relación con el número de incidentes y, por tanto, se encuentre dicha información dispersa fuera de este dominio concreto.

08 Simulaciones de cibercrisis e incidentes

Puesto que los incidentes son el indicador clave del presente estudio, este año se ha querido aportar un análisis más profundo de esta cuestión, ahondando en esta ocasión en cómo preparar a las compañías y entrenar a sus diferentes equipos (alta dirección, equipos tácticos y equipos técnicos/operativos) para hacer frente a estos ciberincidentes y cibercrisis.

09 Percepción del CISO

Una vez analizados datos cuantificables y objetivos sobre el estado de la ciberseguridad en las empresas, es necesario conocer qué es lo que percibe el CISO, qué es lo que realmente piensa sobre las tareas que realiza, las que debería realizar, cómo de concienciada está su dirección y cómo de confiado o confortable se siente para hacer frente al próximo ciberataque que sufrirá su compañía.

10 Percepción del CISO en tiempos de teletrabajo

La COVID-19 ha supuesto un cambio de paradigma en la sociedad. No solo está siendo una crisis en materia sanitaria, sino que está suponiendo todo un reto para las organizaciones en términos de digitalización y ciberseguridad, debido al teletrabajo y la demanda de servicios online.
Las medidas de confinamiento y las restricciones de movilidad dictadas por el Gobierno de España y sus comunidades autónomas han obligado a muchos negocios a cambiar sus procesos y métodos de trabajo para contemplar el teletrabajo, entre otros cambios. Esta forzada digitalización ha supuesto en algunos casos un reto para los CISO, puesto que el contexto de la empresa ha cambiado lo suficiente como para adaptar y replantear rápidamente los modelos de ciberseguridad ante esta nueva realidad.

4. Internet of Things

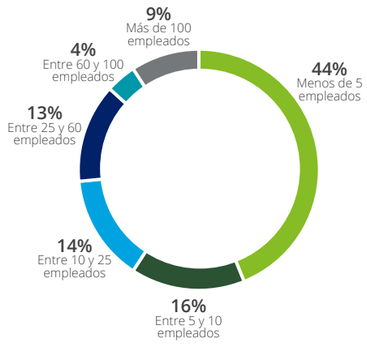
01 Headcount

Un dato relevante para medir el grado de ciberresiliencia de una organización es la cuantificación de los recursos que destina a su ciberseguridad, no solo en términos presupuestarios, sino también en las personas con dedicación en exclusiva a esta tarea.

Más de la mitad de los empleados dedicados en exclusividad a ciberseguridad son recursos externos a la organización

En este contexto y debido al volumen razonablemente elevado de empresas de tamaño pequeño-medio del estudio, solo el 13 % de las empresas tiene más de 60 empleados dedicados en exclusiva a la ciberseguridad. El resto de los rangos tienen una distribución más equilibrada: 16% entre 5 y 10 empleados, 14% entre 10 y 25, y 13% entre 25 y 60.

Gráfico 1.1: Dedicación exclusiva a Ciberseguridad

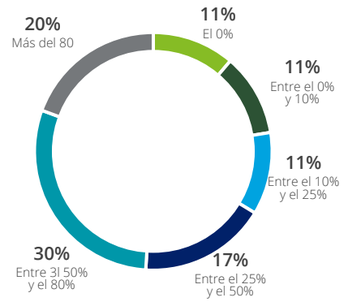


La media de los empleados externos con dedicación en exclusiva al área de ciberseguridad frente al total es del 56%.

Se puede observar cómo solo el 11% de las empresas no tiene personal externo de ciberseguridad, frente al 20% que cuenta con más del 80% de externalización.

De hecho, se observa que lo más habitual es externalizar entre el 50% y el 80% del personal de ciberseguridad, lo cual evidencia **la necesidad de hacer uso del talento externo para poder cubrir las capacidades internas en ciberseguridad.**

Gráfico 1.2: Personal externalizado



Las compañías han evolucionado a una dedicación homogénea de recursos según los dominios de ciberseguridad, destacando el incremento de esfuerzo que ganan las tareas relacionadas con el gobierno y la estrategia

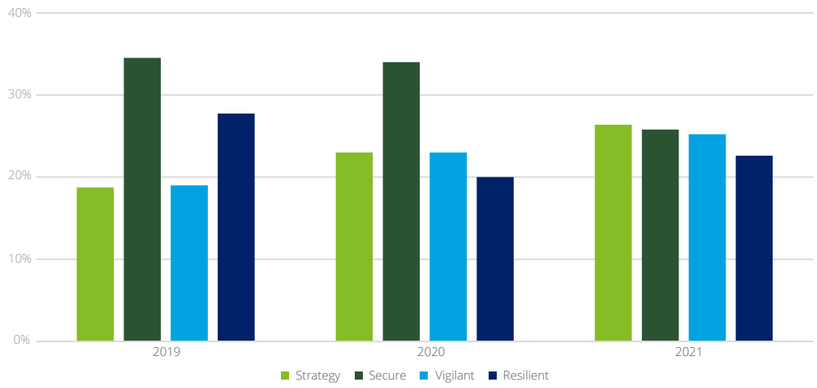
En años anteriores, la distribución por empleados en función de los cuatro dominios de Ciberseguridad de Deloitte, Gobierno[5], Protección[6], Vigilancia[7] y Resiliencia[8], era desigual: tanto en 2019 como en 2020, la asignación de recursos a Protección destacaba con creces sobre el resto de los dominios. En cambio, los datos de 2021 arrojan una luz distinta: evolución hacia la homogeneidad. Con una distribución en Gobierno, 26%, Protección 26%, Vigilancia 25% y Resiliencia 23%, la distribución es más homogénea.

Esto se debe a que poco a poco las organizaciones han evolucionado de la mera implantación de controles y su monitorización a una distribución homogénea de capacidades. El buen gobierno y la capacidad de ciberresiliencia toman entonces un papel clave a medida que va madurando la ciberseguridad en las compañías.

El 81% de los CISO y responsables de ciberseguridad considera que no dispone del personal suficiente

Además de la evidente necesidad de mayor dotación presupuestaria para la contratación de personal de ciberseguridad en las compañías españolas, se ha ido reduciendo porcentualmente el talento de ciberseguridad disponible, no solo en España, sino en prácticamente todos los países del mundo.

Gráfico 1.3: Empleados de Ciberseguridad según Dominio

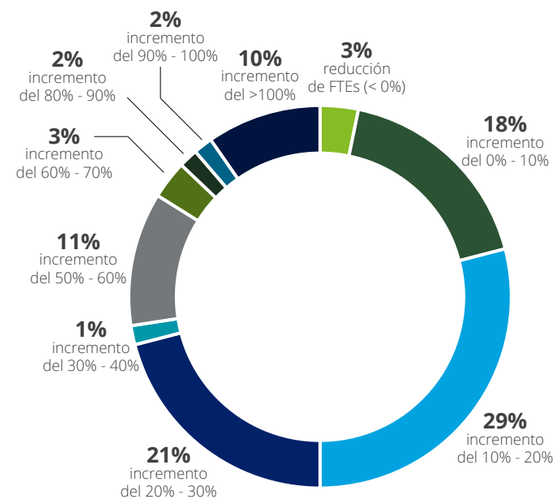


5. Estrategia y gobierno de la ciberseguridad
6. Implantación de controles de ciberseguridad de todo tipo: securización y bastionado de infraestructuras y redes, protección de la información confidencial, protección y gestión de la identidad digital, etc.
7. Típicamente relacionado con todas las tareas de monitorización interna (SIEM, etc.) y externa (monitorización en Internet, ciberinteligencia, etc.) que se realiza desde el SOC (Centro de Operaciones de Seguridad).
8. Todas las tareas de preparación y respuesta ante ciberincidentes o cibercrisis.

Esto ha llevado a una situación que puede considerarse de **"crisis" de talento en ciberseguridad,** puesto que aquellas empresas que disponen de presupuesto suficiente para la contratación de dicho personal se ven incapaces en muchos de los casos de cubrir las vacantes abiertas por falta de candidatos cualificados.

Uno de los factores que más retrasan, o directamente impiden, el desarrollo de las iniciativas de ciberseguridad es precisamente esta falta de personal de ciberseguridad. De hecho, este fenómeno se debe considerar como una vulnerabilidad más en las organizaciones, al no poderse realizarse las tareas necesarias en los tiempos planificados.

Gráfico 1.4: Incremento porcentual de FTEs de Ciberseguridad en 2021



En términos generales, se puede apreciar cómo ha habido un incremento del 38% de media de FTEs[9] de ciberseguridad

Este dato es contundente, **las empresas están incrementando notablemente la cantidad de personal dedicado a ciberseguridad,** hecho que agrava la ya mencionada "crisis" de talento. **La incorporación de personas al mercado laboral con formación en ciberseguridad aumenta más lentamente que la demanda.** Por este motivo, otros profesionales con *background* técnico empiezan a reorientar su carrera a la de ciberseguridad debido a la alta oferta. Hoy en día, se debe considerar la ciberseguridad desde una perspectiva holística, de tal manera que no solo se debe tener en cuenta al personal dedicado al departamento de ciberseguridad, sino que existen otros actores dentro de las organizaciones con roles muy relevantes que son clave en la ciberresiliencia de la compañía. Por ejemplo, los desarrolladores de software o los técnicos del área de comunicaciones IT, entre otros, son piezas imprescindibles en la estrategia ciberseguridad de sus empresas.

En este sentido, para un 45% de las empresas hay responsabilidades de ciberseguridad fuera de este departamento.

Este dato refleja cómo las organizaciones están madurando de tal manera que no solo se atribuye la ciberseguridad a un departamento específico, sino que, al ser la ciberseguridad un activo que aporta valor al negocio a través de la protección de este, la responsabilidad recae en toda la organización, siendo los responsables últimos en velar por la ciberseguridad la alta dirección.

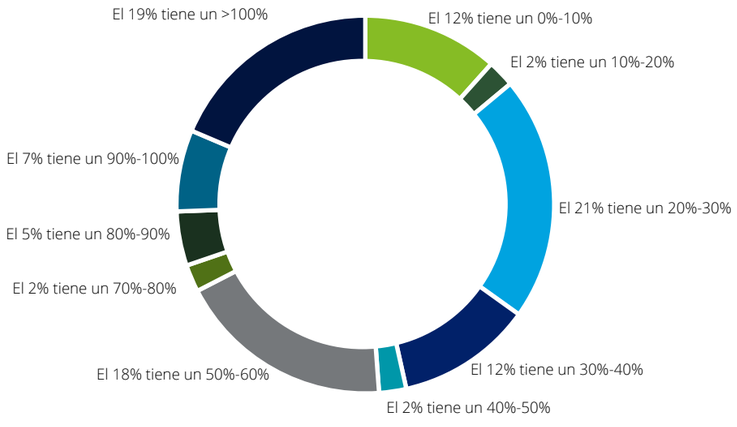
Si se toma únicamente el rango de empresas cuyas responsabilidades de ciberseguridad van más allá de dicho departamento, se puede analizar en qué porcentaje de empleados se aplican estas responsabilidades.

9. Full Time Equivalent por sus siglas en inglés. Hace referencia al número de personal dedicado en exclusiva, en este caso, a labores de ciberseguridad. Por ejemplo, 3,5 FTE equivale a 3 personas y media dedicadas a estas tareas.

Las empresas más concienciadas y con mayor nivel de madurez en ciberseguridad lideran la iniciativa de asignar una parte de la retribución variable del sueldo de todos los empleados si estos cumplen con los objetivos de ciberseguridad de la organización

Hay que tener en cuenta que todos los empleados de la organización pueden ser considerados como un "riesgo humano", puesto que potencialmente son un posible vector de entrada para el atacante, por ejemplo, a través del phishing, o estos pueden percibirse como un "firewall humano" si están bien formados y concienciados.

Gráfico 1.5: Comparativa entre empleados que se dedican a ciberseguridad y empleados del departamento de ciberseguridad



de empleados externos al departamento con responsabilidades de Ciberseguridad

En este contexto, aún son pocas las organizaciones que han empezado a alinear los incentivos de los empleados con los de los responsables de ciberseguridad para prevenir y detectar más eficazmente posibles ataques. Actualmente, **solo el 4% de las organizaciones cuenta con una retribución variable de su sueldo con base en los objetivos de ciberseguridad de la compañía para empleados que no pertenecen directamente a este departamento.**

Son pocas las empresas, pero es una práctica que previsiblemente irá ganando fuerza según las organizaciones alcancen mayores niveles de madurez en ciberseguridad.

