

Deloitte.

El estado de la ciberseguridad en España

Cyber Strategy, Transformation and Assessments

2023



Índice

Cyber Strategy, ¿quiénes somos?	4
Contexto: Otras iniciativas	5
Encuesta Global Future of Cyber 2023	6
Muestra tomada para el estudio	7
Dominios del estudio	10
Módulo 01. Headcount y SOC	12
Módulo 02. Presupuesto y servicios	18
Módulo 03. Estrategia y modelo operativo	24
Módulo 04. Certificaciones, frameworks y formación	30
Módulo 05. Revisiones de Seguridad	34
Módulo 06. Entornos Cloud y tendencias tecnológicas	38
Módulo 07. Incidentes de seguridad	42
Módulo 08. Simulaciones de cibercrisis	48
Módulo 09. Percepción del CISO	52
Módulo 10. Las preocupaciones del CISO en tiempos de teletrabajo	56
Principales conclusiones del estudio	60
Contactos	63

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 en su día a día información actualizada y sectorial para ayudar a las compañías a definir sus estrategias y tomar las decisiones correctas en materia de gobierno de la seguridad en base a comparables. Gracias a la dilatada experiencia madurada en los cientos de proyectos ejecutados durante los últimos 4 años, Deloitte puede realizar benchmarks sectoriales sobre ciberseguridad con un elevado nivel de detalle. 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, nació hace 4 años este estudio, que contribuye y fomenta la compartición de información relevante, lo cual beneficia especialmente a la ciberresiliencia de las compañías españolas. Los servicios de consultoría ofrecidos por Deloitte Cyber Strategy destacan por la definición de planes

estratégicos y directores de ciberseguridad, la definición de los modelos operativos y de gobierno, y la evolución de los SOC y CSIRT de las compañías a través de la mejora de estos servicios, orientando los mismos a la cobertura real de amenazas.

Puesto 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

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 principales preocupaciones, 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 compañía.
- Elevada presión para responder a las expectativas de negocio. Revisiones de seguridad, entornos Cloud y nuevas tendencias tecnológicas que requieren ser conscientes 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 2022 es la cuarta edición del análisis nacional de las tendencias del sector, elaborado con resultados obtenidos del feedback de alrededor de unos 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 la industria.

Para obtener más información sobre los Executive & Board Programs de Deloitte, visita nuestra web <https://executiveprograms.es.deloitte.com/> o 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

Encuesta Global **Future of Cyber 2023**

En diciembre de 2022, Deloitte realizó un estudio internacional denominado Global Future of Cyber Survey 2023¹, en el que se ha vuelto a incluir a miembros del C-Suite/Board, brindando información tanto cualitativa como cuantitativa a través de datos provenientes de más de 1.000 entrevistas y respuestas de clientes en todas las geografías e industrias.

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 2022, 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 de 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 compañías 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 puedan utilizar para 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.

1

<https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html>

Muestra tomada para el estudio

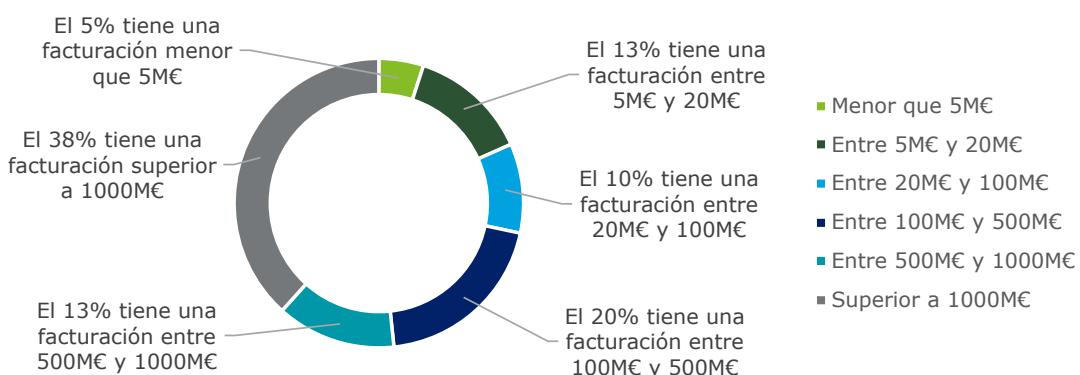
Todas las compañías analizadas son españolas o, en su defecto, su centro de operaciones de ciberseguridad reside en España. Toda la información contenida en el informe se ha anonimizado, manteniéndose en todo momento la confidencialidad y privacidad de las compañías participantes.

Muestra tomada para el estudio

La muestra de este año está fuertemente caracterizada por compañías con una facturación superior a 500 millones de euros al año. Estas suponen más del 50%, por lo que muchas conclusiones tienen un sesgo relacionado con compañías de gran facturación.

A continuación, se analiza el perfil de las compañías del estudio para facilitar la comprensión de los resultados.

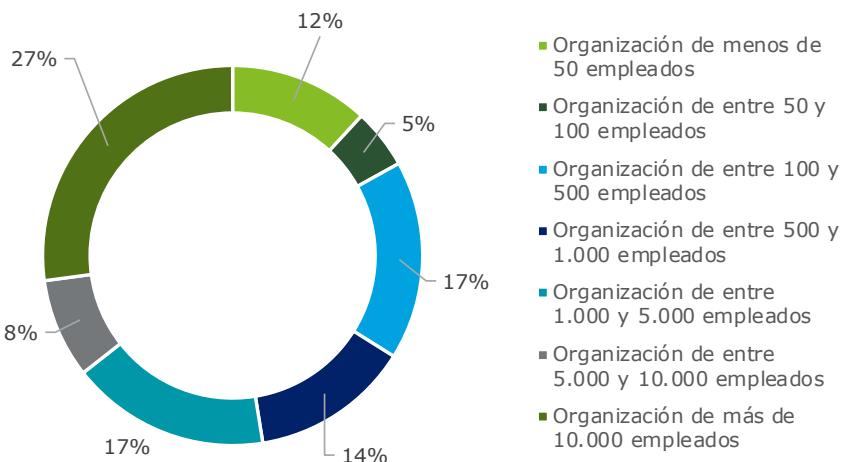
Facturación de la muestra



Headcount²

Como en el apartado anterior, si se analiza la muestra del estudio desde el punto de vista de empleados totales, se puede observar que más del 50% de las organizaciones tienen más de 1.000 empleados, lo que refuerza el sesgo del estudio a grandes compañías.

Empleados de la muestra

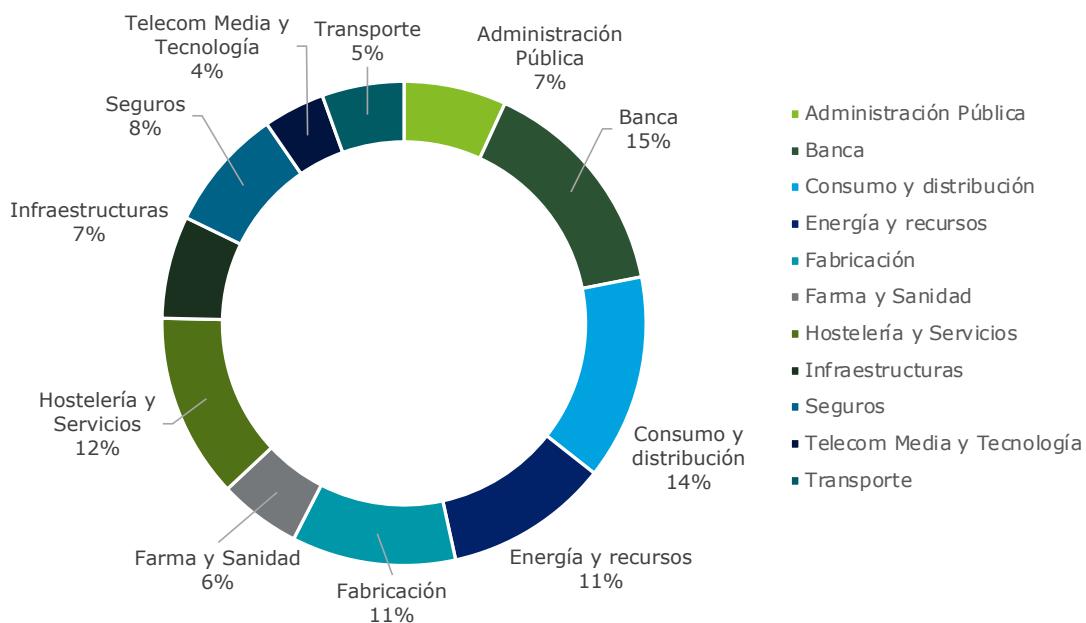


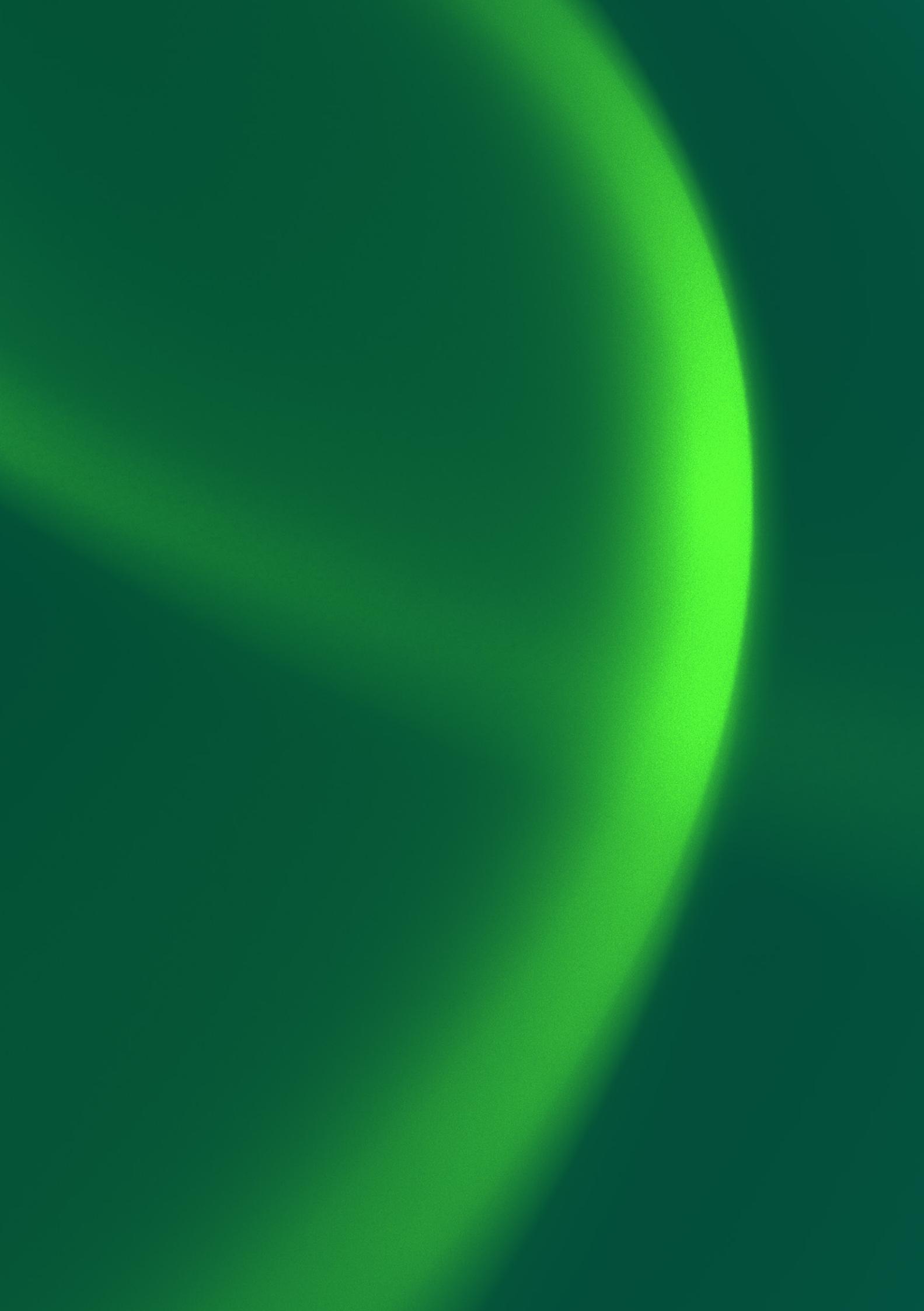
Sectores

Como en años anteriores, la muestra a nivel sectorial es relativamente equilibrada: la representación de cada sector contemplado en el estudio oscila entre un 5% y un 15%, lo que facilita la inclusión de comparativas en el análisis.

Aun así, hay algunas variaciones que merecen ser mencionadas con respecto al estudio anterior. Ha disminuido la representación de Banca y Telecomunicaciones, y ha aumentado la representación tanto de Consumo y Distribución como de Fabricación.

Industrias de la muestra





Dominios del estudio

Módulo 01. Headcount y SOC

El entorno de amenazas en constante cambio y las nuevas tecnologías obligan a las compañías a redimensionar de forma continua el número de personas asignadas a la función de ciberseguridad y evolucionar de forma continua sus centros de operaciones y respuesta.

Módulo 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 tras año, siendo necesaria a su vez la optimización de dichos recursos. Una estrategia muy necesaria 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 un futuro ahorro de costes (al evitar y gestionar eficazmente los posibles ciberincidentes), y no solo como un gasto más para el negocio.

Módulo 03. Estrategia y modelo operativo

Los objetivos del negocio deben ser representados en la Estrategia de ciberseguridad. De igual manera, la definición de un modelo operativo eficiente y el cumplimiento de políticas de seguridad (no solo a nivel nacional) deben ayudar a los CISO a optimizar los recursos dedicados a seguridad y los presupuestos asignados.

Módulo 04. Certificaciones, framework 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 adoptar suele ser objeto de debate y discusión entre la comunidad de CISO, al no haber un verdadero consenso sobre cuáles son los más útiles o demandados en el mercado.

Módulo 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 los resultados pueden derivar posibles planes de acción a ejecutar.

Módulo 06.

Entornos Cloud y tendencias tecnológicas

Una de las preocupaciones del CISO en la actualidad se centra en el uso de las infraestructuras en la nube y en las diferentes modalidades que pueden adoptar las compañías para afrontar los cambios derivados. En este estudio analizaremos también cuál es el uso real que se está haciendo de tecnologías como el IoT³.

Módulo 07.

Incidentes de seguridad

Probablemente la mayor preocupación de los CISO es saber cuándo y cómo recibirá el siguiente ciberataque o sufrirá el próximo ciberincidente. Para facilitar una respuesta, se analizarán cuáles son las estadísticas de incidentes en los últimos años en los diferentes ámbitos empresariales y qué papel jugó el ciberseguro.

Módulo 08.

Simulaciones de cibercrisis e incidentes

Además de seguir transformándose desde un punto de vista tecnológico, las compañías deben realizar labores de adiestramiento de las diferentes capas involucradas en la ciberseguridad. En las simulaciones se intenta crear un entorno similar a una situación concreta, derivada de un incidente, para probar la robustez de los procedimientos de respuesta y preparar, de forma práctica, a las personas en sus respectivos roles y responsabilidades.

Módulo 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 seguro se siente ante el próximo ciberataque al que tendrá que enfrentarse su compañía.

Módulo 10.

Las preocupaciones del CISO en tiempos de teletrabajo

La COVID-19 ha supuesto un cambio de paradigma en la sociedad. No solo está siendo una de las crisis más duras que se recuerdan, sobre todo a nivel sanitario, sino que está suponiendo todo un reto para las organizaciones en términos de digitalización y ciberseguridad.

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 muchos casos un verdadero reto para los CISO, puesto que el modelo de operación de la empresa ha cambiado lo suficiente como para adaptar y replantear rápidamente los modelos de ciberseguridad ante esta nueva realidad.

Módulo 01.

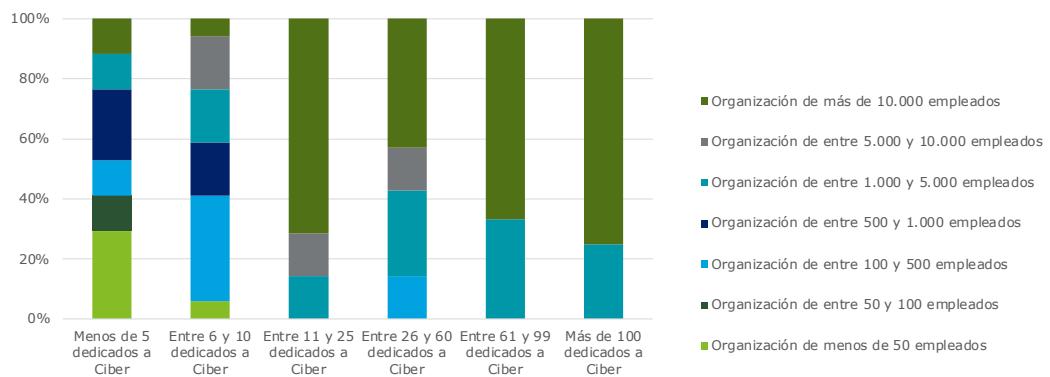
Headcount y SOC

Empleados dedicados en exclusiva a la ciberseguridad

Si se analiza la ratio de personas dedicadas a la ciberseguridad en función de los empleados totales de las organizaciones, destacan los siguientes resultados: aproximadamente el 20% de las organizaciones que tienen menos de 5 empleados dedicados a ciberseguridad tienen más de 1.000 empleados. De hecho, las organizaciones con más de 10.000 empleados tienen ya presencia en rangos tan bajos como el de entre 11 y 25 empleados dedicados a la ciberseguridad en exclusiva.

El 50% de las organizaciones estudiadas tienen menos de 10 personas dedicadas en exclusividad a labores de ciberseguridad.

Comparación empleados ciber y de la compañía



Personal de ciberseguridad externo

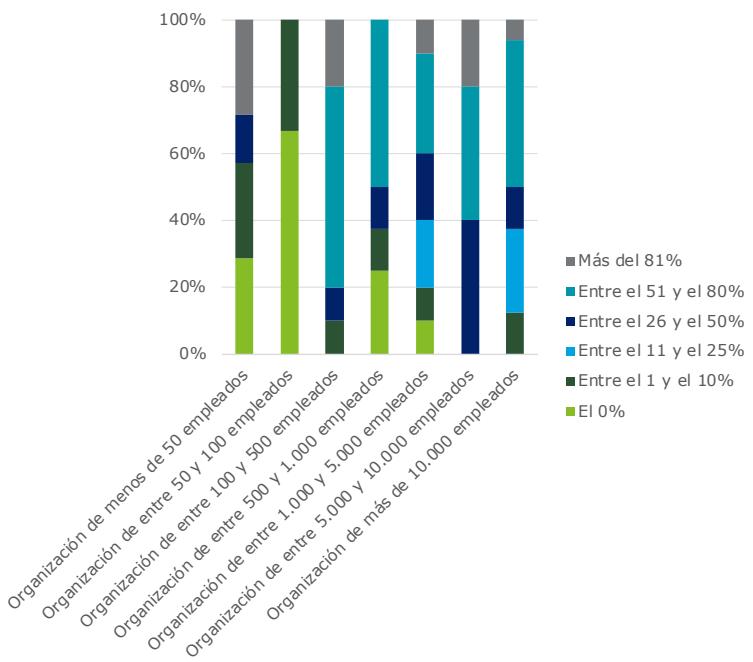
Siguiendo con el análisis del personal dedicado a la ciberseguridad y poniendo el foco en la externalización, los resultados son muy similares a los del año pasado.

