Deloitte.

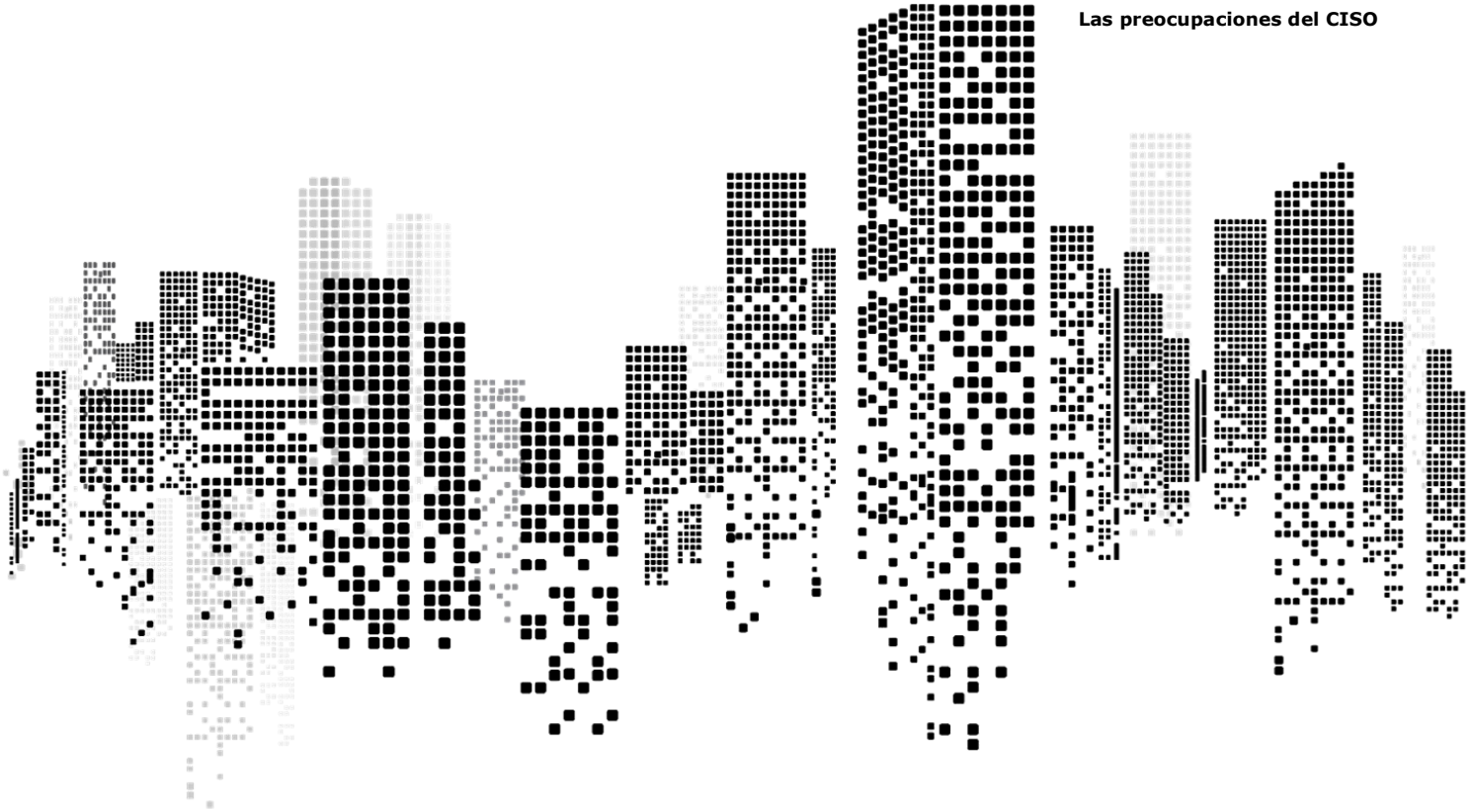
Los retos en ciberseguridad frente a los procesos de transformación

El estado de la ciberseguridad en el 2019

Cyber Strategy, Transformations and Assessment

Contenido

Introducción



Introducción

Este estudio es el resultado del trabajo realizado por el equipo de Cyber Strategy, Transformation and Assessment (CSTA) de Deloitte en colaboración con los CISOs de las empresas que han participado en él.

Cyber Strategy, Transformation and Assessment, ¿Quiénes somos?

Somos un equipo especializado en consultoría estratégica de ciberseguridad. Nuestro liderazgo en el mercado radica en el amplio equipo de perfiles multidisciplinares, el perfecto equilibrio entre el conocimiento técnico y estratégico, así como nuestra propia fuente de conocimiento. Gracias a ello, disponemos del know-how de sectores, tendencias, amenazas y ataques, fabricantes, niveles de madurez y controles en ciberseguridad, como consecuencia de la amplia experiencia adquirida en cientos de empresas a nivel nacional e internacional.

Motivación del presente estudio

El siguiente estudio comparte con la sociedad el estado de la ciberseguridad en las empresas españolas y qué retos tienen por delante en esta materia a tenor de los procesos de transforamción que dichas compañías están afrontando. Gracias a esta información, las empresas pueden conocer más de cerca como están dimensionadas y como están trabajando otras empresas en materia de ciberseguridad, en muchos casos a nivel sectorial.

Este estudio nace con la aspiración de poder resolver algunas dudas que son actualmente objeto de preocupación en materia de ciberseguridad y, para su análisis, se ha contado con la colaboración de los responsables de dicha materia dentro de las emrpresas: los CISOs.