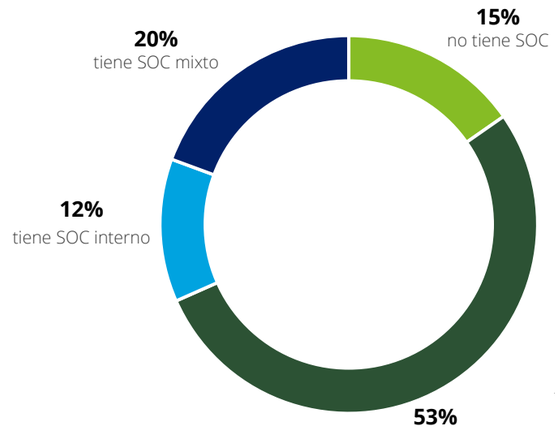
En materia de ciberseguridad es bien conocido que los SOC/CSIRT son servicios que deben estar totalmente integrados con el resto del área. No obstante, la necesidad de una alta especialización y una mayor sofisticación de estos centros de operación ha generado que los proveedores de estos servicios gestionados hayan ganado un papel muy relevante en la industria. Por ello, muchas empresas optan por externalizar estas capacidades en servicios de terceros de forma parcial o total.

Un 53% opta por la externalización total del servicio, mientras que sólo el 12% se ha inclinado por internalizar totalmente esta capacidad. El 20% restante utiliza una modalidad mixta.

La distribución sectorial de las distintas modalidades de configuración del SOC/CSIRT es bastante homogénea: en la externalización pura destaca el sector Transporte, Hostelería y Servicios, con un 23% de las empresas; en el otro extremo, la internalización pura está dominada por el sector Telecom, Media y Tecnología, con un 34%; y la modalidad híbrida, por el sector Banca, con un 27%.

Casi la totalidad de aquellas empresas que no poseen un SOC/CSIRT, tienen menos de 5 empleados dedicados en exclusiva a ciberseguridad, y a su vez, indican que no tienen suficientes empleados para desempeñar las tareas de ciberseguridad. Es decir, son las empresas más pequeñas de la muestra obtenida para el estudio. Por lo tanto, **si excluimos las empresas de menor tamaño, se puede afirmar que todas las empresas disponen de un SOC/CSIRT.**

Gráfico 1.6: SOC/CSIRT propio



El 85% de las empresas cuenta con los servicios de un SOC/CSIRT y casi todos se apoyan en un proveedor externo, bien sea de manera total o parcial

02 Presupuesto y servicios

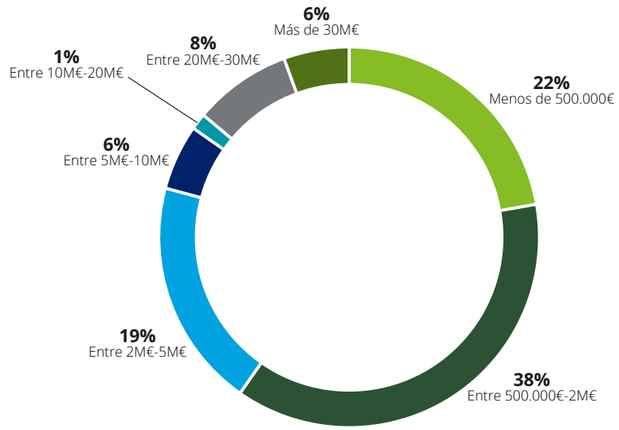
El 79% de las empresas tiene un presupuesto[10] de menos de 5 millones de euros; de ellas, el 28% tiene un presupuesto inferior a 500.000€; el 47% un presupuesto de entre 500.000€ y 2 M€, y el 25%, de entre 2 M€ y 5 M€.

Por otra parte, se aprecia la correlación esperable entre presupuestos y empleados dedicados en exclusiva a ciberseguridad:

- Para presupuestos menores de 500.000€, se dispone de menos de 5 empleados
- Para presupuestos entre 500.000€ y 2 M€, se dispone de entre 5 y 10 empleados. Estas, a su vez, son las empresas que más se externalizan en servicios de terceros.
- Para presupuestos entre de 2 M€ y 20 M€, se dispone de entre 10 y 25 empleados.
- Y para los presupuestos de más de 20 M€ se dispone de más de 60 empleados.

A su vez, en el estudio Future of Cyber de Deloitte realizado a cientos de empresas de todo el mundo, se extraía el siguiente dato: casi el 75% de las empresas con más de 30 trillones de dólares en ingresos (empresas de un tamaño muy relevante)

Gráfico 2.1: Presupuesto de Ciberseguridad



Ciberseguridad representa de media el 9,4% del presupuesto de IT

manifestaron que iban a gastar más de 100 M$ (~88 M€)[11] en ciberseguridad durante este año.
En el presente estudio solo el 6% de los participantes gastan más de 30 M€ en ciberseguridad. No obstante, hay que tener en cuenta que las empresas estadounidenses que participaron en el estudio *Future of Cyber*, disponen de unos presupuestos muy holgados, principal motivo por el que se aprecia un *gap* tan grande.

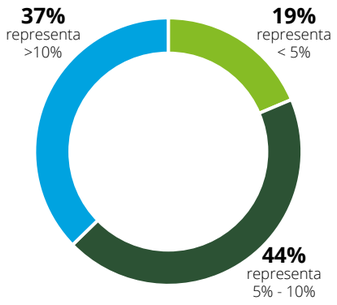
Una comparativa habitual en el sector para analizar la idoneidad de las partidas destinadas a ciberseguridad se basa en comparar este presupuesto frente al de IT.

10. Siempre que se hace referencia al presupuesto de ciberseguridad, se debe tener en cuenta que se excluyen los empleados internos y se incluyen los licenciamientos.
11. Tipo de cambio marcado por el BCE a 12 de enero de 2022.

Gartner, en su estudio *IT Key Metrics Data 2021*, estima que de media el presupuesto de ciberseguridad representa el 4,9% del de IT. Otros analistas sitúan esta cifra alrededor del 10%.

En nuestro caso, esta cifra se sitúa en el 9,4%, donde a su vez se aprecia un ligero incremento respecto al año pasado, en el que el presupuesto de ciberseguridad representaba el 9,3% del de IT (un 0,1% más este año).

Gráfico 2.2: Presupuesto Ciber frente a IT



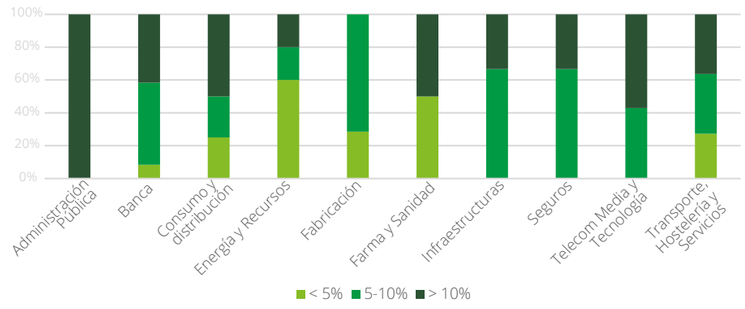
El porcentaje tiene un presupuesto de Ciber que representa un % del presupuesto de IT

Como se puede apreciar, el rango que más destaca son las empresas que destinan a ciberseguridad entre un 5 y un 10% del presupuesto de IT. A su vez, en la gráfica anterior se puede ver cómo las empresas que dedican menos de un 5% del presupuesto de IT a tareas de ciberseguridad son una minoría (el 18%).

Cabe destacar, asimismo, que a mayor inversión en ciberseguridad, menor número de ciberincidentes: **mientras que las empresas que destinan menos de 5 millones de euros en ciberseguridad reciben como mínimo 2,17 ciberincidentes, las empresas que más dinero destinan (30 millones de euros) consiguen reducir ese número a 1,5.** Además, debe tenerse en cuenta que las empresas que más presupuesto dedican a ciberseguridad son a su vez las más grandes y, por tanto, las que se presentan como target más prioritario y evidente para los atacantes. Esto consolida la afirmación de que la inversión en ciberseguridad tiene un claro retorno en materia de ciberresiliencia. Si se realiza un análisis desde el punto de vista de la distribución sectorial, se puede observar que los presupuestos relativos más altos se corresponden con la Administración Pública, Infraestructuras, Seguros y Telecom, Media y Tecnología. En la parte baja de los presupuestos tenemos a Energía y Recursos y Fabricación.

El 63% de las empresas externaliza sus servicios de ciberseguridad, especialmente para tareas de operación y mantenimiento; práctica liderada en mayor medida por las empresas más maduras en ciberseguridad

Gráfico 2.3: Relación entre el presupuesto de Ciberseguridad y el de IT por sectores

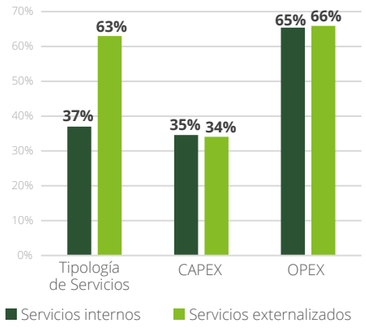


Los CISO y responsables de ciberseguridad están satisfechos con la oferta de servicios disponibles en el mercado, aunque consideran que sus costes son elevados

La dificultad para captar talento y la alta especialización de los proveedores que prestan servicios de ciberseguridad ha propiciado que la externalización de servicios sea una estrategia clave para mantener un nivel razonablemente alto de madurez en ciberseguridad.

De hecho, **el 37% de los presupuestos[12] se dedica a servicios internos, mientras que el 63% a los externos.** Al mismo tiempo, la proporción existente entre la inversión y el gasto se mantiene indistintamente en proporción, sean servicios internos o externos: 34-35% para el CAPEX, y 65-66% para OPEX.
Si hacemos el análisis por sectores, destaca el hecho de que los más maduros en materia de ciberseguridad en España, como por ejemplo la Banca, Energía y Recursos, Seguros e incluso, aunque con algo menos de madurez, Fabricación y Consumo y Distribución, tienden a una mayor externalización que otros sectores con menor grado de madurez.

Gráfico 2.4: Comparativa de distribución de presupuestos



Ahondando en mayor detalle en la oferta de servicios de ciberseguridad disponibles en España, obtenemos que el 67% considera que la oferta es alta, lo cual corrobora que la oferta disponible de estos servicios en el mercado tiene un nivel razonablemente adecuado. Además, esta oferta es considerada muy necesaria. Solo el 11% de las empresas no lo ve así.

A pesar de ello, la práctica totalidad de las empresas considera que estos servicios tienen un coste elevado.

La mayoría de las predicciones en esta materia apuntan a una tendencia al alza de los precios.

Si bien los servicios más básicos de ciberseguridad pueden presentar, en determinados casos, un cierto descenso debido a una mayor oferta por parte de los proveedores, en la mayoría de los casos se espera que los precios aumenten por varios motivos:

- Es bien conocido que las políticas monetarias expansivas acometidas desde los bancos centrales, motivadas en gran parte por la reciente pandemia, están provocando una inflación que por el momento no se sabe si será transitoria o no.
- La escasez de talento formado y con experiencia en ciberseguridad es cada vez mayor, puesto que la demanda de estos perfiles se está incrementando y eso provoca que las presiones salariales al alza repercutan en un aumento de costes de los servicios.
- Finalmente, la demanda de servicios de ciberseguridad aumentará previsiblemente en mayor medida que la oferta, debido a la limitación del anterior punto entre otros. Esto provoca que, porcentualmente, haya cada vez menos proveedores que ofrezcan servicios percibidos como de calidad en el mercado en comparación con dicha demanda.

El salario de los CISO y responsables de ciberseguridad presenta un importante aumento frente a los años previos a la pandemia del COVID-19

Al mismo tiempo, se está observando un incremento en los salarios que perciben los CISO y responsables de ciberseguridad: la mayoría percibe más de 80.000 euros brutos fijos anuales.

Destaca el tramo de aquellos que perciben más de 120.000 euros brutos fijos anuales, el cual ha experimentado un aumento del 20%.

Este fenómeno se debe a la escasez de perfiles con experiencia de más de 5-8 años en puestos relevantes de ciberseguridad, la aparición por primera vez de este rol en los organigramas de las empresas menos maduras, y al hecho de que la figura del CISO empieza a ser percibida como clave y estratégica desde la dirección, motivado especialmente por el aumento de ataques con impactos críticos para el negocio del último año.

12. Cálculo realizado excluyendo el personal interno y dividiendo entre CAPEX y OPEX.

03 Modelo operativo y políticas

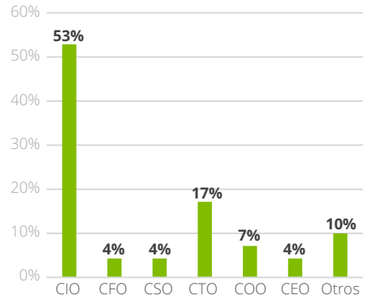
El modelo operativo en el área de ciberseguridad se ve condicionado por múltiples factores como, por ejemplo, el sector en el que opera la empresa o las responsabilidades que se le atribuyen a dicha área. No obstante, también puede verse afectado por la evolución del marco normativo, la transformación digital y el perfil de amenaza de la compañía, entre otros. El modelo operativo no solo es una cuestión interna del departamento de ciberseguridad, sino también externa, donde es clave entender cómo se relaciona la función de seguridad con el resto de las áreas de la organización, así como la dependencia jerárquica de la función de ciberseguridad.