El 50% de las organizaciones analizadas tienen un nivel de externalización de más del 50%.

Es destacable para las compañías con un número de empleados de entre 50 y 100 que más del 60% no tengan externalización, lo que, unido a los resultados del apartado anterior, indica que son compañías que tienen menos de 5 empleados dedicados en exclusiva a la ciberseguridad.

También es reseñable que en las organizaciones con más de 1.000 empleados la externalización cada vez está más presente, llegando a casi el 50% de los casos. Estos resultados son lógicos, teniendo en cuenta que, cuanto mayor es el número de empleados de una entidad, más compleja resulta la gestión de la ciberseguridad, lo que hace que se recurra con mayor frecuencia a equipos expertos externos dedicados.

Externalización en función de los empleados

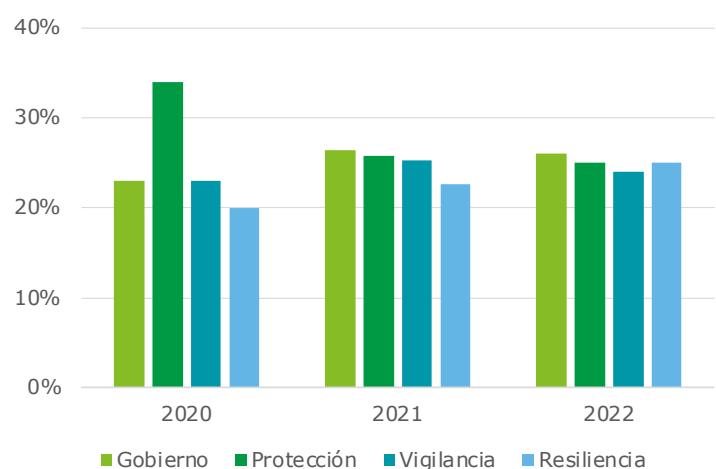


Distribución de empleados según las líneas de ciberseguridad

Deloitte divide la ciberseguridad en cuatro dominios: Gobierno, Protección, Vigilancia y Resiliencia. En los últimos años se ha observado una tendencia a la homogeneización de la distribución de los empleados de ciberseguridad en dichas disciplinas en las organizaciones: Gobierno se ha mantenido estable, y Protección y Vigilancia han cedido terreno a Resiliencia.

La distribución por dominios de ciberseguridad mantiene su tendencia a la homogeneidad.

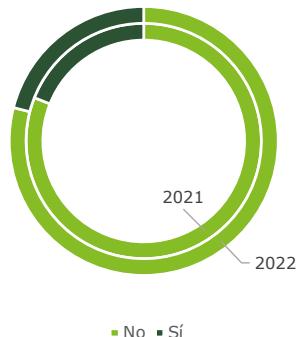
Distribución de empleados por dominios



Dotación del área de ciberseguridad

La valoración de los responsables de ciberseguridad sobre la dotación de recursos de la función técnicamente ha mejorado con respecto al año anterior: el "No" ha pasado de ser un 81% a un 79%, aunque sigue siendo un resultado abrumadoramente negativo, que refleja la dificultad para acceder a un presupuesto o a contratar perfiles adecuados.

Dotación de ciberseguridad

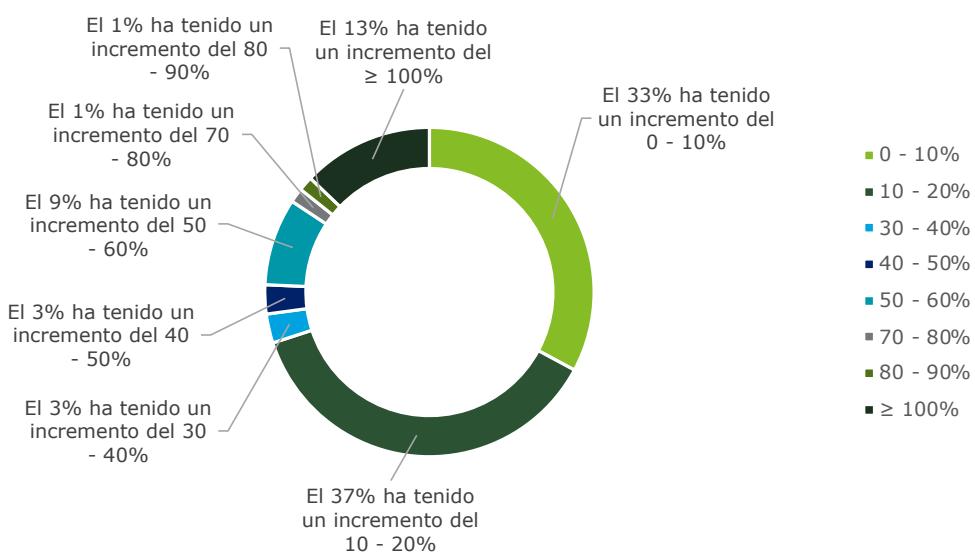


Incremento de FTE en ciberseguridad

Este año, el incremento de FTE de ciberseguridad está dominado por los rangos de 0-10% y de 10-20%, con un 33% y un 37% respectivamente, conformando el 70% de las organizaciones.

En 2022, no ha habido disminución de la plantilla entre las organizaciones objeto del análisis.

Incremento de FTE en ciberseguridad

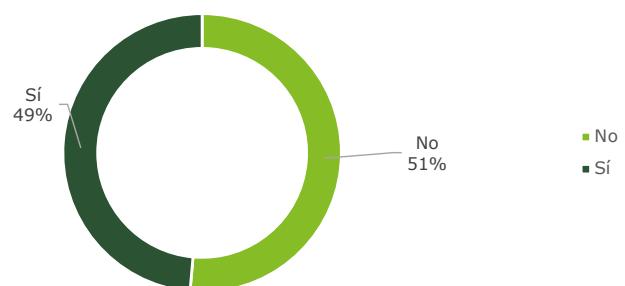


Personal externo al departamento de ciberseguridad con responsabilidades de ciberseguridad

El reparto de las tareas de ciberseguridad más allá de los integrantes del propio departamento sigue siendo una asignatura pendiente: el 51% de las organizaciones del estudio no comparten con otros departamentos las responsabilidades de ciberseguridad.

El negocio y los demás departamentos de soporte todavía no han aceptado las responsabilidades en materia de ciberseguridad que les corresponden.

Departamentos con responsabilidades de ciberseguridad



SOC/CSIRT propio

El 53% de los participantes del estudio tienen un SOC/CSIRT totalmente externalizado, valor que coincide con los resultados del año anterior.

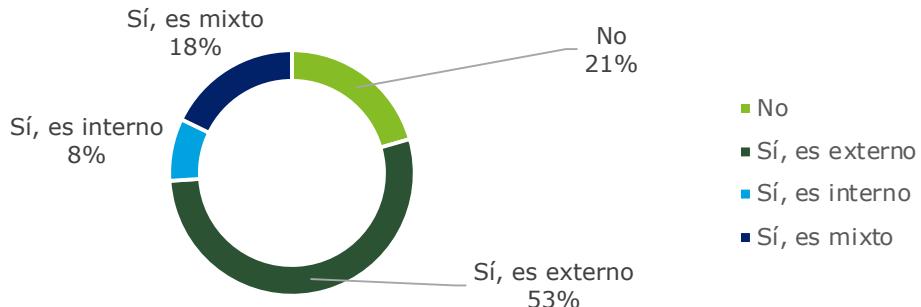
Si se hace un análisis sectorial, cabe destacar que Consumo y Distribución es la industria que más se caracteriza por no tener SOC. La industria con mayor externalización del SOC es Hostelería y Servicios, y la que tiene mayor internalización, Banca.

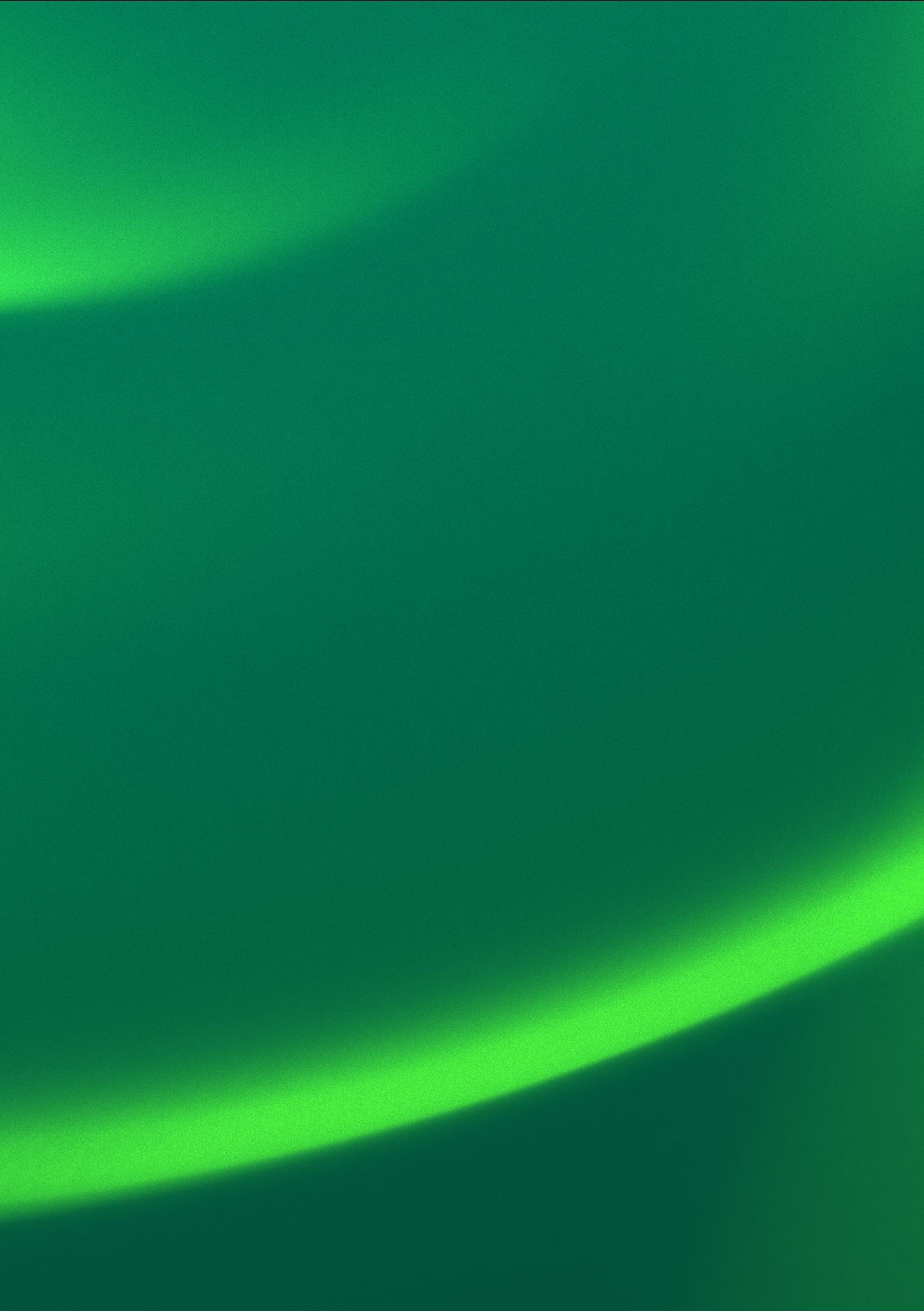
Con respecto al número de empleados dedicados con exclusividad a ciberseguridad, las compañías con menos de 5 empleados dedicados a la ciberseguridad destacan por ser las que no tienen un SOC. Por otra parte, la externalización total del SOC sobresale en las compañías con un rango de empleados dedicados de entre 6 y 10. Estos resultados ponen de manifiesto

una correlación directa entre el nivel de madurez y la profesionalización de los trabajos de monitorización y respuesta ante incidentes.

Todavía hay un 21% de organizaciones que no disponen de un SOC.

Tipología de SOC





Módulo 02.

Presupuesto y servicios

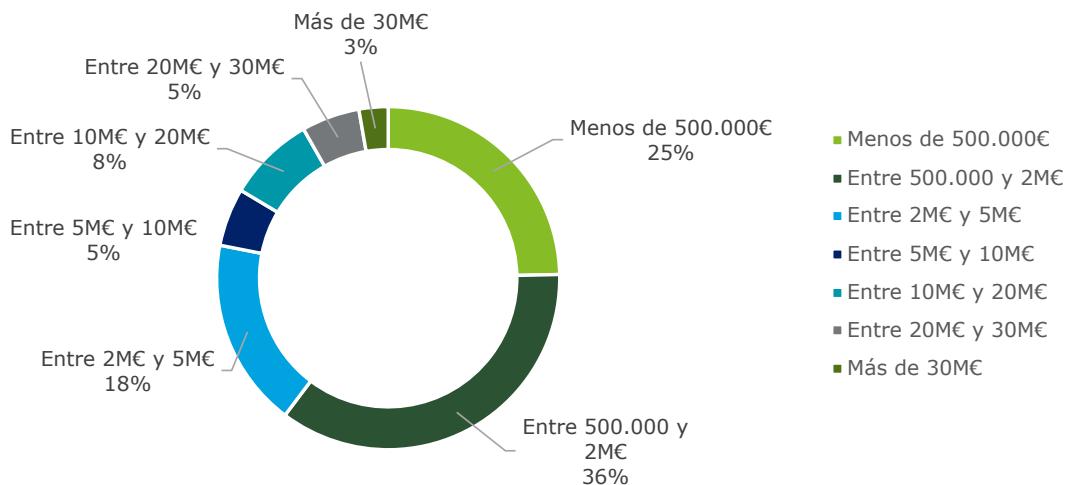
Presupuesto para ciberseguridad

Con respecto a la distribución presupuestaria, se observa que el 25% de las organizaciones tiene un presupuesto menor de 500.000€ en ciberseguridad, y que el 36% entre 500.000€ y 2 millones de euros.

Si se analizan los presupuestos en relación con la distribución sectorial del estudio, se puede destacar que los sectores con presupuestos más altos, superiores a 30 millones de euros, son Banca, por un lado, y Energía y Recursos por otro. Este es el resultado esperado, dado que son industrias con mayor capitalización catalogadas como infraestructuras críticas y, en el caso de la Banca, con una considerable presión regulatoria.

Consumo y Distribución destaca como el sector que tiene los presupuestos más bajos, de menos de 500.000€.

Presupuesto ciber



Relación del presupuesto de ciberseguridad con respecto al de IT

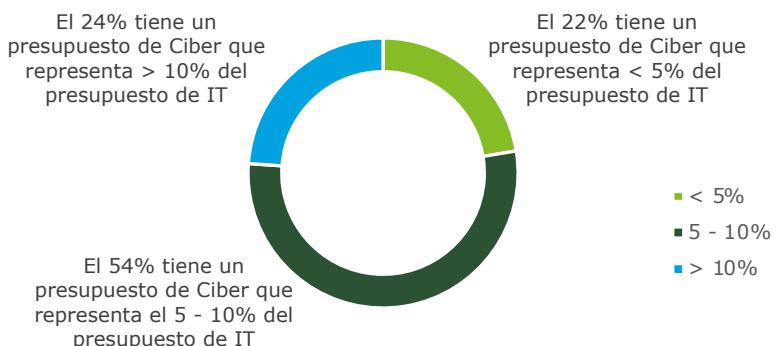
Como ya es habitual en la relación entre el presupuesto de ciber y el de IT, más de la mitad de las organizaciones se posicionan en el rango medio, entre el 5-10%. Cabe reseñar que, con respecto al año pasado, las compañías con una dotación presupuestaria superior al 10% han descendido de un 37% a un 24%.

Cuando se analizan los resultados por sectores, se observa nuevamente que Consumo y Distribución, Fabricación, y Hostelería y Servicios destacan, en este caso, como aquellos sectores en los que la inversión en ciberseguridad está más descompensada con respecto al presupuesto de IT.

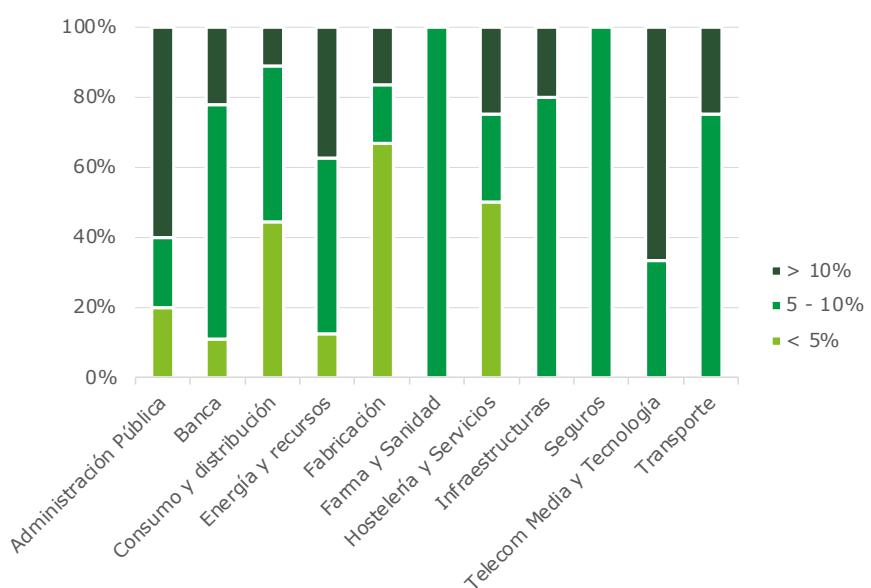
Como en años anteriores, las industrias con mayor presión regulatoria (como las pertenecientes al sector financiero), las consideradas infraestructuras críticas, o las sujetas a RGPD mantienen los mismos niveles de inversión.

Las industrias más alineadas con las tendencias actuales de relación entre presupuesto en ciberseguridad y de IT son Banca, Energía y Recursos, Farmacia y Sanidad, y Seguros.

Ratio presupuesto ciber y IT



Distribución del ratio con IT por industrias

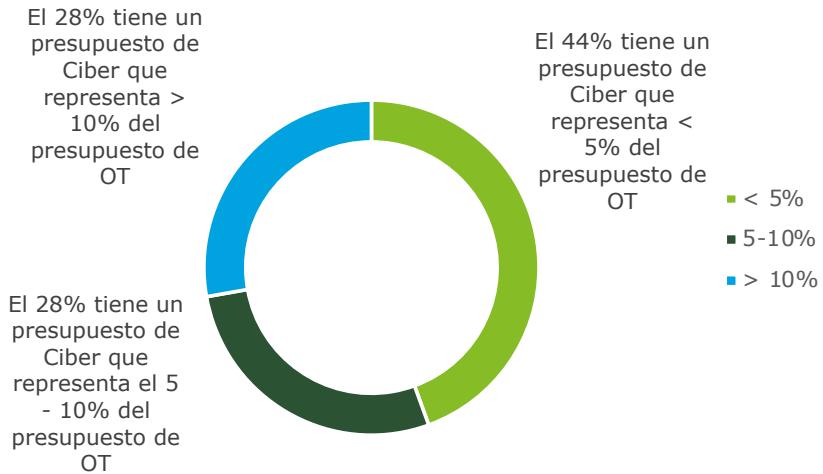


Relación del presupuesto de ciberseguridad con el de OT

Poniendo el foco en el análisis de la distribución del presupuesto de ciberseguridad y analizando lo que se destina a la seguridad de los entornos OT, se aprecia que este último no sigue las mismas tendencias que se observan en la parte de IT. Esto se debe a la relevancia de la continuidad de negocio en estos entornos. La ciberseguridad, cuyas herramientas pueden ser más intrusivas, está relegada a un plano de menor importancia.

La ciberseguridad sigue teniendo capacidad de evolución en los entornos de OT.

Ratio presupuesto ciber y OT

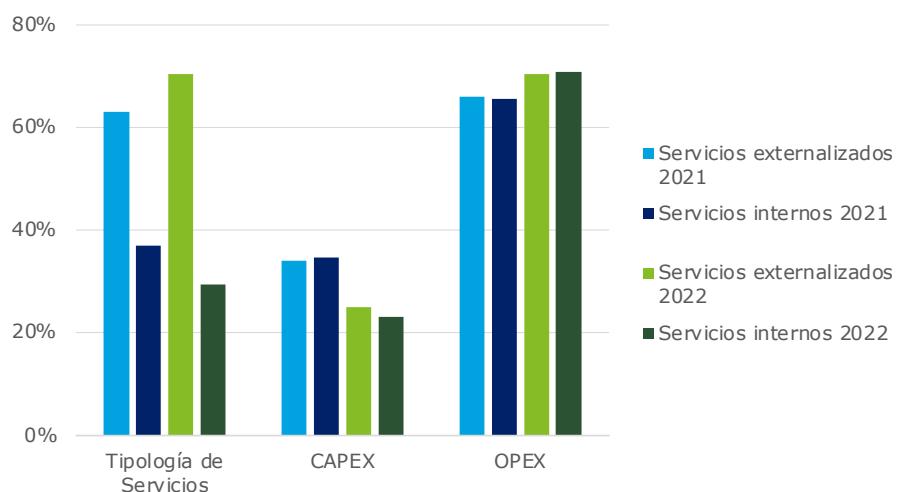


Distribución del presupuesto

Este año, la externalización consolida su dominio en el reparto del presupuesto de servicios, alcanzando el 70%. También el OPEX, tanto para servicios internos como para externos, aumenta su peso en el estudio de este año, alcanzando en ambos casos el 70% también. Esta tendencia confirma, para la muestra analizada, un progreso en la consecución de los objetivos de madurez.

Continúan las tendencias de 2021 hacia la externalización y hacia la operación.

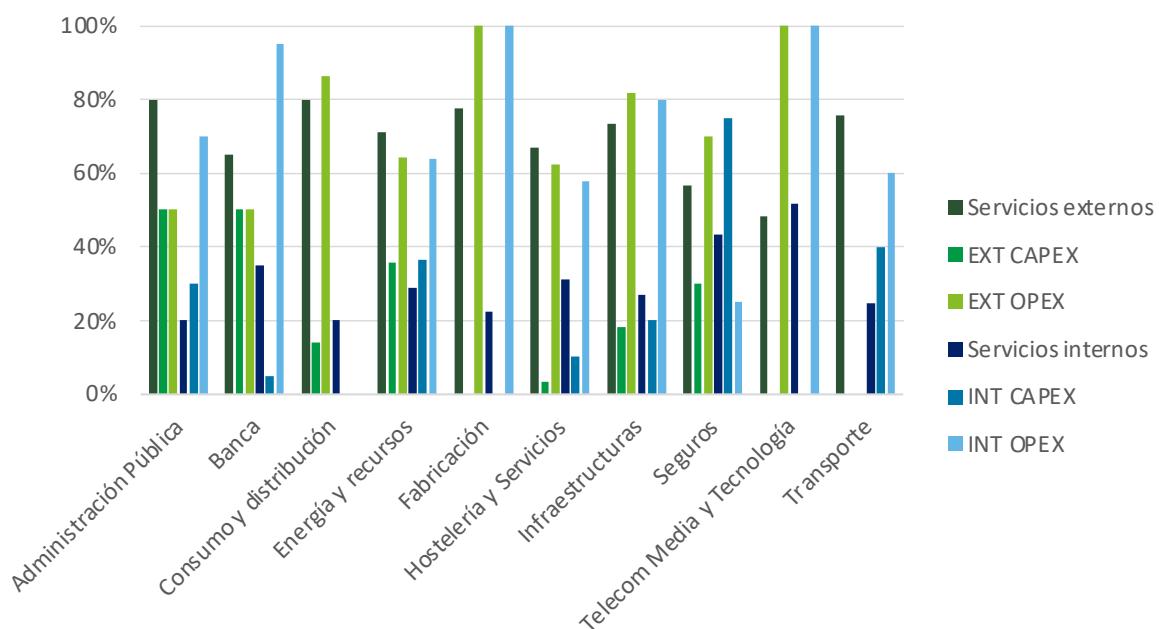
Comparativa de la distribución con 2021



Con respecto a la distribución sectorial, se puede observar que no hay ninguna excepción en la tendencia a la externalización de servicios. Por otra parte, hay sectores en los que hay un claro dominio de la operación, como son Fabricación y Telecomunicaciones, en los que los servicios no

tienen CAPEX asociado. El único caso en el que domina el CAPEX es en Seguros, donde a nivel interno el promedio de CAPEX es notablemente mayor que el de OPEX.

Distribución presupuestaria por industrias



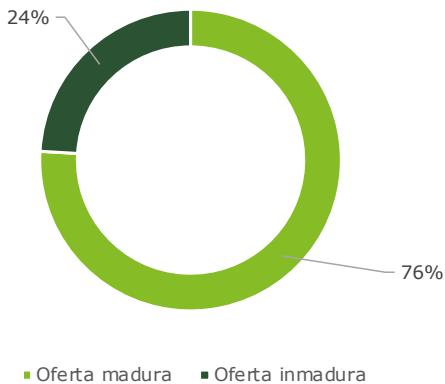
Valoración de la oferta de servicios ciber

Las valoraciones de los servicios ciber en el mercado, como en años anteriores, han estado muy polarizadas.

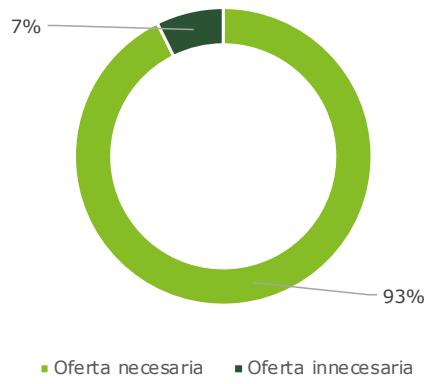
Las tres cuartas partes de los analizados consideran que la oferta es madura y un 93% que es necesaria.

El 85% de las organizaciones consideran que el coste de los servicios ciber en el mercado es excesivo.

Valoración de Madurez de servicios ciber



Valoración Necesidad de servicios ciber

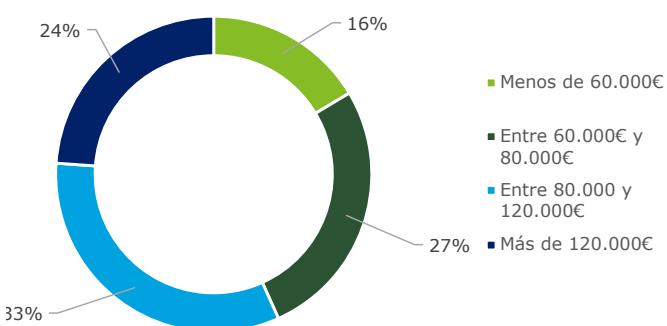


Salario bruto anual del CISO

El rango medio de sueldo anual del CISO sigue siendo de 80.000-120.000€, como en los años anteriores del estudio.

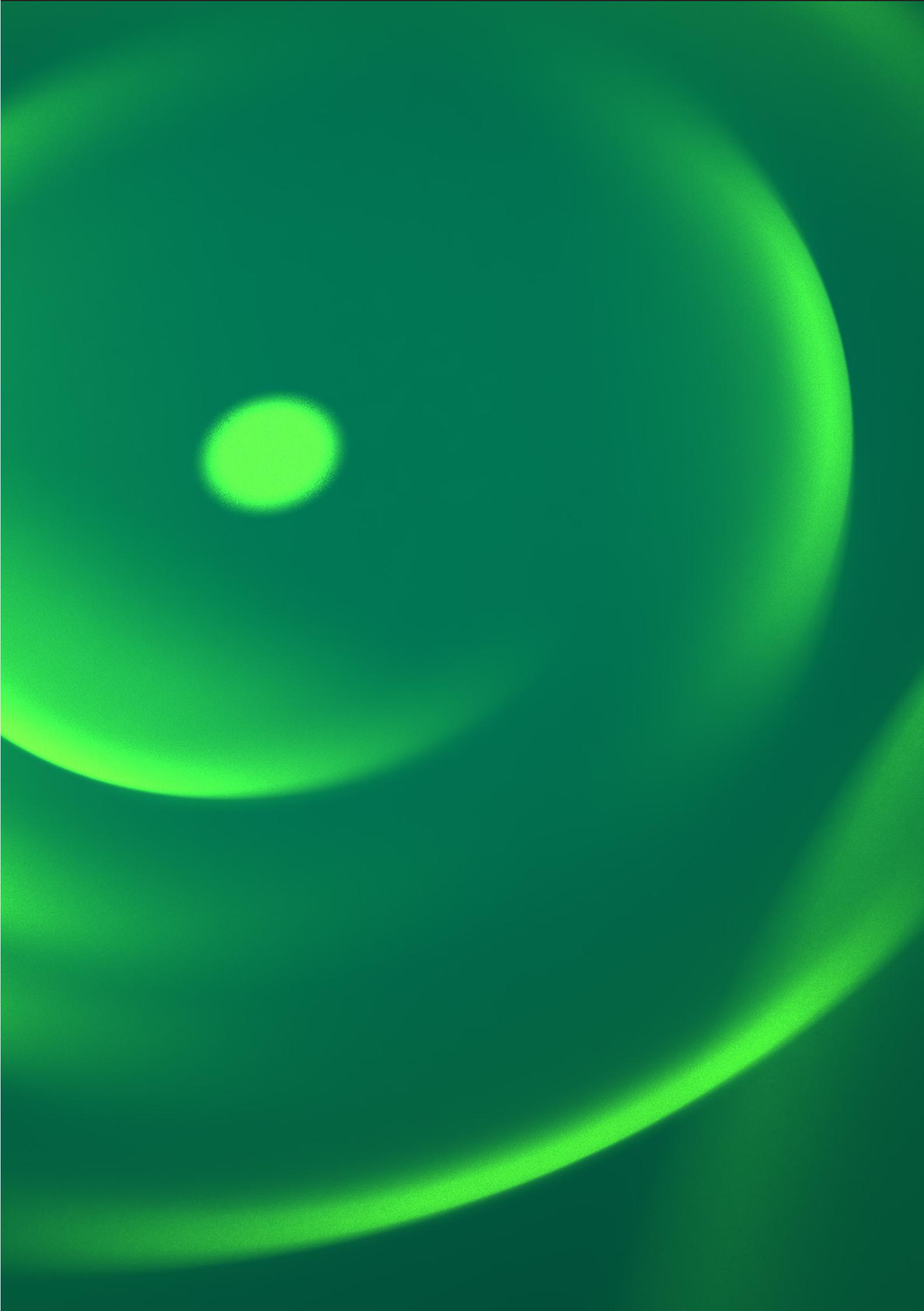
En la evolución anual de salarios, se puede observar cómo el rango que aumenta todos los años es el de más de 120.000€, que, en esta edición, ha conseguido sobrepasar el 20%. De la misma forma, es necesario hacer hincapié en que hay todavía un 16% de CISO en el rango de menos de 60.000€, lo que pone de manifiesto una distorsión del mercado laboral actual, que está experimentando un crecimiento considerable de los salarios, especialmente en el sector privado.

Salario del CISO



Evolución salarial





Módulo 03.

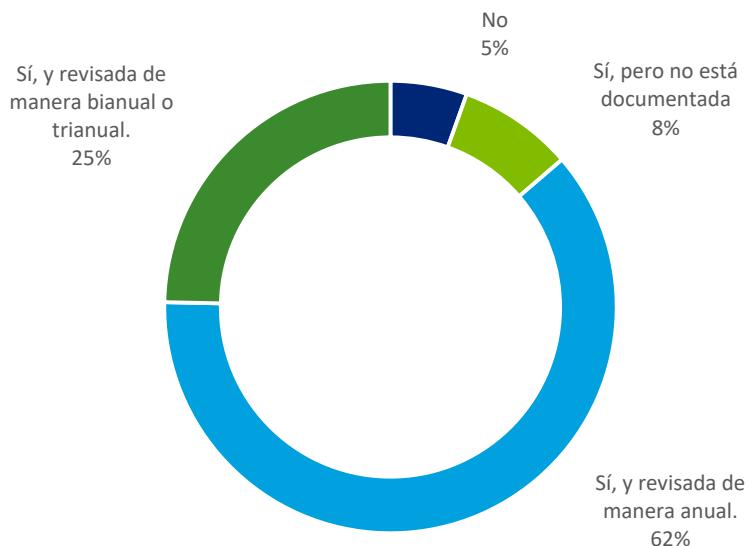
Estrategia y modelo operativo

Estrategia de ciberseguridad de las compañías

A medida que la ciberseguridad adquiere relevancia dentro de las compañías, cada vez es más común y necesario que las mismas inviertan tiempo, esfuerzo y dinero en definir cómo se organizarán todos los recursos disponibles que permitan proteger sus activos.

En este sentido, puede observarse cómo en la actualidad, casi un 90 % de las compañías confirman disponer de una estrategia de ciberseguridad que es revisada de manera periódica, mientras que únicamente un 5% afirma no disponer actualmente de ella.

¿Disponen las compañías de una estrategia de ciberseguridad formalizada y documentada?



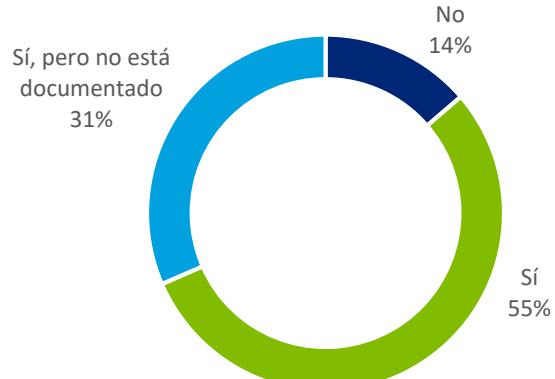
Alineamiento estratégico entre ciberseguridad y negocio

Hoy en día, la necesidad de que los objetivos del negocio se trasladen a la ciberseguridad es vital. A este respecto, es importante tener en cuenta que solo el 55% de las compañías ha realizado un alineamiento formal para ver cómo cubre la ciberseguridad las necesidades de su negocio, poniendo de relieve la existencia de una importante brecha entre ambos aspectos.

Con este alineamiento propuesto, el panorama de amenazas y riesgos será en consecuencia más realista, dando pie a una gestión de incidentes más ágil y adaptada a la realidad de la organización, y facilitando la obtención de presupuestos, como consecuencia directa de dar respuesta a las necesidades de negocio.

Un 14% de las compañías no han realizado aún un alineamiento para ver cómo cubre la ciberseguridad las necesidades del negocio.

¿Se ha realizado un alineamiento estratégico entre ciberseguridad y negocio?

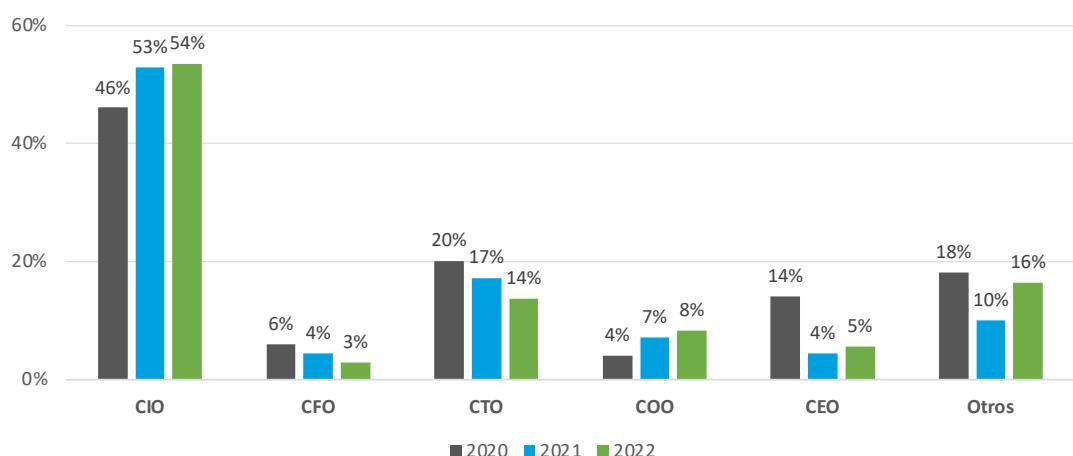


Dependencia del CISO

En cuanto a la ubicación del CISO dentro de la estructura organizativa y su dependencia respecto a la dirección, esta varía en función de cada organización, debido a la diversidad de casuísticas y modelos organizativos presentes en las compañías. 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 misma.

Se puede observar una clara tendencia de cómo predomina la dependencia del CISO directamente del CIO.

¿De quién depende el CISO?

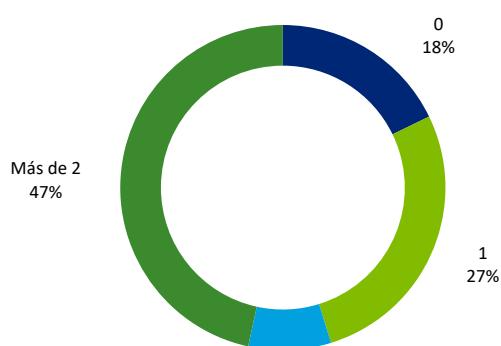


Además, se puede notar un ligero aumento de la dependencia respecto del COO⁴, mientras que, por el lado contrario, cada vez disminuye más la dependencia del CISO respecto al CFO⁵ y al CTO⁶.

Este dato refleja cómo la ciberseguridad tiene cada vez más peso dentro de las tradicionales áreas IT de las compañías, dependiendo directamente más del CIO y dejando de depender de otras áreas, como la parte financiera o de tecnología.