En este sentido, la ubicación organizativa del CISO y su dependencia respecto a los miembros del comité de dirección varía y es diversa según cada organización.

Un 53% de los CISO depende jerárquicamente del CIO[13].

Además, este dato se ha incrementado en un 7% respecto a 2020, lo que contrasta con la tendencia identificada ese mismo año, en el que la dependencia del CISO respecto al CIO disminuía en un 14%, mientras que aumentaba respecto al CEO. Este aspecto puede darse seguramente como consecuencia de que el CIO está cobrando un papel de mayor importancia en el modelo organizativo de las empresas y ha entendido la importancia de la ciberseguridad en casi todas las decisiones clave que debe tomar.

Gráfico 3.1: Jerárquicamente, ¿De quién depende el CISO?



En cualquier caso, se debe prestar especial atención a la implementación de un modelo de este tipo, puesto que la ciberseguridad va más allá del aseguramiento de la tecnología. La ciberseguridad es una función que busca aportar valor al negocio a través de la reducción de los ciberriesgos que esta puede tener y, en muchas ocasiones, estos riesgos se derivan del comportamiento humano, la formación y los procedimientos que puedan exceder el mero alcance tecnológico. Por ello, es concebida como una buena práctica del sector que el CISO dependa del CEO.

Por otro lado, en línea con el estudio realizado el año anterior, los CISO siguen dependiendo en segunda instancia del CTO. Adicionalmente, se mantiene el crecimiento en relación con la dependencia del CISO respecto al COO, incrementándose en un 3% entre el año 2020 y el 2021, y acumulando un crecimiento total del 5% desde al año 2019.

Respecto a las compañías con un presupuesto de ciberseguridad superior a los 10M€, también se ha identificado que **el CISO tiende a depender en mayor medida del CIO y del CTO.**

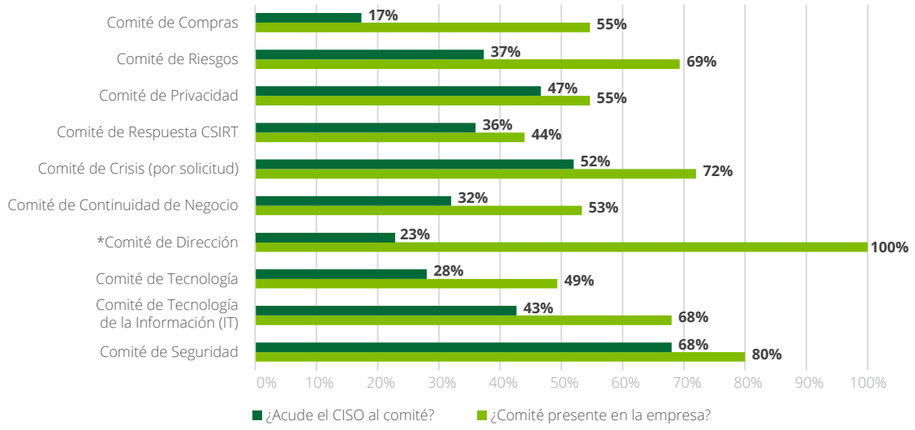
La colaboración entre el área de ciberseguridad y el resto de las áreas de una compañía es fundamental a la hora de fortalecer y securizar el negocio. En este sentido, el CISO, como principal responsable, debe ser el encargado de garantizar que la ciberseguridad se extiende a todo el negocio y que se tiene en cuenta en la toma de decisiones estratégicas. Una manera en la que podemos medir este aspecto es mediante la participación del CISO en los diversos comités establecidos en las organizaciones.

La participación del CISO en los diferentes comités establecidos en las compañías refleja una tendencia ascendente respecto a años anteriores.

13. Chief Information Office, por sus siglas en inglés; responsable de la función de información de la compañía.

Sin embargo, su nivel de involucración en algunos de los comités más comunes sigue siendo baja.

Gráfico 3.2: ¿Cuáles de estos comités de ciberseguridad están formalizados en su empresa?



*Se entiende que todas las empresas disponen de Comité de Dirección o un órgano similar

Adicionalmente, de la gráfica anterior podemos extraer otras conclusiones relevantes:

- **El Comité de Seguridad está presente en la gran mayoría de las empresas, aspecto que refleja la importancia que está cobrando la ciberseguridad en todos los sectores.**

- A pesar de que gran parte de las compañías ha constituido un comité para la gestión de los riesgos, el CISO únicamente está presente en un 37% de los mismos. Esto evidencia que, a pesar de que los CISO tienen mayor participación en dicho comité respecto al año anterior (4%), los ciberriesgos tienden a analizarse de forma paralela al resto de riesgos de negocio. Esto es un grave error, puesto que los ciberriesgos se encuentran entre los riesgos de mayor probabilidad[14] que pueden afectar al negocio de las compañías.

Aunque la participación del CISO ha aumentado este año en los diferentes comités donde la ciberseguridad puede ser una cuestión relevante que tratar, este dato sigue siendo aún demasiado bajo.

- La participación del CISO en el comité de privacidad también se ha visto incrementada (un 15% superior al año pasado), lo que destaca el alto nivel de involucración de este en la gestión de los aspectos relacionados con la protección de los datos personales, a pesar de que la responsabilidad de este ámbito normalmente recae bajo el DPO[15].

- **La participación del CISO en el Comité de Dirección ha aumentado en un 12% respecto al año anterior,** lo que refleja un mayor nivel de involucración con la Alta Dirección. **No obstante, la participación continúa siendo baja (23%),** a pesar de ser un comité que está presente en un 81% de las entidades.

14. Dato según The Global Risks Report 2021. 16th Edition del Word Economic Forum.
15. Data Chief Officer por sus siglas en inglés. Delegado de Protección de Datos en español

Actualmente, en base al estudio realizado, se ha identificado que el CISO asume la responsabilidad de una gran variedad de ámbitos en relación con la ciberseguridad.

Como era de esperar, **el ámbito más común bajo la responsabilidad del CISO es el gobierno de la ciberseguridad:** prácticamente la totalidad (99%) de las empresas que han participado así lo afirma.

El CISO, además de preocuparse por establecer una adecuada gestión de la ciberseguridad, y como se reflejó en años anteriores, es responsable de la primera línea de defensa[16], ya que se encarga de las operaciones de seguridad en un 78% de los casos, un 18% más que el año anterior.

Adicionalmente, **las políticas y el cumplimiento también destacan entre las principales responsabilidades del CISO, siendo este último una de las grandes palancas a la hora de incrementar el presupuesto destinado a la ciberseguridad,** ya que el panorama regulatorio con impacto en la seguridad de las compañías se encuentra en constante evolución y desarrollo (EIOPA, DORA, NIS 2, etc.).

Casi la mitad de los CISOs son responsables de continuidad de negocio

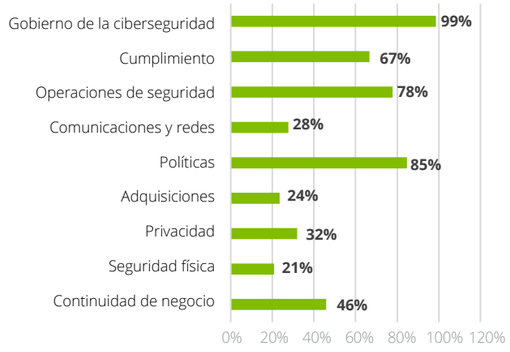
En este contexto, las empresas se ven forzadas a potenciar sus medidas de seguridad para evitar posibles incumplimientos normativos, los cuales quedan evidenciados típicamente tras un ciberincidente o una auditoría.

Además, el incumplimiento normativo es uno de los aspectos que se encuentra en el top 5 de posibles efectos de un ciberataque que más preocupan a las empresas, en este caso, del sector asegurador, tal y como afirma el estudio *II Termómetro de la ciberseguridad en el sector asegurador español,* llevado a cabo por ICEA en colaboración con Deloitte.

Este dato, aunque depende en gran medida de cada organización, tiene bastante coherencia en términos generales si tenemos en consideración que el CISO se preocupa de los riesgos del negocio, al igual que los BCP[17]. De hecho, en la actualidad y, al menos en España, una de las principales causas de interrupción del negocio viene derivada de un ciberataque, típicamente de *ransomware* u otros malwares o ataques de DDoS[18].

Finalmente, cabe resaltar respecto a la función de privacidad que el 91% de los CMO[19] afirmó[20] que sus organizaciones equilibran la recopilación de datos con la generación de confianza de sus clientes, lo cual nos lleva a ver el grado de concienciación de las compañías con el uso de datos de sus clientes más allá de exigencias regulatorias. En España, solo el 32% de las organizaciones atribuye esta responsabilidad a la figura del CISO.

Gráfico 3.3: ¿Qué áreas o ámbitos de responsabilidad dependen del CISO?

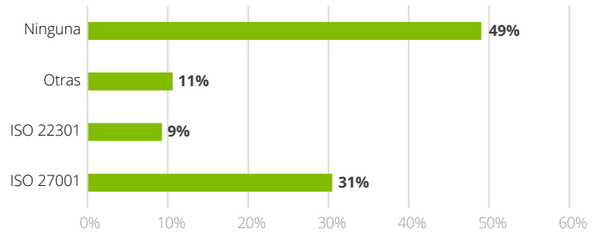


16. Tradicionalmente se ha situado al CISO en la segunda línea de defensa o en la línea "1,5", entre la primera y la segunda línea.
17. Business Continuity plan por sus siglas en inglés. Planes de continuidad de negocio en español.
18. Distributed denial of service por sus siglas en inglés. Ataque de denegación de servicio a través del cual, varios sistemas infectados (botnet) se lanzan de manera coordinada peticiones a un servidor para que este se "sature" y deje de operar.
19. Chief Marketing Officer por sus siglas en inglés. Reponsable de las campañas de marketing y, por tanto, de la recopilación de datos de usuarios.
20. Dato obtenido del Deloitte Future of Cyber 2021 a empresas de todo el mundo.

04 Certificaciones, *frameworks* y formación

En relación con las certificaciones de ciberseguridad, las empresas se decantan en primera instancia por la ISO 27001, como ya se identificó en años anteriores, la cual establece las directrices para la implementación de un Sistema de Gestión de Seguridad de la Información. Adicionalmente, a lo largo del último año se ha identificado un incremento del 1% en el número de empresas que disponen de esta certificación, pasando de un 30% a un 31% en 2021.

Gráfico 4.1: ¿Qué certificaciones relacionadas con la ciberseguridad posee la empresa



Por otro lado, cabe destacar que la certificación ISO 22301 es la segunda más común entre las empresas analizadas.

Sin embargo, se puede observar que existe una gran diferencia entre ambas. **Se ha producido una reducción del 11% en el número de empresas que no disponen de ninguna certificación en ciberseguridad,** lo que refleja que cada año las compañías menos maduras en ciberseguridad están más concienciadas ante el posible impacto en el negocio que puede provocar un ciberataque.

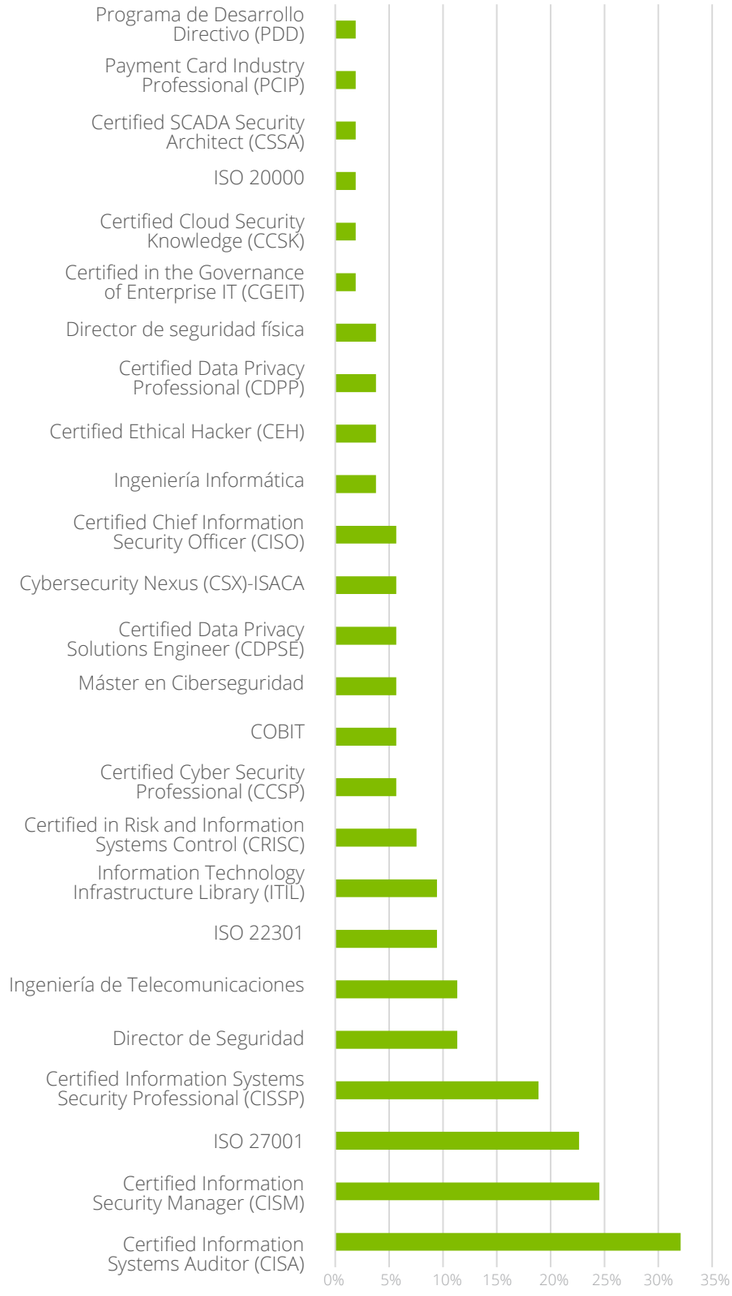
No obstante, aunque la tendencia es positiva, **el hecho de que un 49% de las compañías no dispongan de ninguna certificación en ciberseguridad continúa siendo una cifra inquietante,** por lo que aún existe un gran margen de mejora al respecto.