Presentaciones a la Dirección

Presentaciones a la Dirección

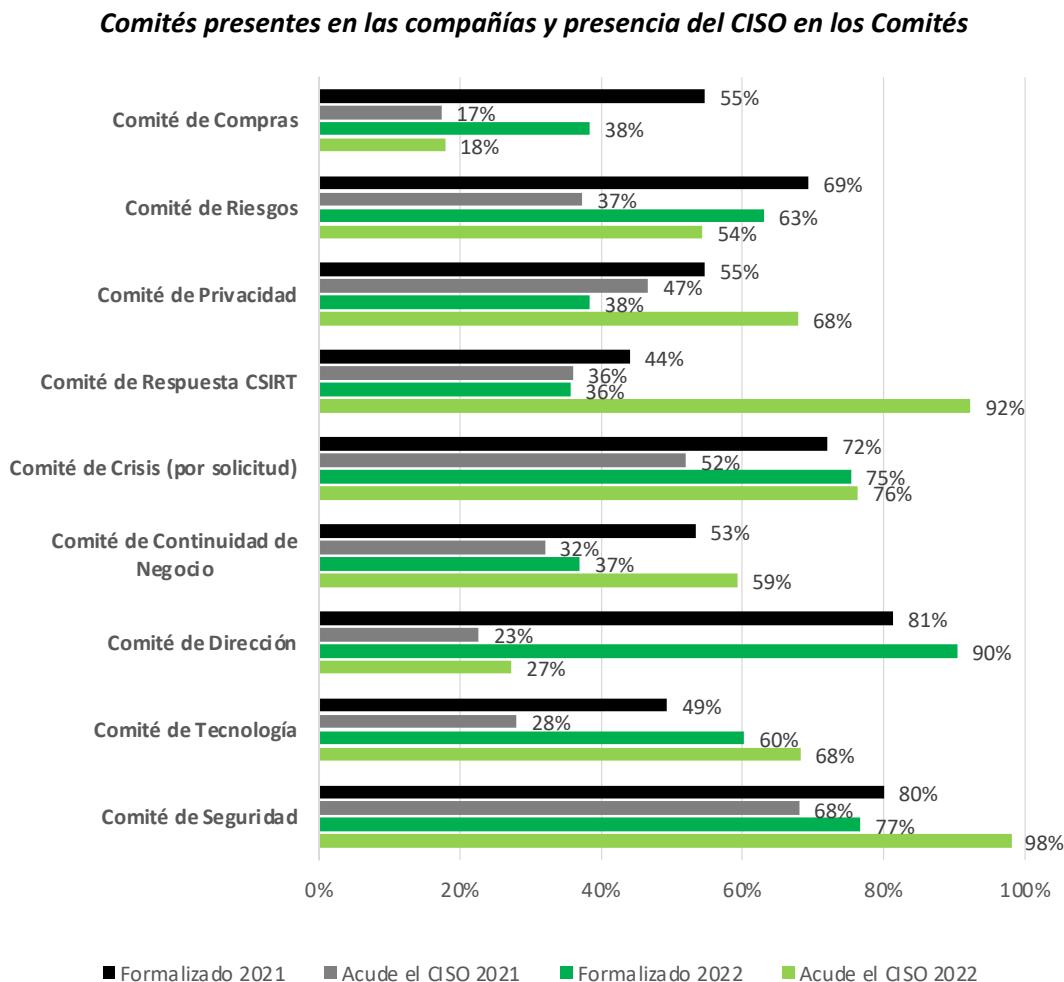


En esta línea y en relación con la mayor influencia de la ciberseguridad dentro de las compañías, destaca cómo casi la mitad de las compañías afirman haber realizado más de una presentación a la Dirección en el último año.

Únicamente un 18% de las compañías afirma no haber realizado ninguna presentación sobre ciberseguridad a la Dirección, lo cual, aunque represente un porcentaje bajo, no deja de ser significativo para seguir trabajando para obtener una mayor involucración y respaldo de la Alta Dirección de las compañías.

- 4 Director de Operaciones 8%
- 5 Director de Finanzas
- 6 Responsable tecnológico de una compañía

Comités existentes y presencia del CISO en los mismos



En esta gráfica, se reflejan las diferencias entre los dos últimos años y se ofrecen algunos datos importantes:

- Este año, se mantiene la tendencia de años anteriores, donde los comités de Tecnología y de Crisis siguen al alza (en este caso, un 11% y un 3% respecto a años anteriores).

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 para poder considerar la ciberseguridad como una práctica necesaria para la consecución de los objetivos de la organización.

- El CISO participa mayoritariamente en el Comité de Seguridad y en el CSIRT, participando de nuevo en todos los Comités, aumentando notablemente su presencia en el CSIRT y el Comité de Crisis.

El CISO participa un 5% más este año en el Comité de Dirección, si bien sigue existiendo un importante gap que cubrir.

Podemos concluir de forma general que, 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.

Áreas o ámbitos de responsabilidad del CISO

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.

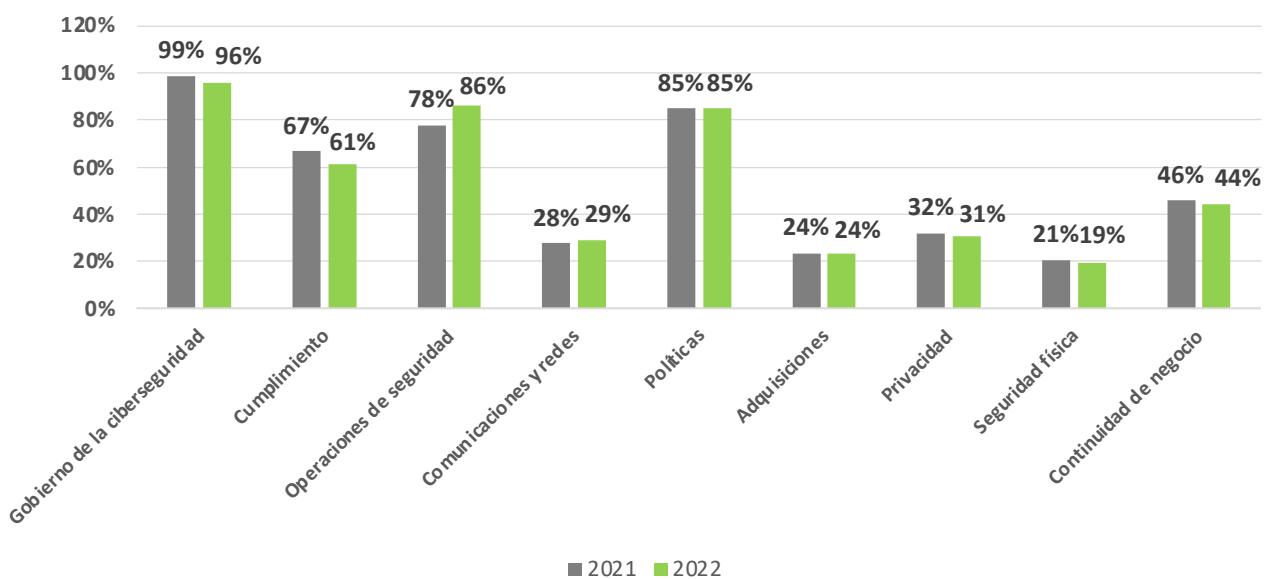
De hecho, con respecto a las áreas o ámbitos de responsabilidad que dependen del CISO, y al igual que en años anteriores, el área que más frecuentemente se encuentra bajo la responsabilidad del CISO es el gobierno de la ciberseguridad, tal y como confirman prácticamente la totalidad de las compañías (96%) que han participado en el estudio.

Adicionalmente, las políticas, las operaciones de seguridad (las cuales han aumentado un 8%), y el

cumplimiento también destacan entre las principales responsabilidades del CISO. Este hecho se debe, en gran medida, al actual panorama regulatorio con impacto en la seguridad de las compañías, que se encuentra en constante evolución y desarrollo (DORA, NIS 2, etc.).

Por último, cabe destacar que únicamente un 12% de las compañías no toman en consideración la ciberseguridad como una función sujeta a la revisión del área de auditoría interna de su compañía, lo cual indica que la mayor parte de estas sí que consideran la ciberseguridad como un área cada vez más importante dentro de sus planes de auditoría y, por ende, de forma general en las compañías.

Áreas o ámbitos de responsabilidad del CISO





Módulo 04.

Certificaciones, frameworks y formación

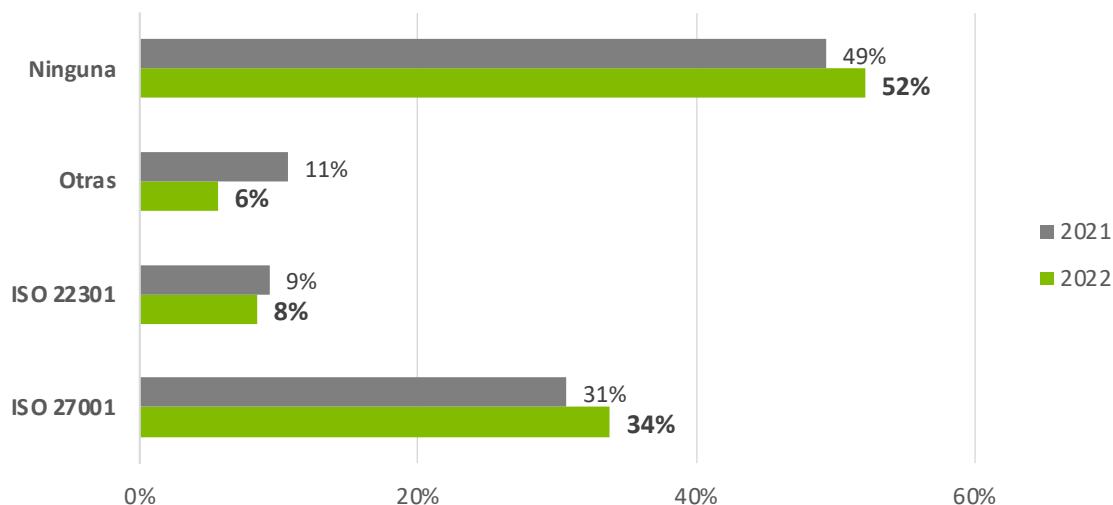
Certificaciones presentes en las compañías

En relación con las certificaciones, las compañías siguen decantándose por la ISO 27001 como la certificación de referencia en ciberseguridad, identificándose un aumento de un 3% en el número de compañías que disponen de esta certificación.

Por otro lado, cada vez son menos las compañías que no disponen de alguna certificación de ciberseguridad, a pesar de que este dato sigue siendo negativo, con casi un 50% de compañías que admiten no contar con una certificación específica.

Sigue existiendo un alto porcentaje de compañías (casi un 50%) que no cuenta con alguna certificación de ciberseguridad, lo cual es un aspecto para trabajar en el corto-medio plazo.

Certificaciones presentes en las compañías



Certificaciones/formación que poseen los CISO

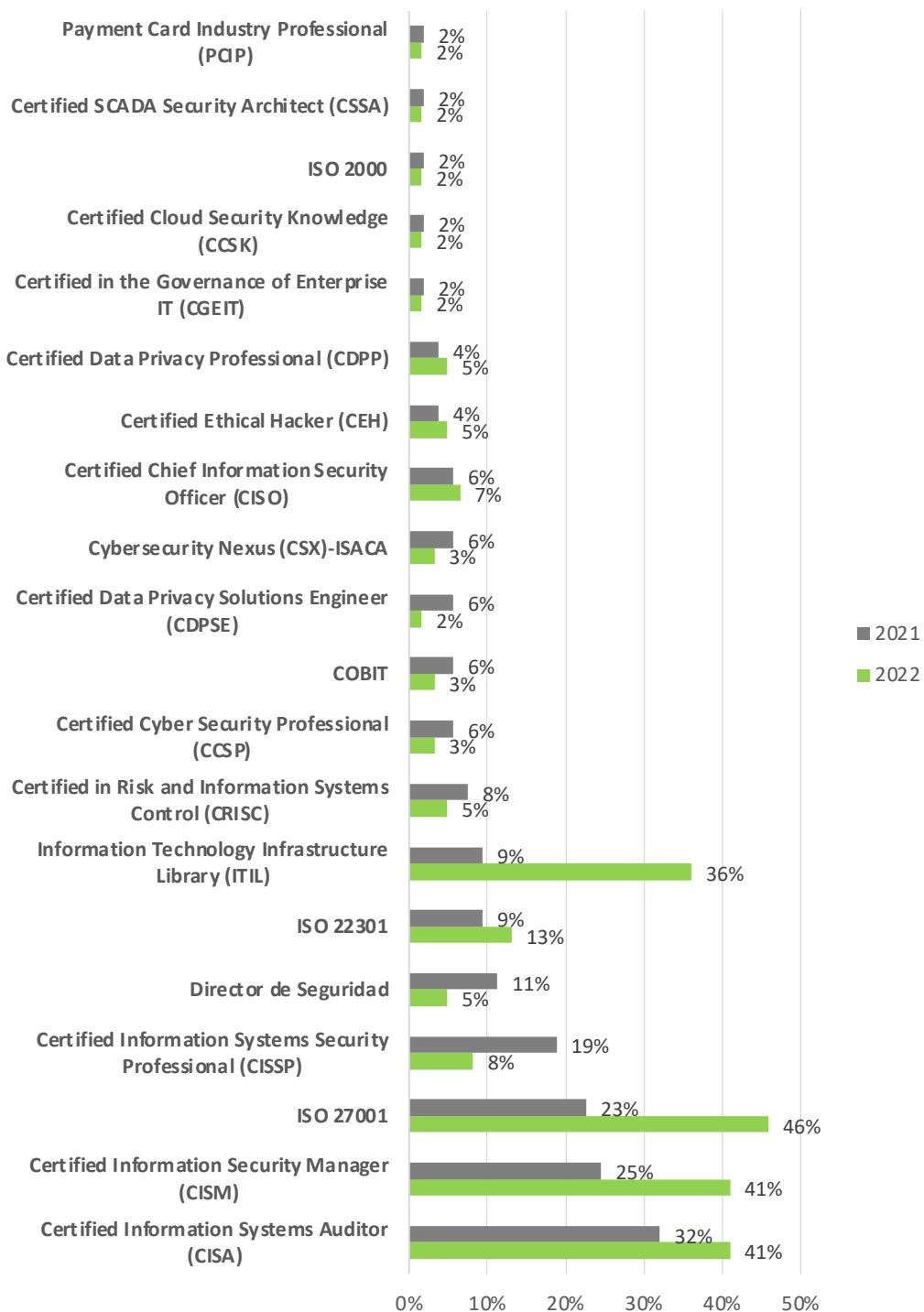
En cuanto a las certificaciones que poseen los CISO, puede observarse que existe una gran variedad de certificaciones de seguridad en el mercado.

En este sentido, las certificaciones más comunes que poseen los CISO, y al igual que ocurría en años anteriores, siguen siendo la ISO 27001, con un 23% de

aumento, CISA y CISM (ISACA), las cuales han aumentado un 16% y 9% respectivamente.

Entre las certificaciones que poseen los CISO, cabe destacar un aumento notable de la certificación ITIL, que ha aumentado un 27% respecto al año anterior.

Certificaciones/formación que poseen los CISO



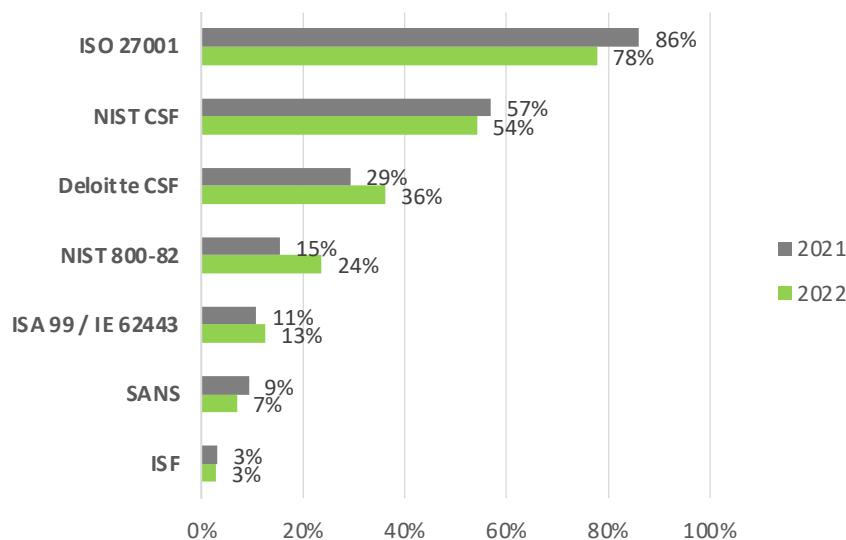
Frameworks que usan los CISO

Dentro de los frameworks que se usan como referencia para la mejora de los procesos de ciberseguridad, puede observarse cómo ISO 27001 sigue siendo el estándar de referencia, si bien ha visto reducido su liderazgo en un 8% respecto al año pasado.

Por el contrario, cabe destacar que la presencia de NIST sigue creciendo, con un aumento del 3%, así como el CSF de Deloitte, con un aumento del 7%, volviéndose a posicionar como uno de los principales frameworks del mercado.

El CSF de Deloitte vuelve a posicionarse como uno de los principales frameworks del mercado.

Framework de referencia en las compañías



Formación y concienciación en ciberseguridad

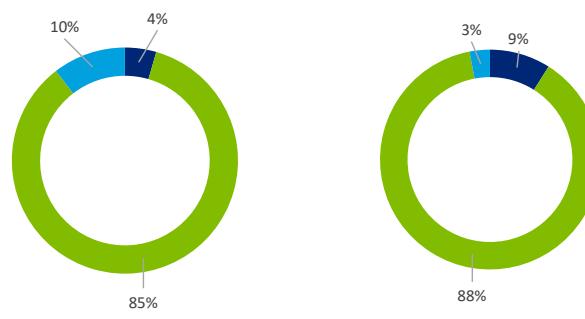
Respecto a las horas de formación y comparando con los resultados del año anterior, puede observarse cómo han crecido notablemente las horas impartidas por las compañías, aumentando de forma online casi un 30%, siendo el crecimiento del formato presencial de únicamente un 1%, lo cual refleja que las **compañías están concienciadas en seguir reforzando la formación de sus empleados** y son conscientes de que el factor humano es unos de los principales objetivos de actuación de los cibercriminales. Sin embargo, aún queda un largo camino por recorrer, debiéndose poner especial foco en la formación presencial.

Respecto a las horas de concienciación y comparando de nuevo los resultados entre este año y el anterior, al igual que ocurría con los resultados respecto a la formación, puede observarse cómo han crecido notablemente las horas impartidas por las compañías, aumentando el formato online un 36% y el

presencial un 6%, denotándose de nuevo y en paralelo a la formación la preocupación por la concienciación de las compañías.

Cabe destacar que la predilección de las compañías vuelve a ser la formación teórica, lo que significa que hay que seguir trabajando en reforzar los esfuerzos hacia la formación práctica.

Formación y concienciación en ciberseguridad



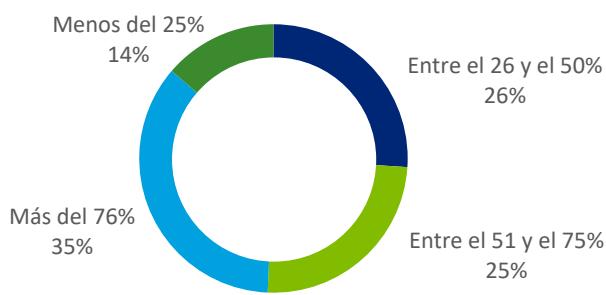
Módulo 05.

Revisiones de Seguridad

Revisiones de seguridad realizadas sobre aquellas aplicaciones consideradas críticas

Uno de los elementos claves en la seguridad de una compañía es la identificación de cuáles son aquellos dispositivos, recursos o equipos que son considerados críticos, teniendo en cuenta para ello la tipología de la información que contienen, los empleados que puedan tener acceso a la misma, o si se encuentra o no expuesta a Internet. Además, es necesaria la comprobación periódica de la protección de la información y esto se realiza a través de las revisiones de seguridad que lleve a cabo la compañía.

Porcentaje de aplicaciones consideradas críticas que son revisadas



Se puede observar cómo el rango porcentual mayor (35%) de las compañías analizadas en la muestra realizan revisiones de seguridad sobre más del 76% de las aplicaciones que identifican como críticas. Según el estudio, solo un 14% de la muestra analizada se limitaría a realizar simulaciones de seguridad únicamente en un cuarto de la totalidad de aplicaciones críticas que contemplan.

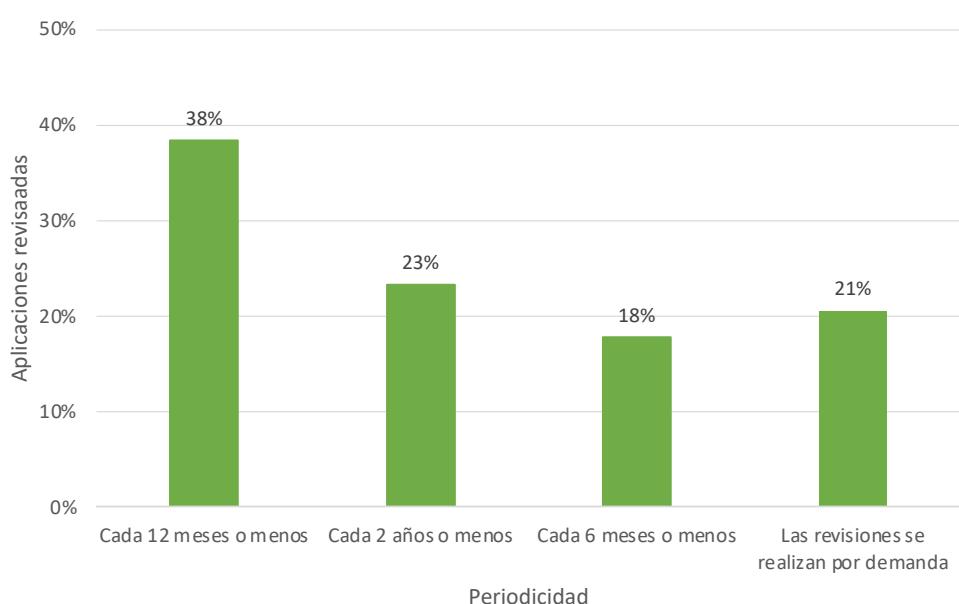
De esta forma, se puede afirmar que, en 2022, el año de este estudio, aproximadamente el 60% de la muestra de compañías analizadas revisa al menos la mitad del total de sus aplicaciones críticas, lo que indica que aún un 40% restante de las compañías analizadas continúan sin revisar la mitad de estas aplicaciones identificadas como críticas.

Periodicidad de las revisiones realizadas sobre las aplicaciones críticas en 2022

Revisar la seguridad aplicada sobre las aplicaciones críticas de una compañía es una de las buenas prácticas de seguridad recogidas por los distintos estándares internacionales de ciberseguridad. Sin embargo, es necesario que la periodicidad de estas revisiones no supere intervalos de tiempo que den lugar a un cambio muy amplio en el panorama de ciberseguridad de las compañías.

Una periodicidad anual es lo ideal para llevar a cabo este tipo de revisiones de seguridad, es decir, las compañías deberían realizar mínimo una revisión al año de sus aplicaciones críticas, siempre y cuando estas aplicaciones no sufran cambios. En caso de sufrirlos, además de la revisión anual es recomendable realizar una revisión tras el cambio producido en las mismas.

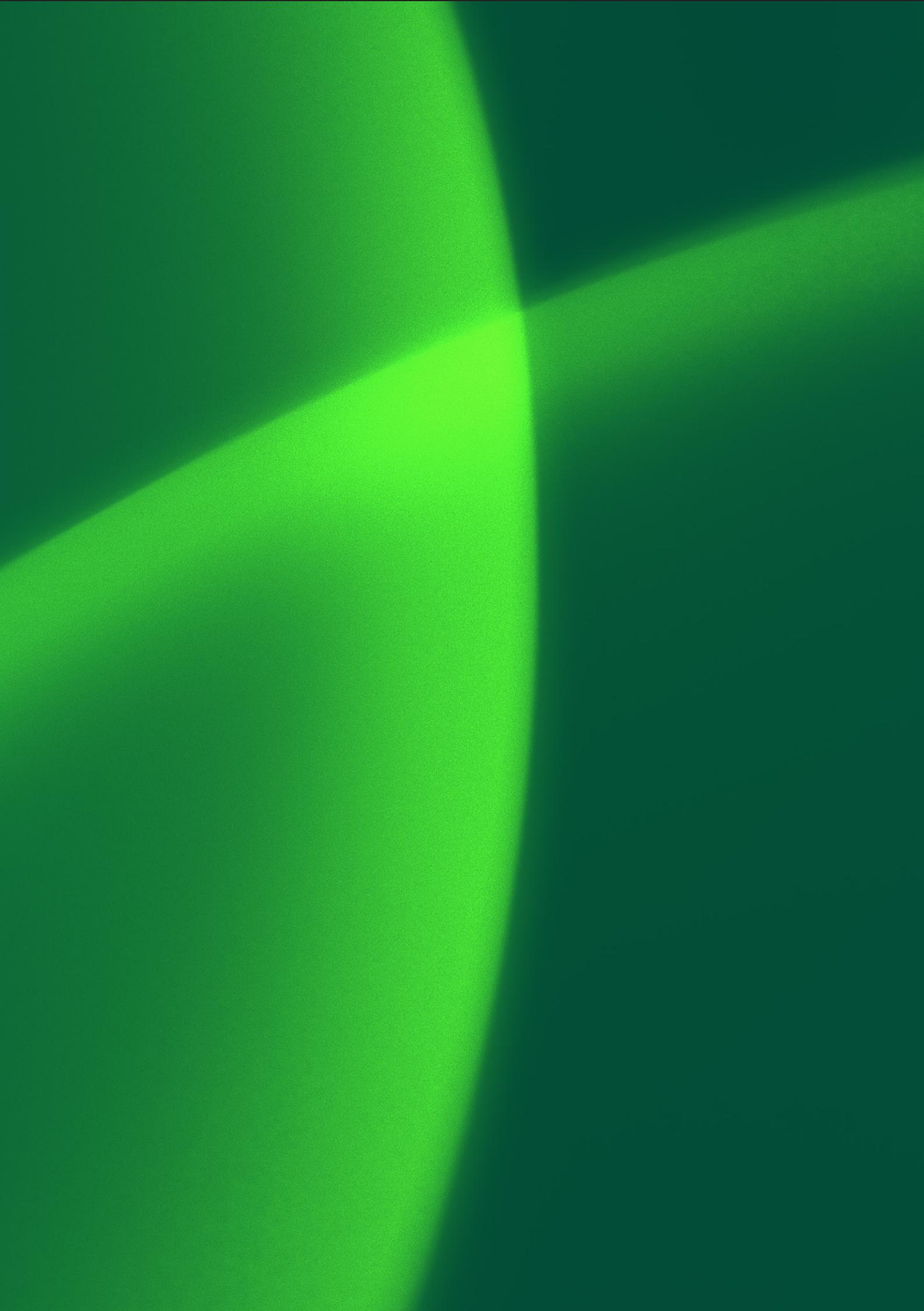
Periodicidad con la que las aplicaciones consideradas críticas son revisadas



Este año 2022, se observa cómo aproximadamente el 40% de las compañías analizadas siguen la práctica de realizar estas revisiones con una periodicidad anual. Sin embargo, este año puede también observarse un crecimiento con respecto a las revisiones bianuales, es decir aquellas que se realizan cada 2 años. Como comentábamos, este tipo de mayores periodicidades pueden dar lugar a cambios de panorama demasiado amplios y a una desactualización en las funcionalidades y la protección de las aplicaciones críticas de la compañía en cuestión.

Por otro lado, un año más continúa siendo preocupante el porcentaje que refleja que únicamente un 21% de las compañías realizan estas revisiones de seguridad bajo demanda.

Se observa un crecimiento en el porcentaje de compañías que realizan sus revisiones con una periodicidad bianual (cada 2 años). Sin embargo, continúa siendo mayoritario el porcentaje de compañías que realizan sus revisiones anualmente.



Módulo 06.

Entornos Cloud y tendencias
tecnológicas

Definición de una estrategia de seguridad en Cloud Computing en 2022 según la muestra de compañías analizadas

Actualmente, se está produciendo un aumento progresivo en el uso de herramientas y servicios Cloud en los distintos sectores de la industria. Por este motivo, las compañías comienzan a aumentar su nivel de concienciación relativo a la protección tanto de servicios contratados como de información exportada o compartida en la nube.

Siguiendo los resultados obtenidos en la muestra analizada, se puede observar cómo el 97% de las compañías contemplan servicios o aplicaciones Cloud externalizadas, frente a un 3% que prescinde de este tipo de servicios.

Esta tendencia deriva en resultados en los que se observa cómo la mayoría de las compañías de la muestra analizada, además de poseer este tipo de servicios, disponen de estrategias de seguridad definidas, donde se detallan los procedimientos de protección de sus recursos en la nube. Así, dentro de este 97% de compañías que disponen de dispositivos Cloud, el 75% de las mismas cuentan con una estrategia de seguridad relativa a Cloud Computing,

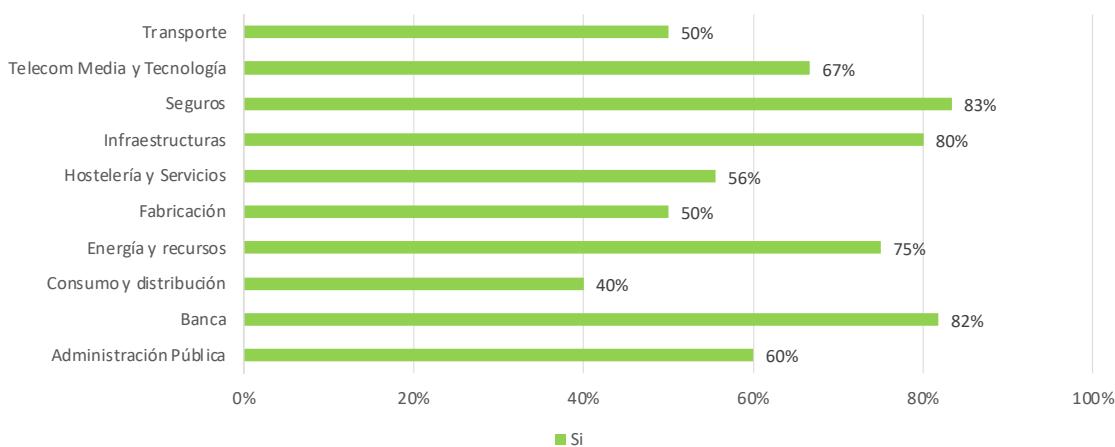
frente a únicamente un 25% de la muestra que no ha definido este tipo de directrices.

Sigue siendo preocupante que un 25% de las compañías que disponen de dispositivos Cloud no hayan hecho el ejercicio de definir una estrategia o metodología, de forma que se establezcan procesos de seguridad destinados a la protección de dichos dispositivos.

El 25% de las compañías con servicios contratados en la nube no cuentan con una estrategia de Cloud Computing definida.

Compañías que disponen de un marco de controles específico para Cloud Computing en 2022

Compañías que disponen de un marco de controles específico de Cloud Computing



A nivel sectorial, el sector Banca y el sector Seguros son los más avanzados, observándose cómo aproximadamente un 83% de las compañías pertenecientes a estos sectores disponen de un marco de controles definido, el cual contiene medidas específicas de seguridad en Cloud Computing.

En contraposición, se observa cómo en 2022 el sector más rezagado en la definición de un marco de control específico para los entornos Cloud es el de Consumo y Distribución, con un 40% de las compañías de este sector aún sin un marco de control Cloud definido.

Distribución de compañías en las que se contemplan medidas específicas de IoT

La tendencia hacia la inclusión de dispositivos IoT en las compañías es cada vez más notable, lo que deriva en la necesidad de definir controles específicos para la protección de este tipo de dispositivos, siendo este caso aplicable dentro del ámbito de Cloud Computing.

En los resultados obtenidos en el análisis de la muestra, se ha registrado cómo en 2022 el 71% de las compañías analizadas disponen de dispositivos IoT y cómo dentro de este porcentaje, el 46% de estas compañías cuentan con medidas específicas de IoT definidas en su estrategia de Cloud. Sin embargo,

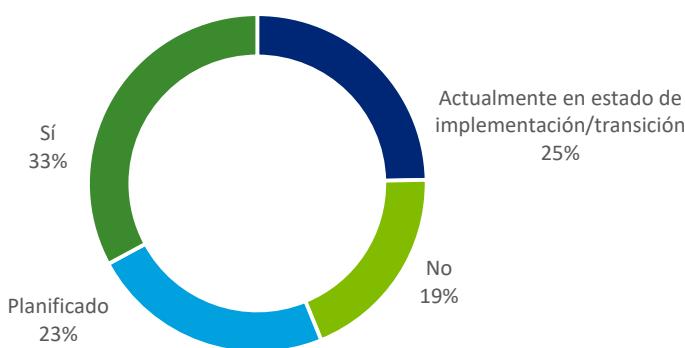
es preocupante que más de la mitad de las compañías que disponen de este tipo de dispositivos no incluyan controles específicos de seguridad en IoT.

Como punto a evolucionar, se observa cómo en 2021 un 67% de las compañías que disponían de servicios IoT contratados contaban con medidas de seguridad específicas definidas para este tipo de dispositivos, frente a un 46% en 2022, lo cual representa un aspecto que mejorar.

Distribución de compañías en las que se han implantado arquitecturas basadas en la tecnología Zero Trust

Las compañías optan, cada vez con mayor frecuencia, por obviar las soluciones que protegen el perímetro para pasar a desarrollar modelos de seguridad basados en tecnología Zero Trust, en los que los recursos y datos confidenciales estén seguros.

Porcentaje de implantación de arquitecturas de negocio basadas en Zero Trust



Analizando la muestra, observamos que únicamente el 33% de las compañías han implantado arquitecturas basadas en Zero Trust, mientras que el 19% no las ha implantado. Las compañías restantes se encuentran o bien en proceso de implementación/transición a este tipo de arquitecturas (25%) o bien tienen planificada esta implantación (23%).

El sector más avanzado en la implantación de este tipo de arquitecturas es el de Telecomunicaciones, Media y Tecnología, contando con el mayor porcentaje de compañías con arquitecturas de negocio basadas en Zero Trust implantadas (67%).

El sector de Consumo y Distribución actualmente registra un menor avance en la implementación de este tipo de arquitecturas; únicamente un 10% de las compañías analizadas disponen de este tipo de arquitecturas. Sin embargo, cabe destacar que este sector cuenta con porcentajes altos de proyectos de implantación planificados o actualmente en estado de implementación.

El 75% de las compañías analizadas en 2022 que disponen de servicios o aplicaciones Cloud contratadas han definido su estrategia de Cloud Computing. Los sectores de Banca y Seguros son los más avanzados en la definición de este tipo de estrategias de seguridad destinadas a la protección de sus recursos en la nube.



Módulo 07.

Incidentes de seguridad

Incidentes de ciberseguridad con consecuencias significativas producidos en las compañías analizadas en 2022

Uno de los indicadores clave para poder comprobar el nivel de madurez de una compañía en ciberseguridad son los incidentes sufridos. Este indicador es, además, al que más atención se le presta debido a las consecuencias que conlleva. Estas consecuencias pueden ser económicas, de pérdida o difusión de datos sensibles e información de clientes, pérdida de control de dispositivos o equipos, suplantación de identidad, etc.

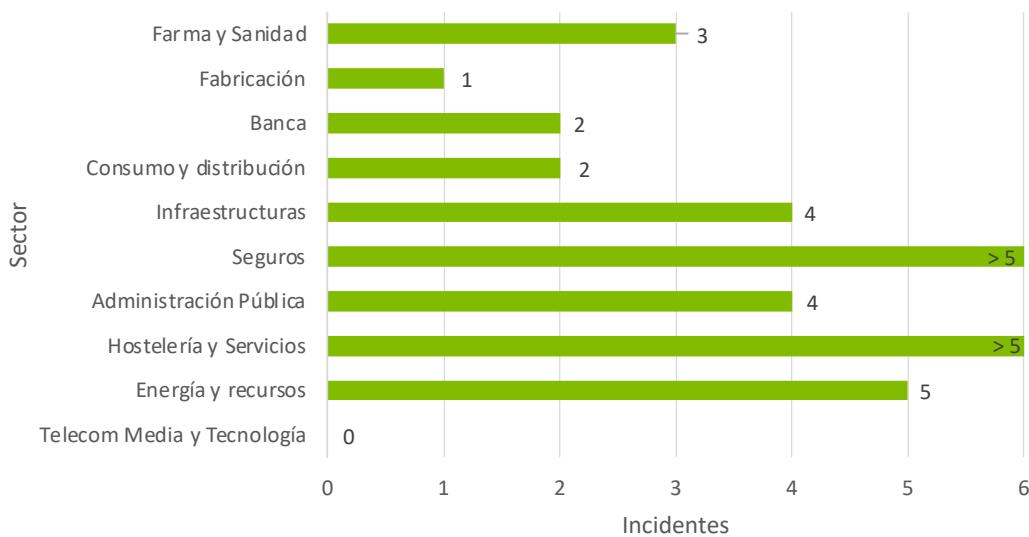
Inevitablemente, este indicador referente a incidentes de seguridad es el más utilizado en las distintas comparativas realizadas en cualquier estudio de ciberseguridad, puesto que aporta una visión general de las compañías analizadas a nivel de madurez de la seguridad implementada.