Cada vez son menos las empresas que no disponen de ninguna certificación de ciberseguridad, a pesar de que este dato sigue siendo negativo con casi un 50% de empresas sin certificar

Adicionalmente, se ha identificado que existe una correlación muy clara entre el hecho de disponer de certificaciones de ciberseguridad y el sufrir menos incidentes, ya que estas certificaciones ayudan a robustecer las medidas de seguridad y a aumentar el nivel de madurez de ciberseguridad de las compañías; aunque no son ninguna garantía ante ciberataques. En relación con las certificaciones y formación, se ha detectado que **un 77% de los CISO que han participado en el análisis posee, al menos, una certificación en materia de Seguridad de la Información.** En comparación con el año pasado, esto supone un incremento del 7%, lo que refleja que actualmente los CISO tienden a interesarse por potenciar y respaldar mediante certificaciones los conocimientos de ciberseguridad adquiridos a lo largo de su experiencia.

El 69% de los ciberincidentes son sufridos por aquellas empresas que no disponen de ninguna certificación en materia de ciberseguridad.

Gráfico 4.2: ¿Qué certificaciones/formación posee el CISO de la empresa?



Por otro lado, tal y como se puede apreciar en el gráfico, cabe destacar que existe una amplia variedad de certificaciones de seguridad en el mercado. Sin embargo, como se identificó el año pasado, **las dos certificaciones más comunes entre los CISO son las siguientes: CISA y CISM, ambas respaldadas por ISACA, y enfocadas en la auditoría y la gestión, respectivamente.** Sin embargo, en el análisis realizado este año predomina la presencia de la certificación CISA, a diferencia del año anterior.

Los CISO y responsables de ciberseguridad son perfiles que cuentan normalmente con muchos años de experiencia y, por tanto, tiene sentido que predomine CISA y CISM entre las certificaciones más habituales, no solo por su evidente utilidad, sino porque estas cuentan con una larga historia en el panorama formativo.

CISA, CISM, la ISO 27001 y CISSP siguen siendo las certificaciones más demandadas por los CISO

Adicionalmente, cabe destacar los siguientes aspectos:

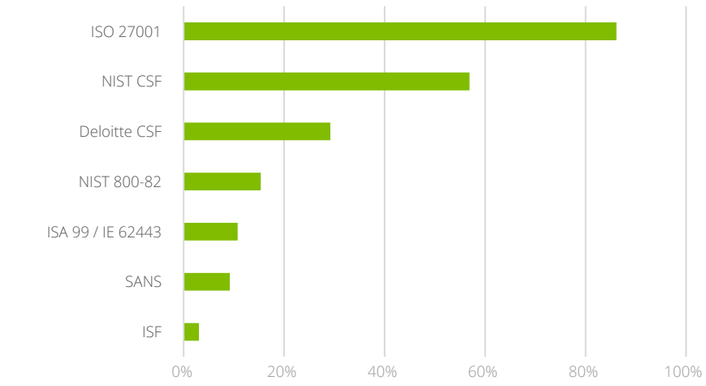
- **Las certificaciones en ISO 22031 han aumentado desde un 4% hasta un 9%,** lo que refleja la importancia que está adquiriendo la continuidad del negocio entre los CISO de las compañías españolas, especialmente desde los ataques de ransomware presenciados en la industria este pasado año.
- También **se ha identificado un aumento considerable en la concienciación respecto a los ciber riesgos,** ya que la demanda de la certificación CRISC ha pasado de un 4% a un 8%. Este dato es realmente positivo, puesto que los CISO están siendo conscientes de la necesidad de definir una estrategia que tenga en consideración la priorización de los riesgos que afectan al negocio a través de una metodología sólida de medición de riesgos.

Como se ha reflejado previamente a lo largo del estudio, la certificación ISO 27001 es la más común entre las empresas analizadas. Adicionalmente, también se ha identificado que dicho estándar es el más utilizado por las compañías como marco de referencia para la mejora de sus procesos. En particular, un 86% de las empresas utiliza el estándar ISO 27001, lo que supone un incremento del 11% respecto a los resultados obtenidos en el año 2020, por lo que vemos que sigue siendo la principal tendencia en el mercado, sobre todo en el caso de las empresas menos maduras y que empiezan a hacer uso de frameworks de referencia.

A continuación, **el segundo marco de referencia más utilizado es el NIST CSF, con un incremento del 12% respecto al año pasado y seguido del Deloitte CSF,**

El CSF[21] de Deloitte se consolida como unos de los 3 principales *frameworks*[22] más utilizados en el mercado, con casi un tercio del mismo; y la NIST es la opción que más fuerza coge con un crecimiento del 12%, mientras que la ISO 27001 sigue siendo la más utilizada con un 86% de uso.

Gráfico 4.3: ¿Qué framework(s) se usa(n) como referencia para la mejora de los procesos de ciberseguridad?



definido en línea con los principales estándares del mercado (ISO, NIST, SANS, etc.), que sigue incrementándose año tras año, y que ya se ha posicionado como uno de los estándares de referencia en el sector con una adopción del 29% entre las más de 100 empresas analizadas.

Adicionalmente, tal y como se puede apreciar en el gráfico, los siguientes *frameworks* más utilizados son el NIST 800-82 y otros como el ISA 99/IE 62443, orientados a la securización y resiliencia de los sistemas de control industrial. La baja adopción de estos estándares refleja que existe un gap importante entre el nivel de madurez de ciberseguridad del entorno IT y el entorno OT, caracterizado por un alto nivel de obsolescencia, y que debe ser reforzado con el objetivo de aumentar la seguridad en el desarrollo de la industria 4.0.

21. Marco de referencia (i.e: ISO 27.000, NIST, Deloitte CSF...)
22. Framework Deloitte Cyber Strategy Framework que aúna las mejores prácticas y los controles de los principales marcos del mercado.

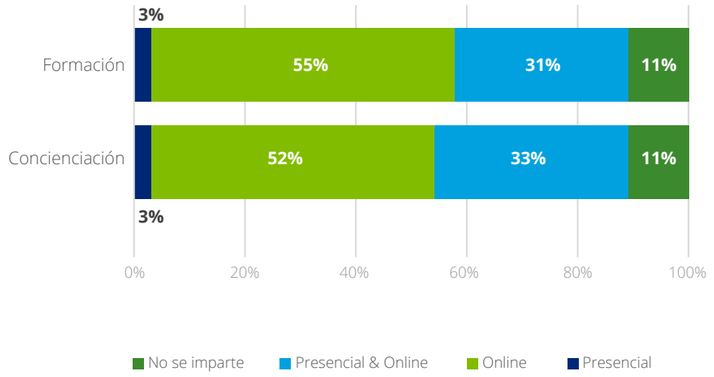
El phishing se ha convertido en el vector de entrada por excelencia de los atacantes. Es el método más económico y efectivo para penetrar en la seguridad de una empresa. Este hecho ha generado que las nuevas campañas de phishing sean más sofisticadas y bien dirigidas. Además, estas se combinan con la información pública a través de LinkedIn, otras redes sociales e Internet en general. Incluso, se aprecia un aumento muy significativo de las campañas de vishing[23] para recabar más información o directamente asegurarse que la víctima abrirá el posterior email que recibirá.

Sin lugar a duda, nuestros empleados (internos y externos) siguen siendo el eslabón más débil de la empresa y es necesario empezar a transformar a las personas en "cortafuegos humanos". Para ello, la concienciación y la formación son imprescindibles.

Las compañías siguen sin diferenciar entre la formación y concienciación en ciberseguridad

Los CISO no tienen clara la diferencia entre ambas modalidades y eso hace que las acciones realizadas se confundan sin una estrategia clara que aborde los principales ciberriesgos humanos de las compañías.

Gráfica 4.4: ¿Cuántas horas anuales se imparten de formación de ciberseguridad a todo el personal?



En este sentido, y en línea con lo que se identificó el año anterior, en el gráfico se observa cómo **las compañías siguen decantándose por la modalidad de formación y concienciación totalmente online**, tendencia continuista iniciada a raíz de la pandemia del Covid-19 y que se mantiene por sus bondades: se evita los desplazamientos para asistir de forma física a las oficinas y hace que el proceso de formación y concienciación sea más fácil y ágil. **Más de la mitad de las compañías se decanta por la modalidad online, mientras que la segunda modalidad preferida por las empresas es la mixta, alternando la formación y concienciación online con eventos presenciales.**

Este dato refleja la gran importancia que tiene la formación y concienciación de los empleados en materia de ciberseguridad a la hora de evitar potenciales ciberataques. **Si tenemos en cuenta que por lo general las iniciativas de concienciación y formación suelen requerir de poca inversión frente a la gran efectividad que presentan, hace que el aumento del nivel de madurez en ciberseguridad de los empleados y, por ende, su nivel de ciberconciencia deba priorizarse en los planes directores de ciberseguridad anualmente.**

A nivel general, otro aspecto a destacar es que se ha identificado que existe un mayor número de empresas que están llevando a cabo planes de formación y concienciación. En total, **el número de empresas que no forman ni concienciar a sus empleados en materia de ciberseguridad se ha reducido en un 14%.** No obstante, aún existe un gran margen de mejora, puesto que **un 11% de las compañías sigue sin formar ni concienciar a sus empleados, lo que supone un alto riesgo.**

Las empresas que imparten más de 20 horas anuales de formación y concienciación a sus empleados han recibido únicamente el 15% de los incidentes sufridos en el último año

23. Suplantación de identidad a través de llamadas por teléfono para obtener más información y/o perpetrar una estafa.

05 Revisiones de seguridad

Es de vital importancia, indistintamente del sector, conocer cuáles son las aplicaciones críticas con las que se cuenta dentro de la empresa y las que de manera directa o indirecta son clave para el funcionamiento de este.

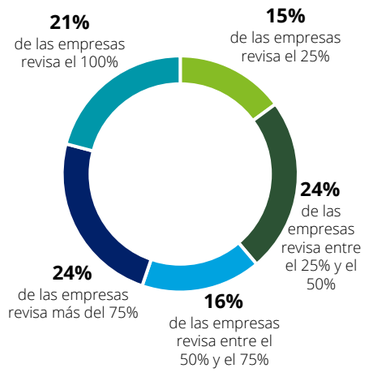
Pero no basta solo con tenerlas inventariadas, sino que resulta casi igual de crítico saber el estado en el que se encuentran y revisar si presentan algún tipo de vulnerabilidad o pueden llegar a presentar un rendimiento por debajo de los umbrales establecidos.

En este sentido, se observa que **el 66% de las empresas revisa al menos la mitad del total de sus aplicaciones críticas. Este dato no es especialmente bueno, puesto que supone que un tercio de las compañías no revisa ni siquiera la mitad de sus aplicaciones críticas. Por otro lado, solo solo el 21% revisa anualmente la totalidad de estas.**

A pesar de que estos datos no son positivos, es cierto que se aprecia un aumento del 7% las empresas que, como mínimo, revisa la mitad de sus aplicaciones críticas. Al mismo tiempo, ha disminuido el número de empresas que no revisa ni una cuarta parte de las aplicaciones; más concretamente, el 15% no hace revisiones del 25% de sus aplicaciones.

En definitiva, seguimos aún en cotas muy bajas de revisión de aplicaciones críticas, pero con una tendencia claramente positiva.