Este dato da pie a entender no solo los procesos de detección de incidentes con los que puede contar una compañía, sino también los mecanismos relativos a la clasificación, mitigación, respuesta y actuación ante incidentes de una compañía. Por otro lado, contribuye a identificar la eficacia de los mismo y las posibles oportunidades de mejora.

El criterio para definir si un incidente es crítico o no es propio de cada compañía, ya que el nivel de criticidad de una compañía de gran tamaño y alto nivel de madurez no es comparable con la criticidad o el impacto que pueda ocasionar un incidente en una organización de menor tamaño y robustez en términos de seguridad. Es decir, cuando en este estudio se hable de incidentes críticos o con consecuencias significativas, se referirá a lo establecido según la muestra de compañías analizada y su criterio.

En este año 2022, la media de incidentes sufridos en las compañías ha disminuido notablemente, lo que nos indica que tanto el tamaño de las compañías como la robustez de sus medidas de seguridad es mayor, y con ello un nivel de madurez en ciberseguridad más alto que el observado en la muestra de 2021.

Número de incidentes de ciberseguridad significativos ocurridos por sector



Dado que hablamos de incidentes cuyo impacto es lo suficientemente grande como para considerarlos significativos, no es de extrañar que el sector que más incidentes haya sufrido a lo largo de 2022 sea el de Hostelería y Servicios. Esto es debido a que las compañías de este sector cuentan con una madurez y una presión regulatoria en ciberseguridad menor que otros sectores. Concretamente, los estándares aplicados a este sector no se extienden más allá de PCI y DSS, lo cual deriva en procesos de seguridad más ad hoc y en niveles inferiores con respecto a otros sectores en la preparación ante a incidentes.

En contraposición, se sitúa el sector de Banca, donde la regulación de ciberseguridad es notablemente más extensa, así como la madurez de sus distintos procesos de seguridad, lo cual concuerda dado el carácter de los datos gestionados por este tipo de compañías, siendo en mayor porcentaje datos de carácter personal.

Por otro lado, cabe destacar que el sector Seguros, a pesar de tener una presión regulatoria similar a la de Banca, es el segundo con mayor número de incidentes significativos sufridos en 2022. Si bien la presión regulatoria es mayor, el sector Seguros cuenta con una madurez en ciberseguridad inferior al nivel de Banca, lo que implica que la preparación de las compañías pertenecientes al sector, así como sus capacidades de detección, respuesta o mitigación de

incidentes, sean ámbitos con margen de mejora.

Todo ello deriva en que sufrir un incidente pueda ocasionar un mayor impacto general en las aseguradoras y que, de los posibles incidentes recibidos, un mayor porcentaje pueda ser significativo para las compañías.

El sector de Hostelería y Servicios contempla el mayor porcentaje de incidentes sufridos con consecuencias significativas debido a un menor nivel de madurez en ciberseguridad y a una presión regulatoria menor.

Amenazas cuya ocurrencia a lo largo de 2022 es más significativa siguiendo la opinión de las compañías de los distintos sectores analizados

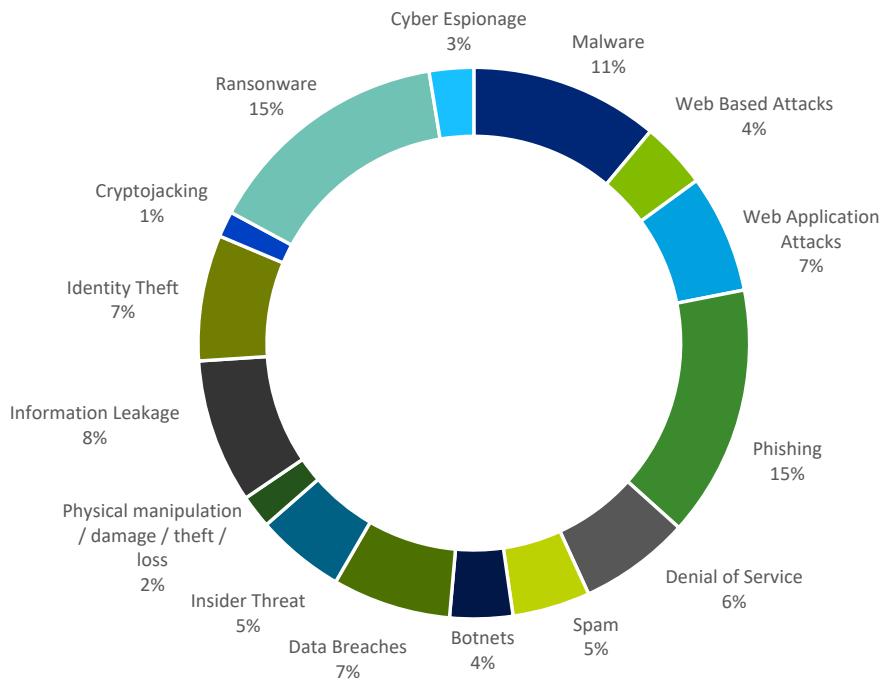
Al igual que hemos podido evidenciar el aumento del número de ciberataques que están sufriendo las organizaciones, hemos constatado un aumento de la sofisticación de las amenazas conocidas.

La tipología de amenazas puede ser muy variada: suplantación de identidad, pérdida o robo de datos de carácter personal, brechas de seguridad en equipos físicos, espionaje, etc.

Se debe tener en cuenta además que año tras año aparecen nuevas ciberamenazas que ponen en jaque al panorama de ciberseguridad mundial en busca de nuevas soluciones de mitigación. Por otro lado, las

técnicas de ataque son cada vez más novedosas y originales, y menos detectables y rastreables. Por este motivo, las compañías deben contar con el mayor nivel de madurez en ciberseguridad del que puedan disponer.

Porcentaje de ocurrencia de ciberamenazas en 2022



En vista a los resultados obtenidos, las tres amenazas principales este año, y al igual que ocurría en anteriores años, continúan siendo el ransomware, el malware y el phishing. Sin embargo, se observa un crecimiento general en los porcentajes del resto de amenazas contempladas en el estudio, contando con un crecimiento de hasta el 3% en el nivel de ocurrencia de web application attacks o botnets. De la misma manera, se observa cómo amenazas cuya ocurrencia era nula en años anteriores, en este 2022 aparecen por primera vez representativas. Un ejemplo de esto es el cryptojacking.

Los porcentajes de malware y phishing observan un decrecimiento del 3-4%, lo cual refleja una relativa sensación de tranquilidad en lo que respecta a aquellas amenazas identificadas tradicionalmente como las más habituales y a las que se les otorga un mayor foco de prevención en las compañías. Sin embargo, esto puede resultar contraproducente tanto para las nuevas amenazas contempladas como para las que ya ocurrían y han aumentado su porcentaje de ocurrencia, por lo que se debe prestar atención a las mismas, ya que en el estudio se comprueba que su grado de ocurrencia está aumentando en lugar de disminuir.

El top 3 amenazas habituales (ransomware, malware y phishing) sigue en cabeza; si bien destaca la nueva tendencia de diversificación de porcentajes de amenazas, apareciendo amenazas no contempladas hasta ahora (como cryptojacking), y siguen creciendo los porcentajes de amenazas hasta ahora minoritarias (web application attacks o botnets).

Porcentajes de contratación de ciberseguros por parte de las compañías en 2022 y datos de utilización de los ciberseguros contratados

La relación entre ciberincidentes y ciberseguros es lógica y evoluciona de manera proporcional, ya que cuantos más incidentes sufre una compañía, mayor es la contratación de ciberseguros.

Un ciberseguro es un concepto similar a un seguro financiero; se trata de un seguro cibernético, es decir, una forma de seguro para compañías e individuos contra los riesgos basados en Internet. De estos posibles riesgos, el más común o al que mayor importancia se le otorga es el de violación de datos.

Un ciberseguro trata de cubrir estos riesgos, generalmente incluyendo compensaciones económicas que pueden derivar de la violación de la seguridad de red de una compañía, el robo de propiedad intelectual o la pérdida de privacidad.

Dado el auge del riesgo en la ciberseguridad, el incremento del número de ataques sufridos por las compañías y la evolución en el impacto de estos en las compañías víctima, los ciberseguros se han convertido en una de las medidas de seguridad más utilizadas por las compañías durante los últimos años. De hecho, se observa una clara tendencia al alza en la contratación de ciberseguros.

Si este dato se desgrana aplicado a sectores según la muestra de este año, vemos cómo todas las industrias analizadas contemplan en mayor o menor medida la contratación de ciberseguros, lo que refleja la creciente concienciación de las compañías en la importancia de disponer de un ciberseguro. En este sentido, los sectores más avanzados en la contratación

de ciberseguros son, por un lado, Banca, y por otro, Energías y Recursos. Son los sectores, junto con Seguros y Hostelería y Servicios, que más dinero invierten en la contratación de ciberseguros, dado el elevado número de incidentes que sufren sus compañías a lo largo del año.

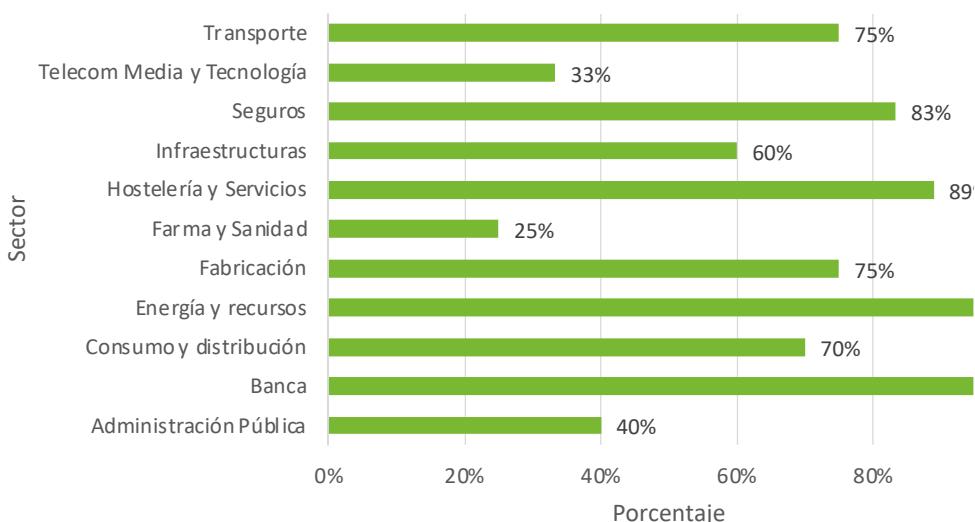
El sector más rezagado es el de Farmacia y Sanidad (dato que puede encontrarse sesgado debido a la poca muestra de compañías de este sector) seguido del sector de Telecomunicaciones, Media y Tecnología.

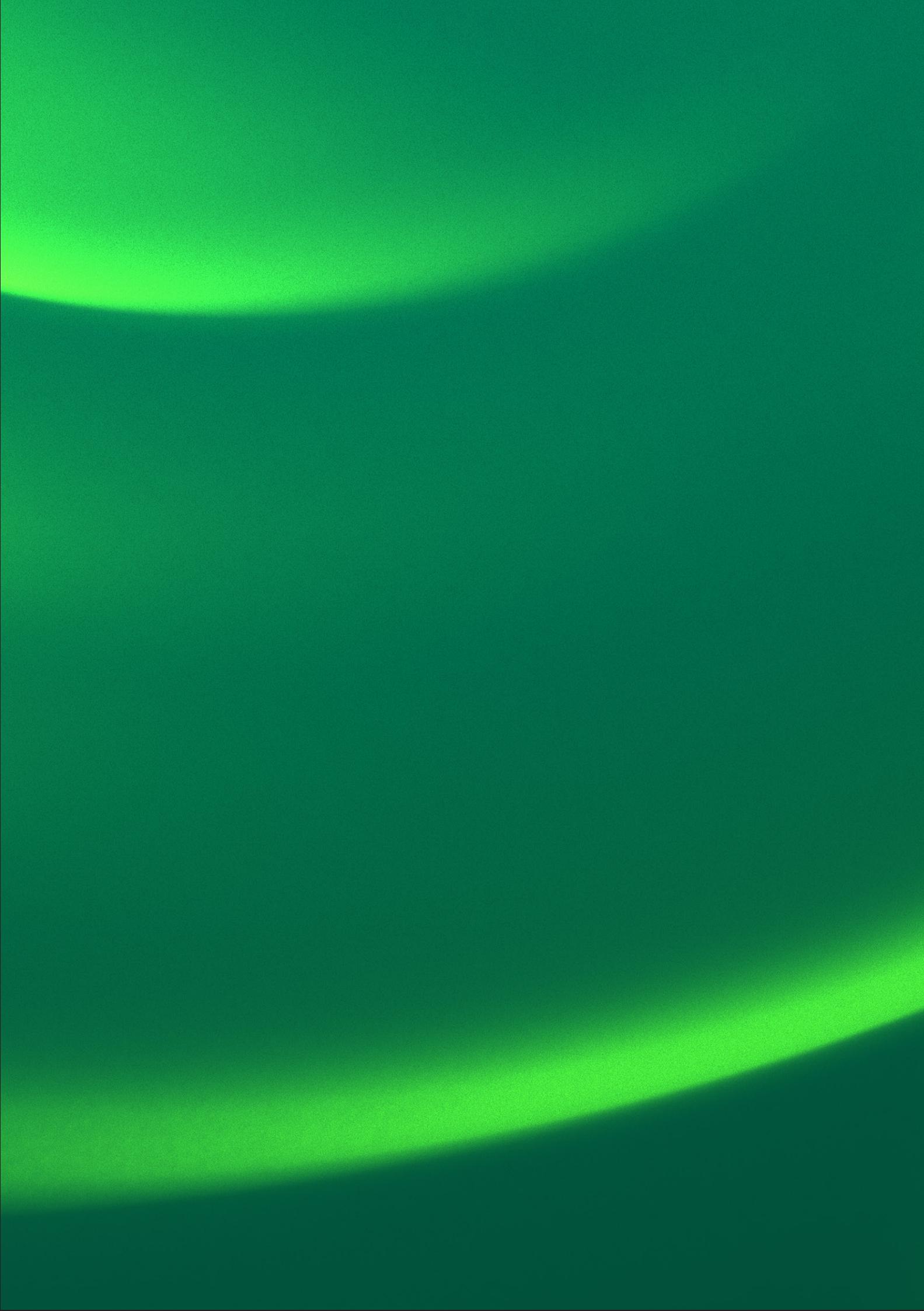
Este último dato concuerda con lo mencionado anteriormente sobre la relación entre la contratación de ciberseguros y el número de incidentes sufridos, ya que el sector de Telecomunicaciones es el que ha sufrido menos incidentes este año, por lo que es entendible que sea el que presenta un menor porcentaje en lo referente a la contratación de ciberseguros.

Cuanto mayor es el número de incidentes sufridos por una compañía a lo largo del año, mayor será el presupuesto invertido en la contratación de ciberseguros por parte de las distintas compañías.

Los sectores más punteros en la contratación de ciberseguros son Banca y Energía y Recursos, seguidos de Seguros y Hostelería y Servicios.

Porcentaje de contratación de ciberseguros en las compañías analizadas en 2022





Módulo 08.

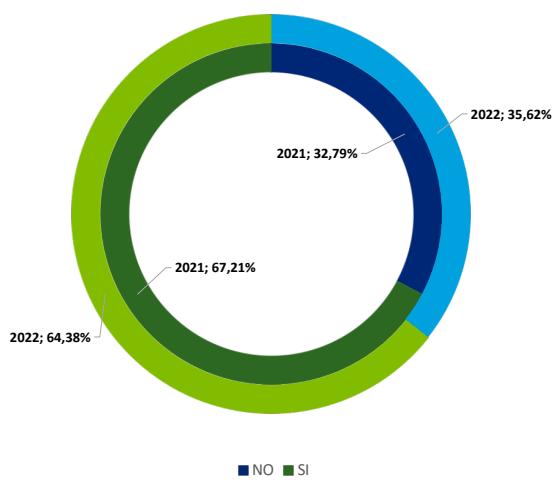
Simulaciones de cibercrisis

La manera óptima de comprobar si los recursos, las instalaciones o los procedimientos de respuesta de una compañía están preparados para sufrir una situación de crisis es la realización de simulaciones de seguridad que engloben este tipo de situaciones críticas, acercando a la compañía a un escenario de actuación real.

La protección es uno de los conceptos más importantes en el ámbito de la ciberseguridad. La protección proactiva consiste en disponer de mecanismos de defensa activos dentro de una compañía, los cuales permitan ejercitarse los distintos recursos para mantenerse alerta y estar preparados ante posibles amenazas, incidentes o brechas de seguridad que puedan provocar la caída de sistemas cuya funcionalidad es clave en la compañía.

Realización de simulaciones de cibercrisis y ciberincidentes en las compañías en 2022

¿Se llevan a cabo ejercicios de simulación en las compañías?



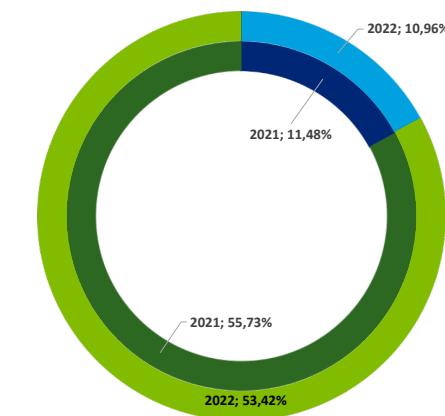
La manera óptima de comprobar si los recursos, las instalaciones o los procedimientos de respuesta de una compañía están preparados para sufrir una situación de crisis es la realización de simulaciones de seguridad que engloben este tipo de situaciones críticas, acercando a la compañía a un escenario de actuación real.

La protección es uno de los conceptos más importantes en el ámbito de la ciberseguridad. La protección proactiva consiste en disponer de mecanismos de defensa activos dentro de una compañía, los cuales permitan ejercitarse los distintos recursos para mantenerse alerta y estar preparados ante posibles amenazas, incidentes o brechas de

No solo se trata de un trabajo de simulación destinado a la preparación de recursos, sino que estas simulaciones permiten también elaborar distintos procesos de lecciones aprendidas e incluso integrar procesos relativos a CTI que permitan a los dispositivos y herramientas de las compañías aprender ante una crisis. Por otro lado, cabe destacar que hoy en día la realización de simulaciones de cibercrisis no se limita a ser únicamente una buena práctica de seguridad para las compañías, sino que también se trata en algunos casos de un proceso obligado por las distintas regulaciones dependiendo del sector de la industria analizada.

seguridad que puedan provocar la caída de sistemas cuya funcionalidad es clave en la compañía. No solo se trata de un trabajo de simulación destinado a la preparación de recursos, sino que estas simulaciones permiten también elaborar distintos procesos de lecciones aprendidas e incluso integrar procesos relativos a CTI que permitan a los dispositivos y herramientas de las compañías aprender ante una crisis. Por otro lado, cabe destacar que hoy en día la realización de simulaciones de cibercrisis no se limita a ser únicamente una buena práctica de seguridad para las compañías, sino que también se trata en algunos casos de un proceso obligado por las distintas regulaciones dependiendo del sector de la industria analizada.

Realización de simulaciones de crisis y ciberincidentes en 2022



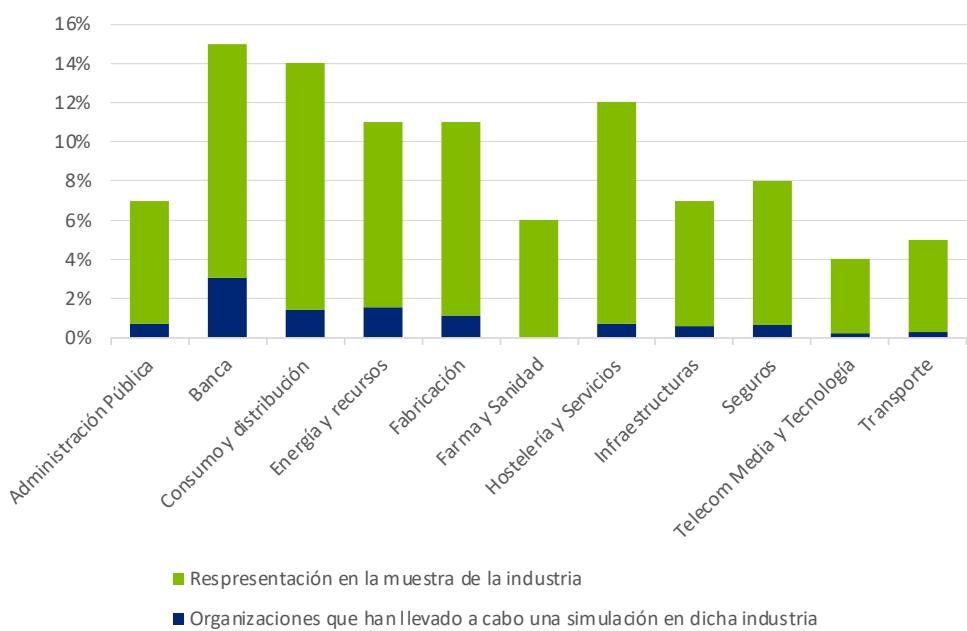
Dentro del 65% de las compañías que realizan simulaciones, podemos observar que un 83% realiza como mínimo una simulación de este tipo al año.

Cabe destacar que el 17% de las compañías cuentan no solo con la realización de al menos un ciberejercicio anual, sino que han desarrollado e implementado programas continuos de simulaciones ante ciberincidentes a lo largo del año.

Aproximadamente el 65% de las compañías analizadas realizan simulaciones de cibercrisis o ciberincidentes. Concretamente, un 83% de este porcentaje realiza mínimo un ejercicio anual, contando con un 17% restante que además cuenta con programas continuos de simulaciones.

Los sectores más avanzados en la realización de este tipo de simulaciones son los sectores de Banca, y Energía y Recursos. Como se puede apreciar a simple vista, las simulaciones no son una práctica habitual todavía, pese a ser de gran importancia para validar si la estrategia, táctica y operación en ciberseguridad de una organización responden a su situación real.

Porcentaje de simulaciones realizadas por sector

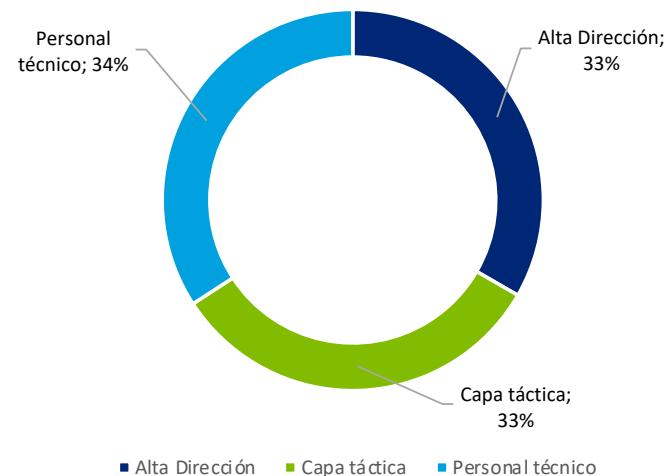


Tipo de simulaciones realizadas en las compañías en 2022 dependiendo del tipo de personal implicado

Si bien el hecho de realizar simulaciones de cibercrisis o ciberincidentes sobre los recursos de una compañía ya se considera en sí una buena práctica, es necesario que estas simulaciones contemplen un objetivo claro en lo referente a saber quién es el colectivo del personal a quien están destinadas.

Es importante que una compañía mantenga todas sus capas de personal preparadas, desde la capa más técnica hasta la capa de Alta Dirección. Es decir, las simulaciones han de abarcar aspectos de todo tipo de nivel, desde el nivel más técnico hasta el nivel más puro de gestión de procesos de seguridad. De esta manera, se mantendrá una homogeneidad en la preparación y en la capacidad de actuación de los empleados ante una situación de crisis.

Tipo de simulaciones de cibercrisis realizadas en 2022



Siguiendo los resultados obtenidos, el 34% de las simulaciones realizadas por las compañías van destinadas a la Alta Dirección. Así, se observa cómo los porcentajes de distribución de las simulaciones son bastante homogéneos, es decir, la cantidad de simulaciones que recibe la Alta Dirección es similar al porcentaje de simulaciones de seguridad llevadas a cabo tanto en la capa táctica como en el personal más técnico.

En comparación con 2021, se observa cómo este porcentaje de simulaciones orientadas a la Alta Dirección ha aumentado considerablemente, de un 25% a un 34%, lo cual aporta una distribución más homogénea de los porcentajes este año 2022.

El 33% de las simulaciones realizadas en esta muestra van destinadas a la Alta Dirección, siendo un porcentaje muy similar con respecto a aquellas simulaciones que van destinadas a la capa táctica y al personal técnico de las compañías en cuestión.

Las simulaciones de cibercrisis son una buena práctica, la cual se encuentra en tendencia creciente entre las compañías. Además, se observa una mayor homogeneidad porcentual en el tipo de simulaciones realizadas por las compañías dependiendo del colectivo del personal al que van destinadas.

Módulo 09.

Percepción del CISO

Preparación de las compañías para hacer frente a incidentes de seguridad

El 95% de las compañías afirman encontrarse “preparadas” para hacer frente a incidentes de ciberseguridad, un 9% más que en 2021.

Un año más, la sensación de ciberresiliencia se ha visto incrementada respecto a años anteriores. Cada año las organizaciones son más conscientes de la situación de su entorno, no solo en cuanto a la necesidad de estar preparadas para hacer frente a un incidente de seguridad, sino que además centran sus esfuerzos en trabajar para mitigar el impacto que este pueda tener en el negocio.

Porcentaje de preparación para hacer frente a incidentes de seguridad por sectores



Si profundizamos en el estudio a nivel sectorial, situamos tanto a Banca como a Telecomunicación, Media y Tecnología como los sectores más preparados. En el lado opuesto, encontramos sectores menos preparados, como Transportes, con tan solo un 25%, y a Consumo y Distribución, que a pesar de su subida de un 37% en comparación con los datos del año pasado, cuenta únicamente con la preparación de la mitad de sus compañías.

Debemos destacar que, al igual que el año pasado, el 100% de las compañías del sector de Banca afirman encontrarse preparadas.

Este esfuerzo realizado por el sector se debe en gran parte a ser uno de los más sometidos a la presión regulatoria. En este sentido, los cambios más recientes ocurrieron a finales de este último año con el desarrollo por parte de la Unión Europea de nuevas políticas de ciberseguridad y resiliencia, destacando las regulaciones de NIS2 y DORA.

Riesgos que generan mayor preocupación en las organizaciones

Por tercer año consecutivo, el 85% de los CISO categoriza la interrupción de las operaciones de

negocio como el riesgo que más preocupa a las compañías.

Riesgos que generan mayor preocupación en las organizaciones



Un año más, los CISO lo tienen claro: todo ciberataque que paralice el desarrollo del negocio es la mayor preocupación de las compañías, debido al impacto directo que estos tienen en el propio negocio. Adicionalmente y debido al momento en el que nos encontramos con la situación en Ucrania, la preocupación por el riesgo geopolítico ha subido cerca de un 50% en comparación con el año anterior. Debemos tener en cuenta que el panorama mundial actual tiene un impacto directo en la ciberseguridad y

resiliencia de las organizaciones, y esto se ve reflejado claramente en los resultados del estudio. Como podemos ver, la situación actual ha generado una gran inestabilidad en el campo de la ciberseguridad. Según datos facilitados por Check Point, el aumento de ciberataques en países pertenecientes a la OTAN ha sido realmente notable desde el inicio del conflicto en Ucrania, creciendo un 120% en comparación con años anteriores.

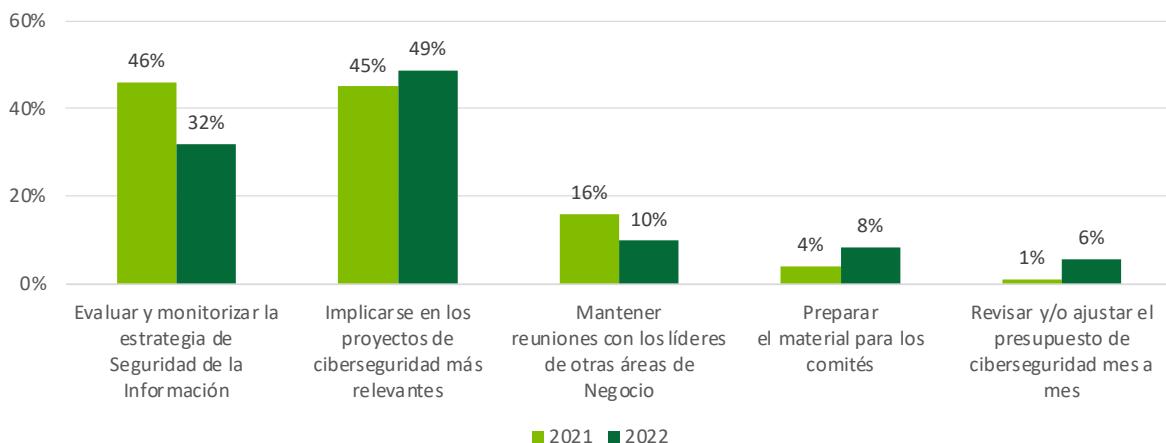
Tareas más importantes para los CISO

Este año, los CISO se han implicado aún más en los proyectos de ciberseguridad relevantes para las compañías.

Este año, la tarea que los CISO priorizan por encima del resto es su propia implicación en los proyectos de ciberseguridad más relevantes. La preocupación por

este tipo de tareas ha sufrido un incremento considerable en comparación con los resultados del estudio del año anterior, lo que ha llevado a dejar en segundo lugar en las agendas de los CISO la evaluación y monitorización de la estrategia de la seguridad de la información.

Tareas más importantes para los CISO

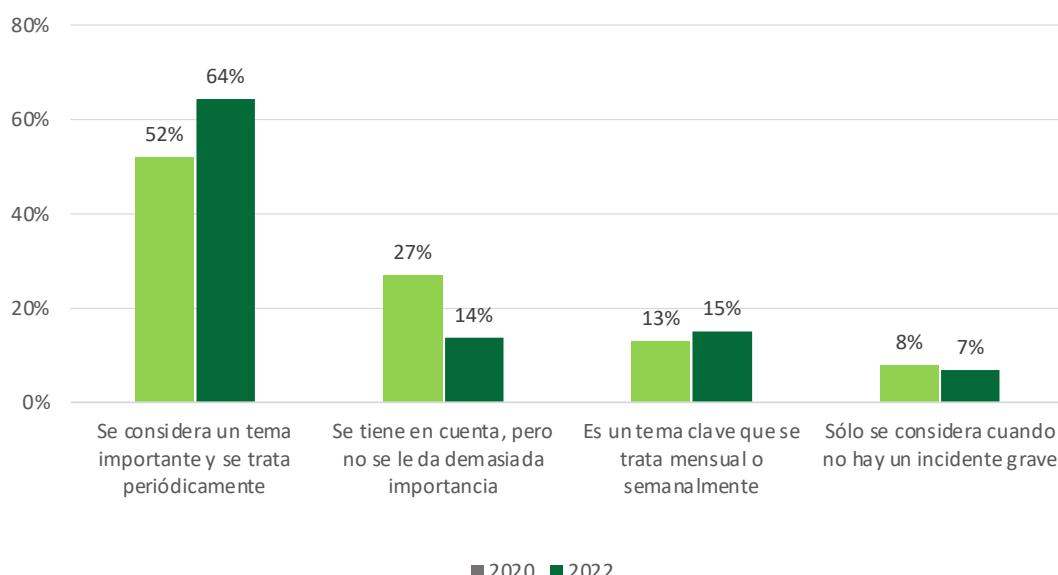


Grado de concienciación de la alta dirección en cuanto a la ciberseguridad en la compañía

La implicación de la Alta Dirección en materia de ciberseguridad es un factor clave, no solo para tener las capacidades necesarias para la mitigación de los riesgos que más preocupan a los CISO, sino también para lograr el nivel de ciberresilencia necesario en las organizaciones.

La Alta Dirección persiste en la concienciación en materia de seguridad.

¿Cuál es el grado de concienciación de la Alta Dirección en cuanto a la ciberseguridad en la compañía?



Mantener el nivel de concienciación en la Alta Dirección en los negocios no es una tarea fácil. A pesar de ello, no podemos acomodarnos en estas cifras, pues aún queda mucho trabajo por realizar por parte de las compañías. La implicación de la Alta Dirección en materia de ciberseguridad sigue siendo un factor decisivo para la protección de los negocios.

Así, mantener su apoyo es indispensable, tanto para la financiación como para la concienciación, y dar importancia a la seguridad debe ser una tarea prioritaria en todas las organizaciones.

Módulo 10.

Las preocupaciones del
CISO en tiempos de
teletrabajo

Preparación de las compañías para afrontar los riesgos de ciberseguridad que conlleva el teletrabajo

El teletrabajo permanece en las compañías y el 100% de las compañías afirman encontrarse "preparadas" ante los riesgos de ciberseguridad que ello conlleva.

Tras la pandemia vivida en el 2020, el teletrabajo ha llegado a los negocios para quedarse. La adopción y normalización de esta situación ha provocado un gran incremento en los ciberataques dirigidos directamente a los dispositivos de los empleados, pues la red del hogar supone una entrada mucho más factible para

los ciberdelincuentes. Por todo esto, un año más debemos preguntarnos si las compañías se encuentran preparadas para afrontar los riesgos que trae consigo el trabajo en remoto.

Si bien en el pasado año el 93% de las compañías afirmaban encontrarse "preparadas" para afrontar los riesgos del teletrabajo, los resultados de este año nos llevan a alcanzar el 100%, lo que supone una subida del 7% y un resultado prometedor para el futuro.

Variación del presupuesto destinado a ciberseguridad

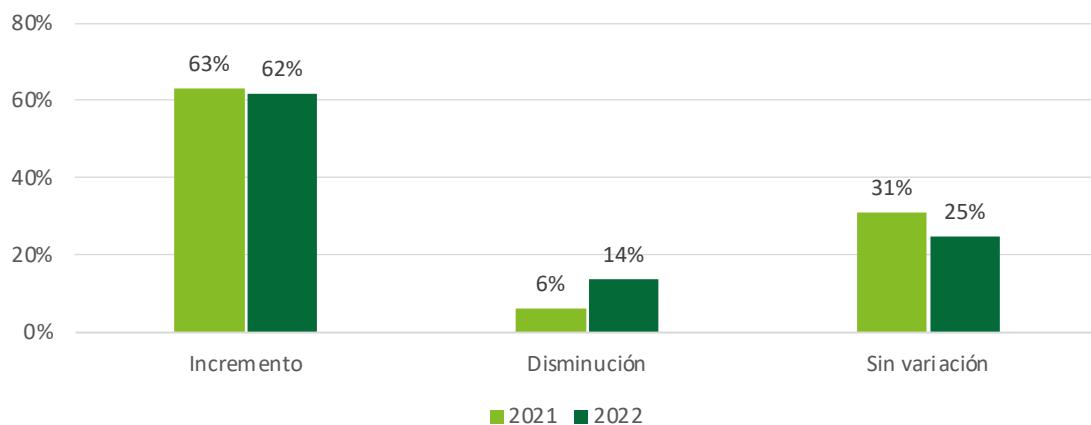
El 62% de las compañías destacan que sus presupuestos se han visto incrementados o se incrementarán a corto plazo.

El año pasado constatábamos que se **habían acabado los recortes presupuestarios en el área de la ciberseguridad, volviendo a la senda del incremento presupuestario periódico**.

Ahora bien, hemos podido evidenciar un pequeño frenazo tras el estudio realizado en un cierto segmento de las compañías, donde vemos cómo

casi un 8% de las compañías han tenido que disminuir su presupuesto anual de ciberseguridad (de las cuales, más del 6% no habían experimentado una variación en el mismo). Sin embargo, el dato no es malo, pues el **62% de las compañías destacan que sus presupuestos se han visto incrementados en el último año**, a pesar de que el actual panorama de inestabilidad es el factor más evidente que puede llevar a una bajada en los fondos que destinan las compañías al campo de la ciberseguridad.

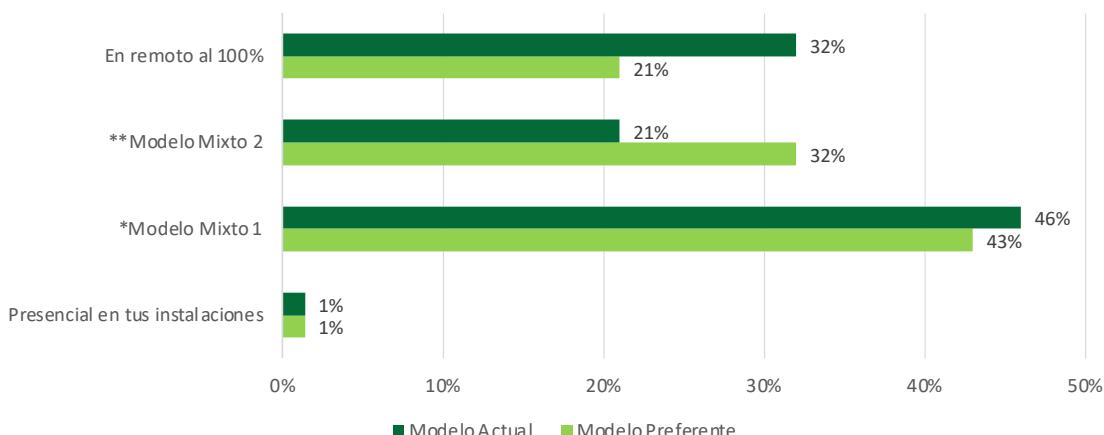
¿Considera que el presupuesto anual de ciberseguridad se ha visto variado o prevé que se vaya a variar debido a la situación actual?



Modalidad de trabajo de los proveedores de servicios de ciberseguridad y modelo preferente del CISO

Un año más, casi el 100% de las compañías se decantan por el modelo de trabajo remoto o híbrido.