Gráfico 5.1 ¿Que porcentaje de las aplicaciones consideradas imprescindibles/críticas son revisadas?



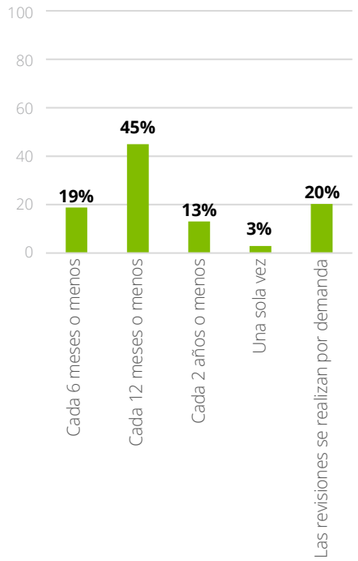
La distribución sectorial de este indicador muestra cómo el sector de la Banca es el que revisa en mayor número y en profundidad sus aplicaciones más críticas, al igual que el de Seguros. En el otro extremo se encuentra el sector de Consumo y Distribución, el cual se encuentra más rezagados.

Dentro de los organismos internacionales de ciberseguridad, se recomienda como buenas prácticas una revisión mínima anual de todas las aplicaciones consideradas críticas, o tras cambios significativos de estas. En este sentido, casi el 64% de las empresas sigue dichas recomendaciones:

El sector de la Banca y el asegurador son los dos más concienciados en la importancia de revisar las aplicaciones críticas del negocio

Es preocupante que el 20% de las empresas participantes sólo realice revisiones de sus aplicaciones críticas bajo demanda y el 3% tras el despliegue inicial de ésta. Es relevante volver a resaltar que, en comparación a los datos proporcionados en 2020, se va produciendo una disminución de las empresas que se despreocupan de la revisión de sus aplicaciones, lo cual al menos refleja una tendencia positiva.

Gráfico 5.2 Periodicidad con la que se revisan las aplicaciones críticas



06 Entornos Cloud y tendencias tecnológicas

Casi la totalidad de los sectores está migrando a la nube, si no lo han hecho ya. Además, el uso intensivo de la infraestructura y plataformas de terceros no solo se hace para aplicaciones asiladas, sino que hoy en día, las empresas confían en la nube para alojar sus aplicativos más críticos o *core* del negocio.

Según los datos obtenidos en el estudio *Future of Cyber* de Deloitte, *"el 94% de los CFO que participaron indicó que está valorando la idea de migrar sus ERP[24] a entornos Cloud"*.

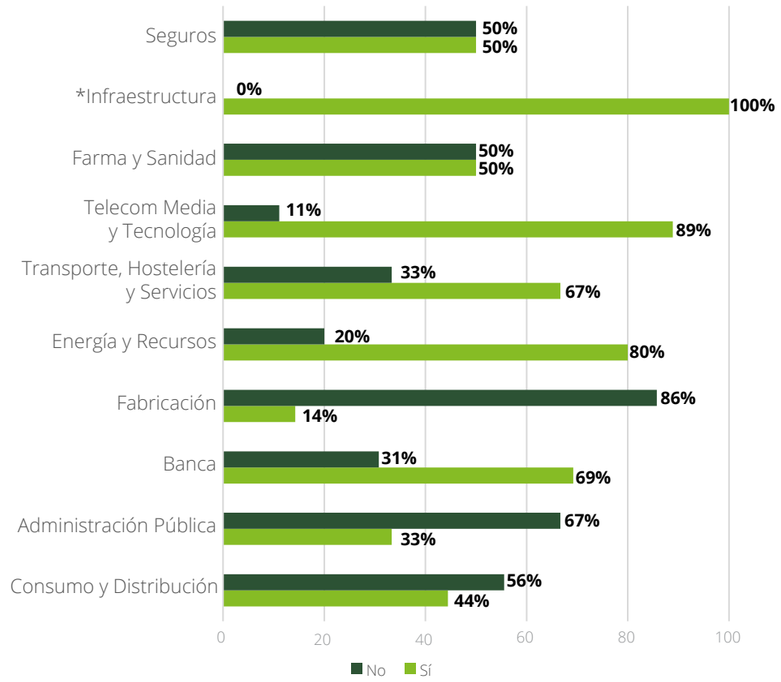
El 19% de las empresas participantes que cuenta con servicios Cloud no dispone de una mínima estrategia definida.

El año pasado el dato era de un 4%, apreciándose un aumento muy negativo de empresas que no disponen de una estrategia para sus servicios Cloud. No obstante, este dato no se debe a empresas que hayan dejado de tener una estrategia definida, sino a empresas que debido a la pandemia se han visto forzadas a buscar soluciones más escalables, de fácil acceso y alta disponibilidad para así poder trabajar a distancia, es decir, la nube. Esta transición se ha hecho de manera abrupta y, en la mayoría de los casos, sin poder planificar con tiempo una estrategia de ciberseguridad. En cualquier caso, muchas de estas empresas sí se encuentran inmersas en esta definición o lo harán en el corto plazo.

Dado que sigue aumentando el uso de servicios Cloud, muchas empresas van más allá de la definición de una simple estrategia y dan el paso a la creación de un marco de controles específicos de seguridad para la nube y así asegurar la protección de dichos servicios. **De las empresas participantes que cuentan con una estrategia de seguridad Cloud, el 71% cuenta también con un marco de controles específicos para la nube, lo cual es un dato positivo.**

A nivel sectorial, solo el sector de Infraestructuras cuenta con un 100% de empresas que tienen para su infraestructura de seguridad Cloud un marco de controles específicos. La gran mayoría de sectores cuenta con, al menos, un 50% de empresas con un marco de control específico. Sectores como la Fabricación, la Administración Pública o el Consumo y Distribución no llegan a ese 50% en implantación de marcos de control específicos para Cloud.

Gráfico 6.1: Sectores que cuentan con un marco de control Cloud



*Se debe tener en cuenta que Infraestructuras es un sector que representa solo el 4% del total de la muestra, además de que dichas empresas son de un tamaño razonablemente grande. Por todo ello, puede llegar a malinterpretarse que Infraestructuras es el sector más avanzado respecto a los marcos de control específicos para Cloud. La cual sería una conclusión errónea.

24. Enterprise resource planning por sus siglas en inglés. Sistemas financieros o de planificación de recursos empresariales.

Por otro lado, año a año los dispositivos IoT[25] están cobrando más presencia dentro del parque tecnológico de las empresas españolas, aunque no en todos los sectores está teniendo el mismo impacto. Aun así, sorprende el total de empresas que cuentan con estos dispositivos. **El 75% de las empresas consultadas cuentan con dispositivos IoT en el desarrollo de su negocio.**

Al haber cada vez más empresas que se inclinan por hacerse con dispositivos IoT, también son más las que son conscientes de la necesidad de su securización. Es por ello que **el 67% de las empresas que cuenta con dispositivos IoT, contemplan a su vez estos en su estrategia de ciberseguridad para protegerlos. Es de destacar la comparativa con este mismo dato en el año anterior, donde solo se contaba con un 56% de empresas que contemplaba los dispositivos IoT en su estrategia; dato positivo que evidencia una clara evolución.**

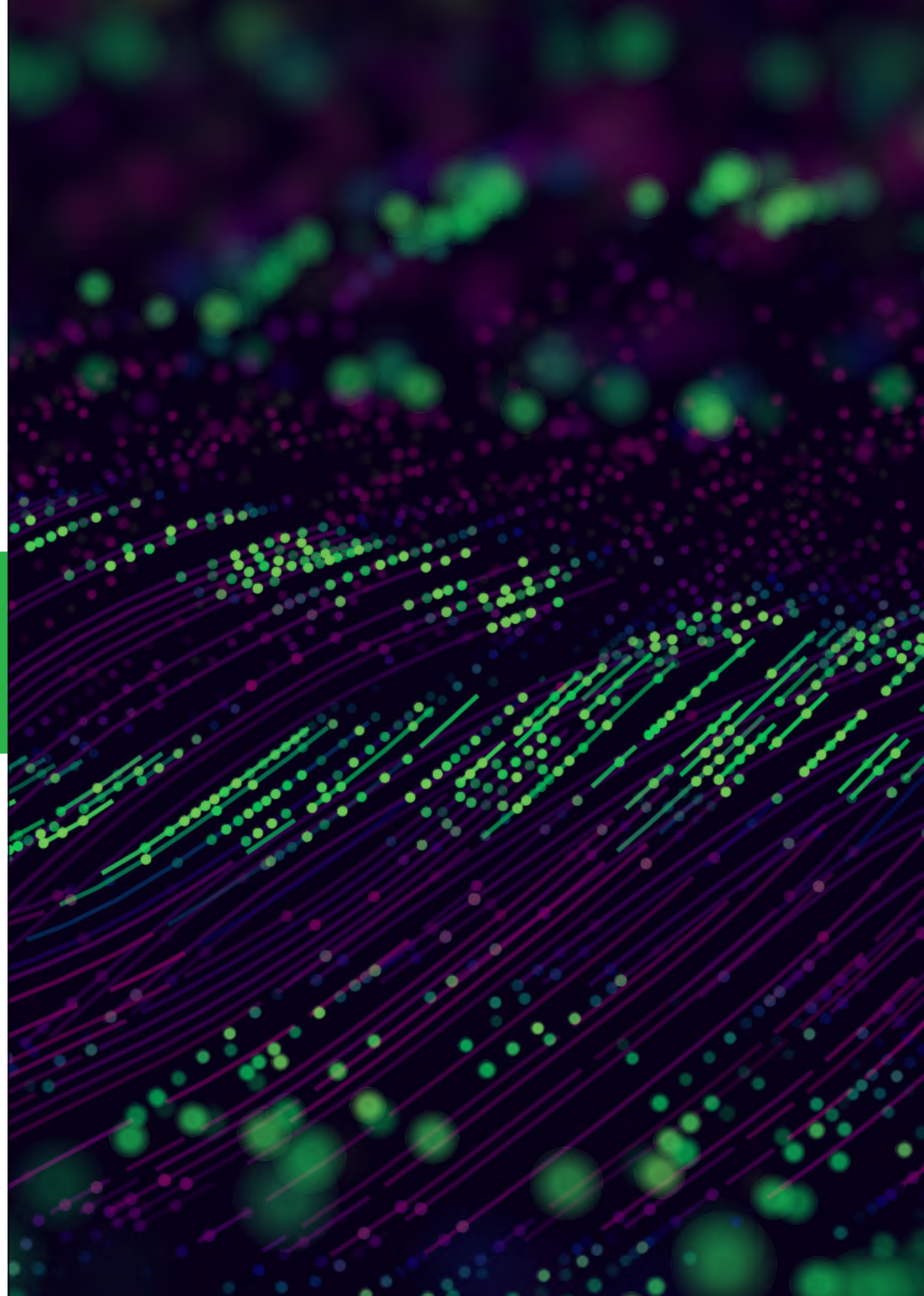
En este contexto, cabe resaltar cuáles son las iniciativas que están priorizando las compañías en su transformación digital a nivel internacional (datos extraídos de *Future of Cyber* de Deloitte):

1. Análisis de datos
2. Cloud
3. Cloud ERP
4. Inteligencia Artificial y computación cognitiva
5. OT[26] / ICS[27]
6. IoT
7. Blockchain y criptomonedas

Todas estas iniciativas, no solo presentan retos desde la perspectiva transformacional de las compañías, sino que también son retos para el área de ciberseguridad. Esta área debe adaptarse a estas nuevas disrupciones y para las cuales los controles tradicionales o bien no sirven o bien dichos controles deben ser modificados para poder cubrir estos nuevos activos.

El 71% de las empresas que dispone de una estrategia Cloud, también cuenta con un marco de controles específicos para la nube

25. Internet of Things por sus siglas en inglés. El Internet de las cosas.
26. Operational Technologies por sus siglas en inglés. Tecnologías industriales de operaciones.
27. Industrial Control Systems por sus siglas en inglés. Tecnologías para la securización de los entornos industriales.



07 Incidentes de seguridad

Los incidentes de ciberseguridad son un indicador clave de gran interés para los CISO y responsables de ciberseguridad. El número de incidentes sufridos puede ser un reflejo sobre el nivel de madurez de las organizaciones y cómo están respondiendo las iniciativas que ponen en marcha, motivo por el cual cobra especial relevancia en este estudio.

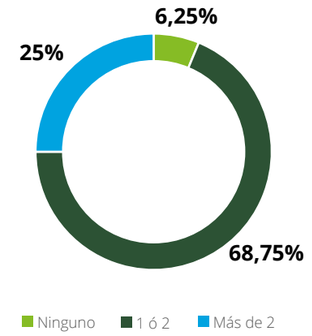
Adicionalmente, este indicador ha sido uno de los indicadores que con mayor frecuencia se ha correlacionado con otros para inducir nueva información.

En este último año se ha experimentado un más que notable aumento del número de ciberataques y sofisticación de las amenazas conocidas. Que estos ciberataques posteriormente pasen o no a ser ciberincidentes con impactos relevantes para la compañía depende en gran medida de la robustez de las medidas de ciberseguridad de cada organización ha implantado. Nótese la diferencia entre ciberataque y ciberincidente.

El 94% de las empresas ha sufrido al menos un incidente grave de ciberseguridad a lo largo de 2021

En este sentido, casi el 69% de las empresas afirma que ha sufrido entre 1 y 2 ciberincidentes de gravedad durante este último año, agravándose la situación para el 25% de las empresas que afirma haber sufrido más de 2 ciberataques durante 2021.

Gráfico 7.1: ¿Cuántos incidentes críticos de ciberseguridad se han producido en su empresa en el último año?

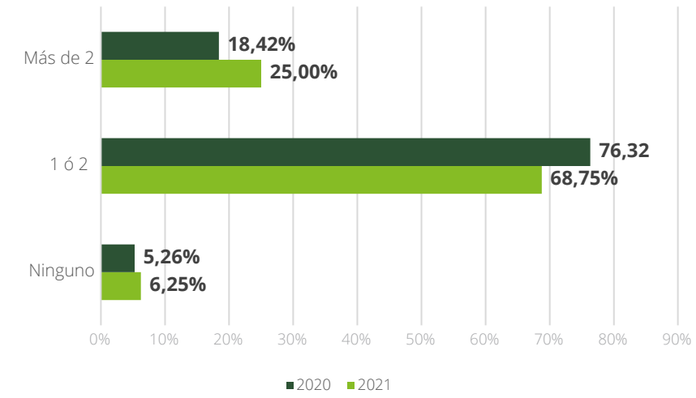


Además, según la comparativa del año 2020 con respecto a este último año, se observa cómo el número de empresas que ha recibido 1 o 2 ataques se ha reducido. En cambio, las empresas que han sufrido al menos 1 ciberincidente han aumentado casi un 7%. Es un dato significativo y que tiene su explicación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

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

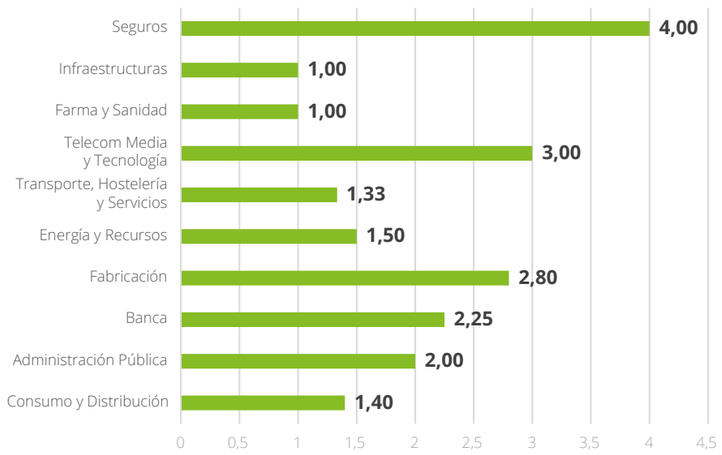
Este año se ha experimentado un 26% más de ciberincidentes con impactos significativos respecto al año pasado

Gráfico 7.2: Evolución de los incidentes entre 2020 y 2021

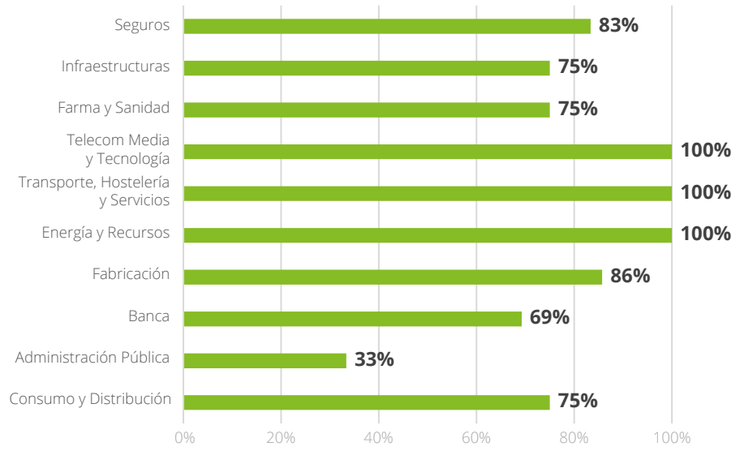


Si desgranamos este dato por sectores, podemos apreciar cómo varios de estos se encuentran por encima de los dos incidentes de media al año. Entre dichos sectores, encontramos el de Seguros, Telecomunicaciones, Media y Tecnología, Fabricación, Banca y Administración Pública.
Cabe destacar que ciertos sectores como el de la Banca y Seguros se encuentran fuertemente regulados y cuentan con nivel de madurez en ciberseguridad razonablemente elevado, motivo por el cual el número de incidentes que sufren se debe más a que son un objetivo prioritario para los cibercriminales, más que al hecho de una falta de ciberresiliencia por su parte.

Gráfica 7.3: Media de incidentes por sector



Gráfica 7.4: Porcentaje de ciberseguros contratados según sector



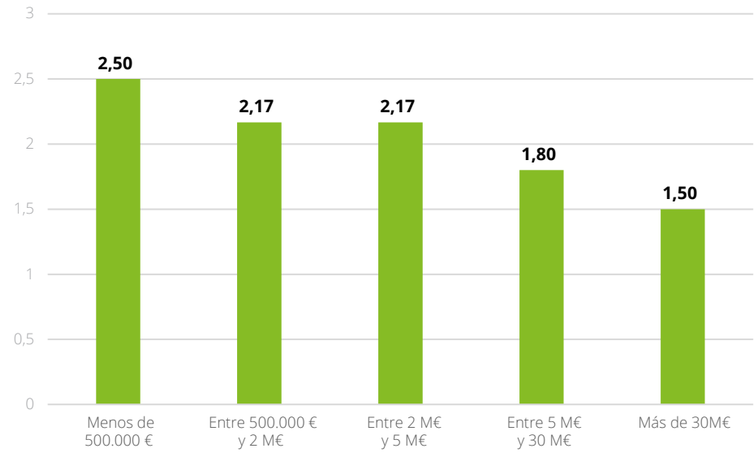
Los ciberseguros guardan una estrecha relación con los ciberincidentes sufridos: a mayor número de ciberincidentes, mayor es la contratación de estos seguros por parte de las empresas.

Podemos corroborar la anterior afirmación atendiendo al dato sectorial que refleja cómo uno de los sectores que más ciberseguros contrata es el de Telecomunicaciones, Media y Tecnología, es a su vez uno de los que más ataques sufre a lo largo del año.

Otros de los sectores que más invierten en ciberseguros son Transporte, Hostelería y Servicios y Banca, debido al mismo motivo por el que invierte el sector tecnólogico.

Si comparamos el número de incidentes con el presupuesto dedicado a ciberseguridad, se observa una clara relación entre la media de incidentes que sufren las empresas, con el presupuesto que se dedica a ciberseguridad. Por lo general, las empresas con más facturación son las que más invierten en sus departamentos de ciberseguridad. También suelen ser las más atacadas debido a su mayor superficie de ataque y mayor impacto potencial que puede provocar el atacante. A pesar de ello, se puede comprobar la eficacia de esos presupuestos más holgados en ciberseguridad, puesto que se aprecia su retorno en términos de menos ciberincidentes sufridos.

Gráfica 7.5: Media de incidentes según el presupuesto en ciberseguridad



Las conclusiones de este estudio están en sintonía con los diferentes informes que se han publicado por distintos organismos internacionales, como por ejemplo ENISA: **las máximas preocupaciones que aparecen en estos momentos a nivel general son el malware, el phishing y el ransomware.**

Estas amenazas son las que más preocupaciones generan en las empresas consultadas, independientemente del sector al que pertenecen. Cada vez son más los ataques de ransomware que sufren las empresas y la sofisticación de estos como, por ejemplo, el ransomware de triple extorsión (se aprovecha el acceso a cada máquina infectada para coordinar ataques DDoS cuyos botnes son dispositivos de la compañía, además de realizarse en paralelo una fuga información sensible).

El caso del phishing también es bastante preocupante, puesto que cada vez se opta más por lanzar campañas más personalizadas y difíciles de detectar por los usuarios. Por este motivo, el entrenamiento de los empleados en la identificación y reporte del phishing es crucial.

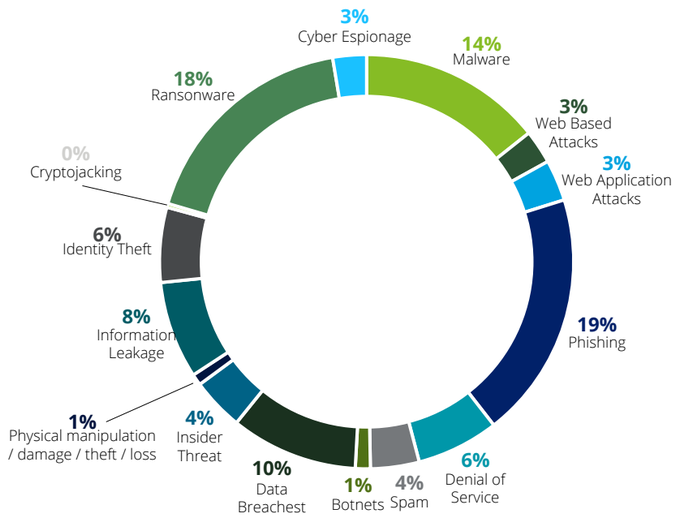
Como se puede apreciar, muchas de las amenazas pueden combinarse en un mismo ataque, donde destaca el phishing, que es el vector de entrada por el que se decantan mayoritariamente los atacantes.

El ransomware, el phishing y el malware en general, entre las principales preocupaciones de los CISO

En el estudio *Future of Cyber* de Deloitte se llega a la conclusión de que las empresas están empezando a buscar un equilibrio correcto entre la recopilación de los datos de clientes (para ayudar al negocio) y que estos sean los mínimos necesarios (para contentar a los usuarios y disponer de menos información sensible a ser fugada de la compañía). En este sentido, el 91% de los CMOs considera que sí se está llegando a dicho equilibrio.

Finalmente, en este mismo estudio se llega a la conclusión de que las compañías consideran que es clave compartir información de los ataques sufridos y que esta información evita que se pueda comprometer al sector, aseverando al mismo tiempo que el daño reputacional en estos casos es mínimo y la transparencia genera más beneficios que perjuicios.

Gráfica 7.6: Porcentaje de amenazas más habituales



08 Simulaciones de crisis y ciberincidentes

Las simulaciones de cibercrisis o ciberincidentes se han convertido en una herramienta imprescindible para preparar a los equipos de respuesta ante un evento disruptivo real.

Los enfoques proactivos de gobierno de la ciberseguridad actuales, frente a los reactivos del pasado, fuerzan a que todos los equipos (alta dirección, equipos tácticos y equipos operativos/técnicos) gestionen de forma recurrente en un entorno controlado aquellos escenarios de ciberataques que presentan mayor riesgo para la compañía. En algunos casos, como es en el sector de financiero, estas empresas no solo se ven obligadas a realizar dichos ciberejercicios por buenas prácticas sectoriales, sino que se ven obligadas por la propia regulación de la industria.

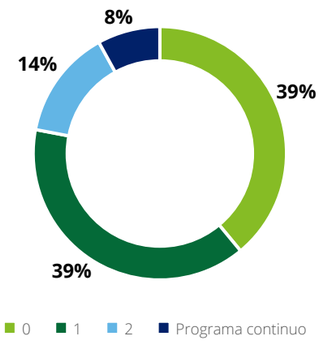
Más del 60 % de las compañías realiza como mínimo 1 ejercicio de simulación de cibercrisis o ciberincidente al año

Por ello, y debido a la importancia de los incidentes en las estrategias de ciberseguridad de las compañías, este año se ha decidido en este estudio ahondar un poco más en la fase previa de prueba y entrenamiento ante ciberincidentes.
Se ha experimentado una creciente demanda de simulaciones de crisis y ciberincidentes debido a la satisfacción de quienes se someten a estas actividades.

Solo el 40% de las organizaciones no contempla la realización de este tipo de simulaciones, al contrario que el 60% restante; lo cual es un dato positivo y que muestra una clara tendencia alcista. No obstante, tan solo un 7% del total enmarca la ejecución de estas simulaciones en un programa continuo, y no como actividades puntuales. Se trata de un dato aun negativo, puesto que las buenas prácticas apuntan a que estos ciberejercicios deben realizarse de forma periódica.