¿Cuál es la modalidad de trabajo actual de sus proveedores de ciberseguridad y cuál es el modelo preferente?



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

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

Como hemos visto en los últimos tiempos, el teletrabajo ya es una realidad normalizada e intrínseca en nuestra sociedad. Este año, el 99% de las compañías han afirmado decantarse por este modelo de trabajo, ya sea en modo completamente remoto o de manera híbrida.

Este modelo híbrido proporciona beneficios no solo para los trabajadores, ya que les permite tener un horario y una vida laboral mucho más flexible, sino que también proporciona un ahorro a las compañías,

de forma que reducen el número de empleados que trabajan en sus propias instalaciones. Este es un factor clave para que el modelo conocido como Mixto 1, el cual consiste en un modelo presencial en las instalaciones del proveedor y en remoto en las oficinas de la propia compañía, siga siendo tanto el prioritario como el preferido por los CISO.



Principales conclusiones del estudio

Módulo 01. Headcount y SOC

En lo que respecta al personal de los departamentos de ciberseguridad, destaca que el 80% de las organizaciones consideran estar infradotadas, opinión reforzada por los resultados del estudio, en el que el 50% de las organizaciones estudiadas tienen menos de 10 personas dedicadas en exclusiva a la ciberseguridad. Como consecuencia de esta situación, el 50% de las organizaciones tienen un nivel de externalización de más del 50%.

Por otra parte, con respecto al servicio de SOC/CSIRT, es destacable que un 21% de las organizaciones no lo poseen.

Módulo 02. Presupuesto y servicios

La capacidad presupuestaria continúa este año la tendencia de los años anteriores y sigue alineada con las tendencias actuales de relación entre presupuesto en ciberseguridad y en IT. Los sectores que destacan a este respecto son Banca, Energía y Recursos, Farmacia y Sanidad, y Seguros. Por el contrario, Consumo y Distribución destaca como el sector que tiene los presupuestos más bajos, de menos de 500.000€.

Como en años anteriores, el rango de sueldo anual del CISO se mantiene en 80.000-120.000€, aunque sigue habiendo un 16% de CISO que cobran menos de 60.000€ anuales, lo cual no se corresponde con las responsabilidades del puesto.

Módulo 03. Estrategia y modelo operativo

Dentro de la estrategia de ciberseguridad de las compañías, destaca en los datos de este año que un 14% de las compañías no han realizado aún un alineamiento para ver cómo cubre la ciberseguridad las necesidades del negocio, lo que nos indica que debemos seguir trabajando conjuntamente para alinear ambos mundos e ir de la mano.

En cuanto al modelo operativo, se puede observar una clara tendencia de cómo, en línea con años anteriores, predomina cada vez más la dependencia del CISO directamente del CIO y menos del CFO y CTO, destacando que el CISO participa un 5% más este año en el Comité de Dirección, hecho que refleja la preocupación de la Alta Dirección por la seguridad. No obstante, sigue existiendo un importante gap en este sentido, que se deberá trabajar en el corto-medio plazo.

Módulo 04. Certificaciones, framework y formación

Dentro de las certificaciones de las compañías, siguen decantándose por la ISO 27001 como la certificación de referencia en ciberseguridad, si bien sigue existiendo un alto porcentaje que no cuenta con ninguna certificación de ciberseguridad, con casi un 50% de las compañías sin contar aún con una, lo cual es un aspecto que se debe solventar. Destaca también cómo el CSF de Deloitte vuelve a posicionarse como uno de los principales frameworks del mercado.

Entre las certificaciones que poseen los CISO, y al igual que ocurrían en años anteriores, sigue siendo la ISO 27001 la más común, la cual ha aumentado un 23%, seguido de CISA y CISM, ambas respaldadas por ISACA.

En cuanto a formación y concienciación, la predilección de las compañías vuelve a ser la formación teórica, lo que implica que habrá que seguir trabajando en reforzar los esfuerzos de las compañías hacia la formación práctica.

Módulo 05.

Revisões de seguridad

Al igual que en 2021, el sector Banca vuelve a ser el más puntero en la industria en lo referente a la realización de revisiones de seguridad sobre sus aplicaciones críticas. Le sigue este año Consumo y Distribución como segundo sector más avanzado.

Se observa un crecimiento en el porcentaje de compañías que realizan sus revisiones con una periodicidad bianual (cada 2 años). Sin embargo, continúa siendo mayoritario el porcentaje de compañías que realizan sus revisiones anualmente.

Módulo 06.

Entornos Cloud y tendencias tecnológicas

El 92% de las compañías de la muestra analizada disponen de un servicio Cloud contratado. Dentro de este porcentaje, el 75% ha definido una estrategia Cloud. A su vez, de estas empresas analizadas que cuentan con servicios Cloud contratados y además definen su estrategia de Cloud Computing, el 83% cuenta con un marco definido de controles específicos para la nube.

El 25% de las compañías con servicios contratados en la nube no cuentan con una estrategia de Cloud Computing definida.

Del 75% de las compañías analizadas que disponen de servicios o aplicaciones Cloud contratadas, los sectores de Banca y Seguros son los más avanzados en la definición de este tipo de estrategias de seguridad destinadas a la protección de sus recursos en la nube.

Módulo 07.

Incidentes de seguridad

En 2022, la media de incidentes sufridos en las compañías ha disminuido notablemente, hecho que indica que tanto el tamaño de las compañías como la robustez de sus medidas de seguridad es mayor, lo que implica un nivel de madurez en ciberseguridad más alto que el observado en la muestra de 2021.

El sector Hostelería y Servicios contempla el mayor porcentaje de incidentes sufridos con consecuencias significativas. Esto se debe a su menor nivel de

madurez en ciberseguridad y a una presión regulatoria menor.

El top 3 de amenazas habituales (ransomware, malware y phishing) continúa siendo el mismo. Sin embargo, destaca la nueva tendencia de diversificación, con la aparición de amenazas no contempladas anteriormente en el panorama de muestras analizadas, como cryptojacking, y siguen creciendo los porcentajes de amenazas hasta ahora minoritarias (web application attacks o botnets).

Cuanto mayor sea el número de incidentes sufridos por una compañía a lo largo del año, mayor será el presupuesto invertido en la contratación de ciberseguros por parte de las distintas compañías. Los sectores más punteros en la contratación de ciberseguros son, por un lado, Banca, y por otro Energía y Recursos, seguidos de Seguros y Hostelería y Servicios.

Módulo 08.

Simulaciones de cibercrisis e incidentes

Aproximadamente, el 65% de las compañías analizadas realizan simulaciones de cibercrisis o ciberincidentes. Concretamente, un 83% de este porcentaje realiza mínimo un ejercicio anual, contando con un 17% restante que además cuenta con programas continuos de simulaciones.

El 33% de las simulaciones realizadas en esta muestra van destinadas a la Alta Dirección, siendo un porcentaje muy similar con respecto a aquellas simulaciones que van destinadas a la capa táctica y al personal técnico de las compañías en cuestión.

Las simulaciones de cibercrisis son una buena práctica en tendencia creciente entre las compañías. Además, se observa una mayor homogeneidad porcentual en el tipo de simulaciones realizadas por las compañías, dependiendo del colectivo del personal al que van dirigidas.

Módulo 09.

Percepción del CISO

En el estudio realizado este año, el 95% de las compañías afirman encontrarse “preparadas” para hacer frente a incidentes de ciberseguridad, un 9% más que en 2021. Además, por tercer año consecutivo, los CISO categorizan la interrupción de las operaciones de negocio como el riesgo que más preocupa a las compañías. Sin embargo, debemos destacar el aumento de un 50% en la preocupación por el riesgo geopolítico, debido principalmente a la situación en Ucrania, que impacta directamente en la ciberseguridad y resiliencia de las organizaciones.

Por otro lado, un año más, la Alta Dirección persiste en la concienciación en materia de seguridad, donde debemos tener en cuenta que los datos obtenidos se mantienen en las cifras del año pasado, por lo que no podemos acomodarnos en estas cifras y se refleja que aún queda mucho trabajo por realizar por parte de las compañías.

Módulo 10.

Las preocupaciones del CISO en tiempos de teletrabajo

El teletrabajo es una realidad normalizada e intrínseca en nuestra sociedad, y es por ello por lo que este año los resultados de nuestro estudio son prometedores, pues el 100% de las compañías afirman encontrarse “preparadas” ante los riesgos de ciberseguridad que esto conlleva.

Trabajar desde casa es un beneficio no solo para los trabajadores, sino que también proporciona un ahorro a las compañías, reduciendo el número de empleados que trabajan en sus propias instalaciones. Este es un factor clave, por el cual el modelo conocido como Mixto 1, el cual consiste en un modelo presencial en las instalaciones del proveedor y en remoto en las oficinas propias de la compañía, sigue siendo tanto el prioritario como el preferido por los CISO.

Contactos



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



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



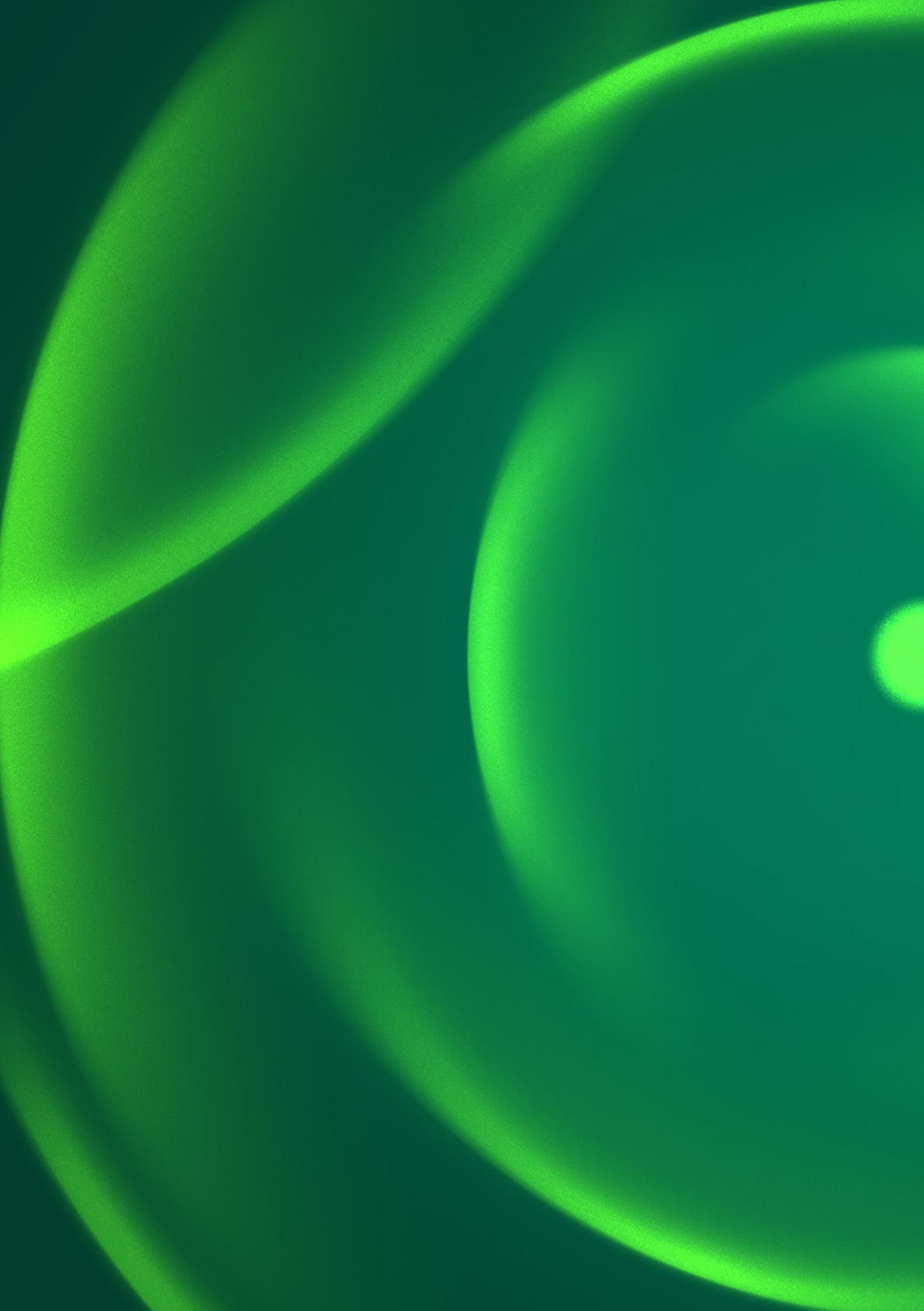
Gianluca D'Antonio
Socio Risk Advisory - Cyber
gdantonio@deloitte.es

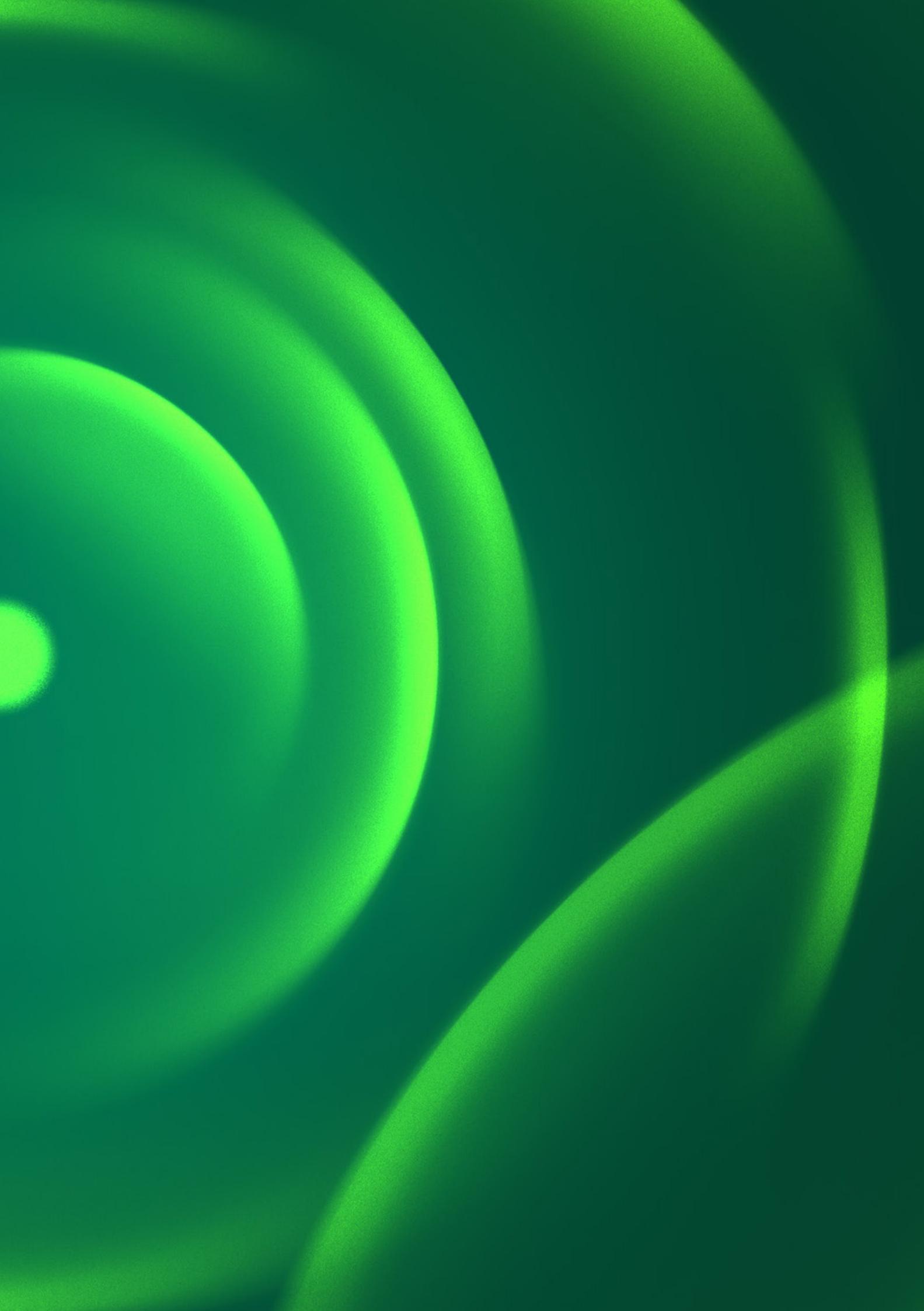


Alejandro Viana
Delivery Manager
Risk Advisory - Cyber
aviana@deloitte.es



Susana Mejido Castro
Delivery Lead
Risk Advisory - Cyber
smejido@deloitte.es





Deloitte.

Deloitte hace referencia, individual o conjuntamente, a Deloitte Touche Tohmatsu Limited («DTTL»), a su red global de firmas miembro y sus entidades vinculadas (conjuntamente, la «organización Deloitte»). DTTL (también denominada «Deloitte Global») y cada una de sus firmas miembro y entidades vinculadas son entidades jurídicamente separadas e independientes que no pueden obligarse ni vincularse entre sí frente a terceros. DTTL y cada una de sus firmas miembro y entidades vinculadas son responsables únicamente de sus propios actos y omisiones, y no de los de las demás. DTTL no presta servicios a clientes. Para obtener más información, consulte la página www.deloitte.com/about.

Deloitte presta los más avanzados servicios de auditoría y assurance, asesoramiento fiscal y legal, consultoría, asesoramiento financiero y sobre riesgos a casi el 90% de las empresas de Fortune Global 500® y a miles de empresas privadas. Nuestros profesionales ofrecen resultados cuantificables y duraderos que contribuyen a reforzar la confianza de la sociedad en los mercados de capital, permiten que los negocios de nuestros clientes se transformen y prosperen, y lideran el camino hacia una economía más sólida, una sociedad más justa y un mundo sostenible. Con una trayectoria de más de 175 años, Deloitte está presente en más de 150 países y territorios. Para obtener información sobre el modo en que los cerca de 415.000 profesionales de Deloitte de todo el mundo crean un verdadero impacto, visite la página www.deloitte.com.

Esta publicación contiene exclusivamente información de carácter general, y ni Deloitte Touche Tohmatsu Limited («DTTL»), ni su red global de firmas miembro o sus entidades vinculadas (conjuntamente, la «organización Deloitte») pretenden, por medio de esta publicación, prestar un servicio o asesoramiento profesional. Antes de tomar cualquier decisión o adoptar cualquier medida que pueda afectar a su situación financiera o a su negocio, debe consultar con un asesor profesional cualificado.

No se realiza ninguna declaración ni se ofrece garantía o compromiso alguno (ya sea explícito o implícito) en cuanto a la exactitud o integridad de la información que consta en esta publicación, y ni DTTL, ni sus firmas miembro, entidades vinculadas, empleados o agentes serán responsables de las pérdidas o daños de cualquier clase originados directa o indirectamente en relación con las decisiones que tome una persona basándose en esta publicación. DTTL y cada una de sus firmas miembro, y sus entidades vinculadas, son entidades jurídicamente separadas e independientes.