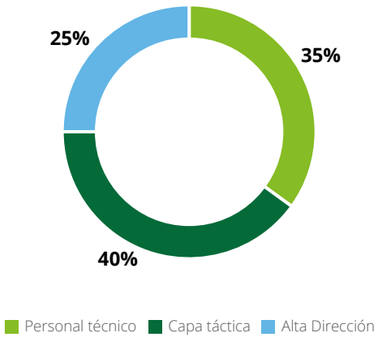
Cierto es que tanto los equipos técnicos/operativos como los tácticos son las primeras líneas de defensa para contener un ciberincidente. No obstante, una vez que estos pasan de la categoría de incidentes a crisis, la implicación de la alta dirección es imprescindible. Por este motivo, a pesar de que puedan llegar a pesar más las simulaciones de los equipos tácticos y operativos/técnicos respecto a las de la alta dirección, la diferencia actualmente es demasiado elevada.

Gráfico 8.1: ¿Cuántas simulaciones ha podido realizar en el último año de una cibercrisis?



Solo en el 25% de los casos predominan las simulaciones de cibercrisis dirigidas a la alta dirección, frente a los casos en los que destacan más las simulaciones a los equipos tácticos y operativos

Gráfico 8.2: ¿Cuál es el prinicpal tipo de simulaciones de cibercrisis que se realizan en su empresa?



09 Percepción del CISO

El 86% de las compañías considera que se encuentran “adecuadamente preparadas” para hacer frente a los ciberincidentes

Esta sensación de ciberresiliencia se ha visto notablemente incrementada respecto al pasado estudio, donde apenas la mitad de las compañías (el 52%) se consideraban “preparadas” para hacer frente a los incidentes de seguridad.
Este incremento se debe a la combinación de mayor inversión en ciberseguridad, más entrenamiento de los equipos de respuesta ante incidentes y crisis (incluidos la alta dirección), así como a la propia experiencia adquirida tras haber sufrido incidentes reales de seguridad en el pasado año.
En el análisis sectorial realizado sobre esta cuestión destaca el caso de la Banca, **la cual se erige como el sector con mayor preparación ante incidentes (el 100% de las empresas) según sus máximos responsables de seguridad**. No obstante, este sector y el resto presentan una tendencia al alza respecto a esta sensación de resiliencia.

Es lógico que el *ransomware* u otros ciberataques que paralizan el negocio sean la mayor preocupación: no solo suponen un impacto directo en el negocio y la misión que desempeña la compañía, sino que el pasado año se han vivido numerosos ataques de este tipo en España, especialmente en el sector salud y el asegurador, cuyas consecuencias han sido bien conocidas por toda la industria.

Gráfico 9.2: Riesgos que generan mayor preocupación en las organizaciones

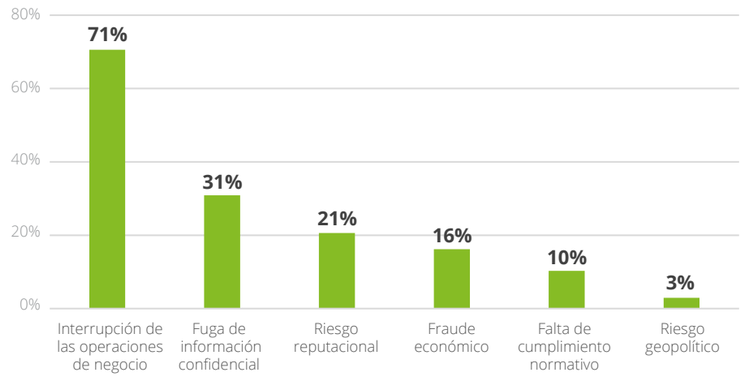
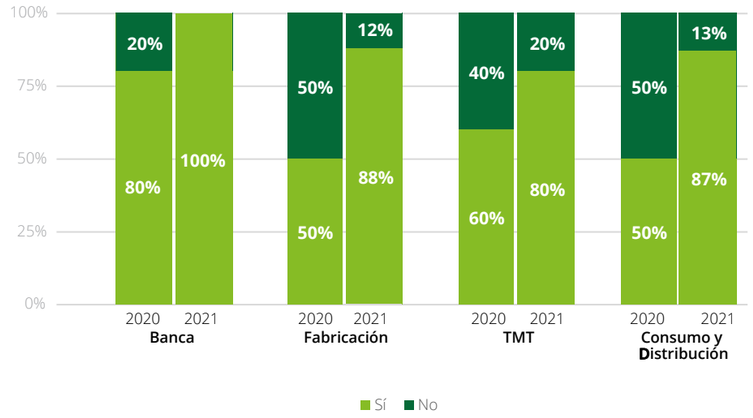


Gráfico 9.1: ¿Se encuentra su compañía preparada para hacer frente a los incidentes de ciberseguridad?



Los CISO lo tienen claro: el 71% considera que la interrupción de las operaciones de negocio se alza un año más como el riesgo que más preocupa en sus compañías

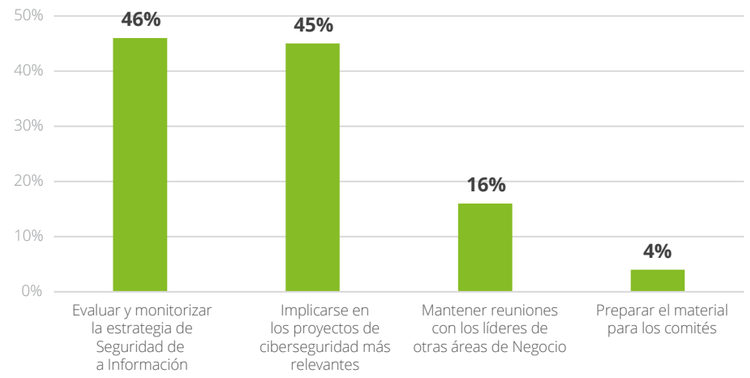
Varias compañías han experimentado cómo **la recuperación ante un ciberataque sofisticado de ransomware puede suponer varias semanas e incluso meses,** lo cual deriva en un dilema para la operación diaria de la compañía que casi siempre suele exceder lo planificado previamente. Eso sin contar las pérdidas económicas, que suelen rondar los 1,8 millones de euros según otros estudios[28].

Las tareas que los CISO consideran más relevantes por encima del resto son la evaluación y monitorización de la estrategia de la seguridad de la información, siguiéndole muy de cerca y con un gran incremento respecto al pasado estudio, la implicación en los proyectos de ciberseguridad más relevantes como respuesta a los múltiples proyectos sobrevenidos que se han acometido, en ocasiones concurrentemente, para dar respuesta de manera segura a las nuevas formas de trabajo.

Por último, este estudio busca conocer cuál es el grado de concienciación e implicación real en materia de ciberseguridad por parte de la alta dirección y este año el resultado ha sido prometedor.

Este año, los CISO se han implicado más en los proyectos de ciberseguridad relevantes para la compañía frente a otras tareas. Esto es consecuencia de los procesos de transformación donde la nube, IoT o filosofías ZeroTrust son las grandes protagonistas.

Gráfica 9.3: Tareas más importantes para los CISO



28. Informe Ransomware Trends: risks and resilience de Allianz realizado sobre compañías de entre 100-5.000 empleados.

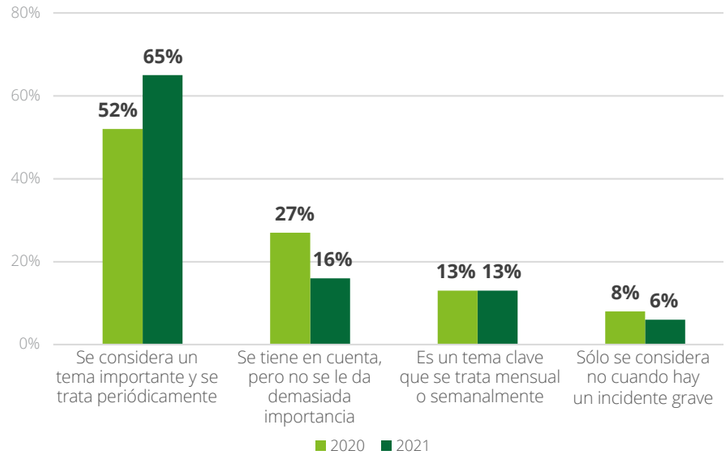
En concreto, un **65% de las compañías considera que su dirección se encuentra en el mayor nivel de concienciación, al considerar que la ciberseguridad que es un tema importante y es tratado periódicamente en sus comités.** Se aprecia un incremento del 25% de este indicador de máximo nivel de concienciación respecto al estudio de pasado año.

El decidido apoyo institucional a la ciberseguridad, junto a la necesidad de abordar los proyectos de digitalización en las compañías, han actuado de catalizadores para, en última instancia, incrementar el respaldo por parte de los equipos directivos a la ciberseguridad de sus compañías.

En el estudio de Deloitte *Future of Cyber 2021* confirma este hecho: el 41% de las empresas destaca cómo la transformación digital y el IT híbrido es la tarea más compleja que se afronta en materia de ciberseguridad, frente a otras gestiones como la ciberhigiene[29] (26%), las limitaciones del talento en ciberseguridad (20%) o la gestión del *shadow IT* (13%).

La alta dirección empieza a estar concienciada en materia de ciberseguridad

Gráfica 9.4: ¿Cuál es el grado de concienciación de la alta dirección en cuanto a la ciberseguridad en la empresa?



29. La agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA) declaró que «la higiene cibernética debe considerarse de la misma manera que la higiene personal y, una vez que se integre adecuadamente en una organización, serán simples rutinas diarias, buenos comportamientos y chequeos ocasionales para garantizar que la salud en línea de la organización esté en óptimas condiciones».

10 Las preocupaciones del CISO en tiempos de teletrabajo

Las organizaciones han visto cómo a causa de la pandemia sus procesos de digitalización se han acelerado para dar respuesta a las nuevas modalidades de teletrabajo, lo que consecuentemente ha generado una mayor superficie potencial de ataque expuesta a Internet.

Por este motivo, cabe preguntarse si las compañías están preparadas para afrontar conveniente y diligentemente lo que para muchos es una situación disruptiva.

Si bien en el pasado año más de un 70% de las compañías se sentía al menos "preparadas" para afrontar un escenario de trabajo en remoto masivo, en el presente este dato asciende al 93%, los cuales aseveran que, como mínimo, se encuentran "preparadas" y aptas para abordar esta situación, lo que supone un aumento del 18% año tras año.

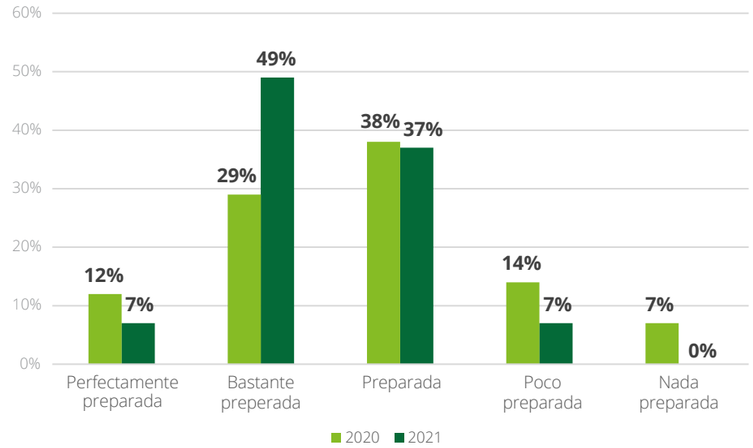
A pesar de los ímprobos esfuerzos de las compañías para adoptar medidas de seguridad para asegurar las condiciones del teletrabajo, los ciberatacantes intensificaron sus ataques, tal y como matiza este estudio.

El pasado año se produjo una preocupante interrupción en la alcista tendencia que los presupuestos de ciberseguridad venían experimentando desde tiempo atrás. Estos recortes en el presupuesto de ciberseguridad tenían su respuesta en la incertidumbre que la pandemia generaba sobre las cuentas de resultados de las compañías.

Sin embargo, el presente informe refleja cómo se retoma el camino de una mayor dotación de fondos al área de ciberseguridad. **El 63% de las compañías destaca que sus presupuestos se han visto incrementados o se incrementarán como consecuencia de la pandemia.** Por el contrario, un año atrás la opción preferente era optar por la disminución de estos, tal y como confirmaba un 57% de los participantes en el estudio.

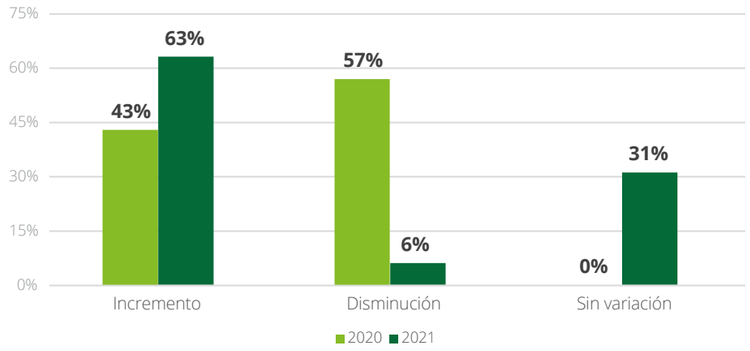
El teletrabajo: la nueva normalidad donde el 93% de las empresas se considera preparadas en ciberseguridad para afrontar esta realidad laboral

Gráfico 10.1: ¿Cómo de preparada está su empresa para afrontar los riesgos de ciberseguridad que conlleva el teletrabajo en situaciones como la actual?



El 72% de las compañías detectó un recrudecimiento de los ciberataques sufrido en el mismo momento que estas se adentraban en el escenario del teletrabajo masivo.

Gráfico 10.2: ¿Considera que el presupuesto anual de ciberseguridad se ha visto variado o prevé que se vaya a variar, debido a la situación actual?



Se acabaron los recortes presupuestarios para el área de ciberseguridad debido a la pandemia. En el último año las empresas volvieron a la senda del incremento presupuestario periódico de esta área

En este sentido, cabe destacar no sólo los proyectos *one-off* abordados para afrontar las iniciativas de despliegue de nuevas formas de teletrabajo y necesidades de digitalización del negocio, sino que los servicios de ciberseguridad deberán prestarse de forma recurrente a través de tareas de operación, mantenimiento y monitorización y respuesta, que en última instancia engrosarán previsiblemente la partida presupuestaria de ciberseguridad los próximos años.

Superado el debate sobre la funcionalidad e idoneidad del teletrabajo, las organizaciones diseñan nuevas modalidades de trabajo que cubran las expectativas de empleados, directivos y proveedores.

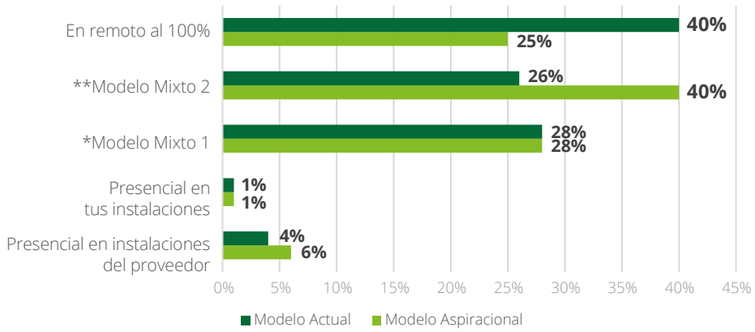
En relación con los proveedores de ciberseguridad, se presenta una importante brecha entre la configuración presente en la actualidad y la aspiracional de los CISO.

La mayoría de CISO no quiere un teletrabajo ni una presencialidad del 100%, más bien se decantan por un regreso paulatino de su personal externo a sus oficinas, donde se combine la presencialidad con el trabajo en remoto

Mientras que el esquema preferente en la actualidad está conformado por el trabajo en remoto casi al 100% en muchos de los casos, **los máximos responsables de seguridad demandan un modelo híbrido, mediante el cual los proveedores alternen entre la asistencia a sus instalaciones junto al trabajo en remoto,** práctica que ya se está observando al comienzo de 2022.

Sin embargo, en ningún caso existe predilección por la sistemática presencialidad de los proveedores en las instalaciones de clientes, opción existente en tiempos previos a la pandemia.

Gráfico 10.3: ¿Cuál es la modalidad de trabajo actual de tus proveedores de ciberseguridad y cuál es tu modelo preferente?



* Modelo Mixto 1: presencial en las instalaciones del proveedor y en remoto.
** Modelo Mixto 2: presencial en las instalaciones de la propia empresa y en remoto.

Conclusiones

Principales conclusiones del estudio

En primer lugar y aludiendo al número de empleados dedicados en materia de ciberseguridad, **el 81% de los participantes considera que no cuenta con suficientes empleados.**

También se aprecia cómo las responsabilidades de ciberseguridad se escapan fuera del departamento, donde el 44% de los participantes cuenta con apoyo y tareas realizadas en esta materia por otras áreas.
Se trata de un dato positivo, pues si se hace a través de una correcta coordinación, es síntoma de una mayor concienciación y ciberresiliencia organizacional.

La mayoría de las empresas cuenta con un SOC[30]/CSIRT[31], solo el 15% (las más pequeñas) no cuenta con estos centros de operaciones especializados en ciberseguridad.

Los recursos financieros en materia de ciberseguridad se consolidan y siguen aumentado. De hecho, representan el 9,4% respecto a los de IT (1% más respecto al año pasado).

Dichos presupuestos van mayoritariamente a tareas de mantenimiento (OPEX[32]) frente a las nuevas inversiones (CAPEX[33]).

También destaca cómo **sigue aumentando la externalización de los servicios de ciberseguridad,** práctica que además lideran las empresas que pertenecen a los sectores con mayor nivel de madurez en ciberseguridad.

Con respecto al modelo operativo, se ha identificado que **en más de la mitad (53%) de las empresas analizadas el CISO reporta al CIO,** dato que ha sufrido un incremento respecto al año anterior.

El CISO ha ganado visibilidad a través de una mayor participación en los diversos comités definidos en las compañías, donde destaca **un aumento del 12% en su participación en el Comité de Dirección.** Aunque la tendencia es positiva, resulta evidente que la figura del CISO aún no ha adquirido la suficiente relevancia como para participar en la toma de decisiones estratégicas de las organizaciones.

Uno de los principales aspectos que se ha identificado a lo largo del estudio es que **el número de empresas que no dispone de ninguna certificación en materia de seguridad se ha reducido en un 11% respecto al año anterior.** A pesar de ello, aún el 49% de las compañías no dispone de ninguna certificación en materia de ciberseguridad. Estas últimas fueron las que recibieron el 69% del total de ciberincidentes, motivo por el cual resulta clave el esfuerzo de que las empresas se certifiquen.

Las 5 certificaciones por las que los CISO se decantan más son: CISA (32%), CISM (25%), ISO 27001 (23%), CISSP (19%), y Director de Seguridad (11%).

Cabe resaltar en el estudio realizado este año el aumento en la demanda de las certificaciones ISO 22301 (5%) y CRISC (4%), indicativo de la preocupación del impacto en el negocio, especialmente por los ataques de *ransomware* más conocidos y una mayor preocupación por gobernar la ciberseguridad a través de la medición de los ciberriesgos por parte de los CISO.

Por lo que respecta al framework empleado por las compañías para la mejora de sus procesos de ciberseguridad, el más utilizado es el estándar ISO 27001, con un crecimiento del 11% respecto al año anterior, y que alcanza un nivel de adopción del 86% a pesar del nivel moderado de certificación en dicho estándar (solo el 31%). **En cuanto al Deloitte CSF, se mantiene como el tercer framework más utilizado en España, convirtiéndose en uno de los principales estándares del mercado.**

En cuanto a la formación y concienciación, cabe destacar que **el número de empresas que no dedican tiempo a formar y concienciar a sus empleados se ha reducido en un 14%. De hecho, las empresas que imparten más de 20 horas de formación y concienciación a sus empleados han recibido únicamente el 15% de los incidentes sufridos en el último año,** lo que denota la clara relación entre el nivel de formación y concienciación de los empleados y los incidentes sufridos.

A nivel de revisiones de aplicaciones críticas, **solo un 66% de las empresas consultadas revisa al menos la mitad de las aplicaciones del negocio que se consideran como críticas y, en cambio, solo el 21% de las aplicaciones críticas son revisadas en su totalidad.**

Es de interés recalcar la importancia de realizar revisiones de las aplicaciones críticas del negocio, ya que refuerza la protección de la organización y de sus datos, por lo que preocupa que el **15% de las empresas consultadas no revisen ni la cuarta parte de sus aplicaciones.** No obstante, año a año se aprecia una evolución en este sentido y cada vez son menos las empresas que no revisan las aplicaciones que sustentan su negocio, lo cual es un dato esperanzador.

En cuanto a la periodicidad con la que se realizan las revisiones comentadas anteriormente, casi el 64% de las empresas consultadas sigue las buenas prácticas de los organismos internacionales y realizan dichas revisiones, al menos, de forma anual.

Por otra parte, cada año se puede observar la importancia de los servicios Cloud. Ya no hay discusión posible: la mayoría de las empresas está migrando a la nube, si no lo ha hecho ya. A pesar de ello, hay un 19% de las empresas que dispone de infraestructura o servicios en la nube, pero no tiene una estrategia Cloud bien definida.

Por otra parte, otras tecnologías igualmente disruptivas como IoT, está presente en el 75% de las empresas consultadas y, al menos, el 67% contempla medidas específicas para estos dispositivos.

El análisis sectorial de los incidentes ocurridos en el año 2021 indica que **los sectores de Telecomunicaciones, Media y Tecnología y el de Fabricación son los que más número de incidentes reportan al cabo de este último año.**

El 94% de las empresas ha sufrido al menos un incidente grave de ciberseguridad a lo largo de 2021.

Se está produciendo un **incremento en el número de ciberataques sufridos,** ya que la media de incidentes ha aumentado considerablemente respecto al año 2020. Cabe destacar que las empresas que más presupuesto dedican a la ciberseguridad son, en general, aquellas que menos incidentes con consecuencias graves sufren. Unido a ello se observa que las empresas que más empleados destinan a la ciberseguridad son las organizaciones que igualmente menos ataques reciben a lo largo del año.

En lo que respecta a las amenazas, las empresas consideran el malware, el ransomware y el phishing como aquellas más preocupantes.

Las compañías, conscientes de la necesidad de estar preparadas para hacer frente a los incidentes, realizan cada vez más ciberejercicios de simulación de crisis e incidentes. Esta práctica está aumentando con el tiempo y **solo el 39% no realiza ningún tipo de entrenamiento** de este tipo (dato que se está reduciendo con el tiempo).

A pesar de este buen dato, pocas son las empresas que presentan un programa continuo de simulaciones, situándose solo el 8% en este nivel óptimo de entrenamiento recurrente.

Superar un fuerte y disruptivo reto como el enfrentado durante la pandemia ha propiciado que los CISO consideren a sus compañías más preparadas para hacer frente a los incidentes de ciberseguridad en 2021, frente a lo mostrado en 2020.

Sin embargo, esta podría tratarse de una falsa sensación de seguridad, dado que el estudio también desprende que el número de incidentes sufridos en 2021 respecto al pasado año ha aumentado notablemente.

Continuando con las preocupaciones del CISO, se erige como la mayor inquietud la interrupción de negocio, seguida de la fuga de información confidencial y el riesgo reputacional, en concordancia con los datos de ciberincidentes reportados en la industria.

Por último, el estudio arroja un dato positivo sobre el grado de concienciación de la alta dirección respecto a la ciberseguridad. En concreto, establece cómo **el 65% de los comités de dirección considera a la ciberseguridad un tema importante que es tratado periódicamente,** experimentando este mayor nivel de concienciación un aumento del 25% respecto al año anterior.

Una vez superados los mayores momentos de incertidumbre fruto de la pandemia, donde la dotación de presupuesto a la función de seguridad se vio reducida o congelada como respuesta a las previsiones a la baja en cuanto a volumen de facturación y beneficios, tal y como desprendió el informe de Deloitte *El Estado de la Ciberseguridad en España 2020* , la iniciativa privada afronta una nueva realidad de aceleración de su producción y prestación de servicios que va acompañada de un incremento de las partidas destinadas a ciberseguridad. En concreto, **el 63% de los CISO afirma que el presupuesto se incrementará como resultado de la pandemia,** mientras que un año atrás el 57% confirmaba una disminución de su partida de presupuesto en ciberseguridad por esta misma causa.

Los CISO se ven confiados: **el 93% de las compañías se considera, como mínimo, preparadas para afrontar esta nueva modalidad de teletrabajo,** representando un 18% de aumento respecto al pasado año.

A pesar de ello, el modelo actual predominante donde el trabajo en remoto se acerca al 100%, se verá modificado por un modelo híbrido aspiracional por parte de los CISO, donde demandan que sus trabajadores combinen la modalidad presencial y remota.

30. Security Operation Center por sus siglas en inglés. Centro de operaciones en ciberseguridad
31. Computer Security Incident Response Team por sus siglas en inglés. Equipo de Respuesta ante Emergencias Informáticas, el cual suele encontrarse dentro del SOC en muchas organizaciones.
32. Operating expense por sus siglas en inglés. Gastos de operación.
33. Capital expenditures por sus siglas en inglés. Capital destinado típicamente a inversiones y adquisiciones.

Carmen Sánchez Tenorio
Socia Responsable Risk Advisory
csancheztenorio@deloitte.es

César Martín Lara
Socio Risk Advisory – Cyber
cmartinlara@deloitte.es

Gianluca D'Antonio
Socio Risk Advisory – Cyber
gdantonio@deloitte.es

Miguel Olías De Lima
Senior Manager Risk Advisory – Cyber
moliasdelima@deloitte.es

Alejandro Viana
Delivery Manager Risk Advisory – Cyber
aviana@deloitte.es

Deloitte.