En el proceso de toma de decisiones, sobre todo si estas tienen un carácter estratégico, es necesario no solo hacer un ejercicio de análisis interno de fortalezas y debilidades, sino también tener una referencia externa de cuáles son las tendencias y que están haciendo el resto de competidores para poder tener una base comparativa.

El equipo de Cyber Strategy, Transformation and Assessment de Deloitte ha realizado un ejercicio de entendimiento sobre una muestra de más de 50 empresas españolas y/o cuya base de operaciones de seguridad reside en España.

"La estrategia del presente para gobernar las amenazas del futuro"

Contenido

A continuación, se analizarán las principales conclusiones sobre la información obtenida y analizada en el estudio.

Estas cuestiones están divididas en 7 temas, los cuales son frecuentemente preocupaciones que suelen trasladar los CISO en diferentes foros:

1. Headcount y SOC

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 y evolucionar de forma continua sus centros de operaciones y respuesta.

2. Presupuesto y servicios

Sin lugar a dudas, este sigue siendo un reto continuo para los CISOs que demandan mayores presupuestos, pero a su vez es necesaria la optimización de dichos recursos. Una estrategia que empiezan a implementar muchos CISOs radica en concienciar a la alta dirección para que perciban los servicios bajo su responsabilidad como una inversión o ahorro de costes (evitando ciberincidentes) y no solo como un gasto para el negocio.

3. Modelo operativo y políticas

La definición de un modelo operativo eficiente y el cumplimiento de políticas (no solo a nivel nacional), ayudan a los CISOs a optimizar el personal dedicado a seguridad y los presupuestos asignados.

4. 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 del mercado. Estas, a su vez, evidencian de forma objetiva la consecución de niveles de madurez por materias específicas de ciberseguridad para ambos. Que certificaciones y frameworks abordar suele ser objeto de debate y discusión entre los diferentes CISOs, al no haber un verdadero consenso sobre cuáles deben ser estos.

5. Revisiones de seguridad, entornos cloud y tendencias tecnológicas

Bajo esta agrupación temática se analizan las principales cuestiones que suelen estar en los últimos artículos y congresos de ciberseguridad. Se recoge información sobre las revisiones de seguridad realizadas en entornos críticos, el uso de infraestructuras en la nube y cuál es el uso real que se está haciendo de tendencias tecnológicas como son IoT, blockchain, *machine learning*, etc.

6. Incidentes de seguridad

Sin lugar a duda, una de las grandes preocupaciones de los CISO es cuándo recibirá el siguiente ciberataque o sufrirá un ciberincidente. Para facilitar una respuesta, se analizará cuáles son las estadísticas de incidentes en los últimos años de diferentes empresas y que papel jugó el ciberseguro para, de esta manera, tener una referencia comparativa del mismo.

7. Percepción del CISO

Una vez analizados datos cuantificables y objetivos sobre el estado de la ciberseguridad en las empresas, es necesario conocer que es lo que percibe el CISO, que es lo que realmente piensa sobre las tareas que realiza, las que debería realizar, sobre cómo de concienciada está su dirección y cómo de seguro se siente ante el próximo ciberataque al que tendrá que enfrentarse su compañía.

Principales conclusiones del estudio

Principales conclusiones del estudio

Headcount y SOC

- Tendencia clara a la externalización y concentración de funciones por terceros.

  La mayoría de la plantilla de ciberseguridad en las empresas es personal externo, siendo este el 100% en algunos casos. Se observa una tendencia elevada en la externalización del personal de ciberseguridad para ser más flexibles a la hora de afrontar cambios sin asumir costes fijos de personal y dar respuesta al entorno impredecible del mercado.

- Las empresas pequeñas-medianas son las que más se decantan por el ciberseguro.

  Cuando estas cuentan con menos de 10 empleados en ciberseguridad contratan en la mayoría de casos un ciberseguro. Es decir, las empresas con menor nivel de madurez de ciberseguridad intentan mitigar el impacto económico en caso de ciberincidente de esta forma.

- Menos dependencia de personal crítico en los sectores más regulados.

  En los sectores más regulados se ha hecho mayores esfuerzos en ciberseguridad y el porcentaje de empleados críticos es menor al tratarse de empresas más maduras y, por tanto, donde se ha sabido diversificar el riesgo de forma más efectiva.

- Solo el 33% de las empresas cuenta con la totalidad de su personal crítico como empleado interno.

  Las empresas siguen teniendo de forma general una elevada concentración de responsabilidades críticas en materia de ciberseguridad sobre personal externo. Esto genera una alta dependencia de proveedores clave.

- Aproximadamente la mitad de las empresas disponen de un SOC/CSIRT de forma externalizada.

  Debido a la complejidad y coste de disponer de un SOC/CSIRT propio, el 53% de las organizaciones optan por externalizar este servicio en proveedores especializados.

- Solo hay consenso sobre que funciones quedan dentro de la responsabilidad de un SOC/CSIRT en el caso del análisis de malware y análisis forense.

  El 51% de las empresas sí que incluyen la función de análisis de malware y análisis forense dentro de las funciones de su SOC/CSIRT. No obstante, el resto de funciones no siempre están incluidas. La capa de definición e implantación de políticas de ciberseguridad queda normalmente fuera, así como la propia respuesta ante incidentes.

Presupuestos y servicios

- El presupuesto medio en ciberseguridad es el 8,5% del presupuesto de IT/OT.

  Este dato es poco homogéneo porque hay empresas que disponen de un presupuesto mucho menor y otras que su presupuesto se eleva bastante por encima de esta media, al mismo tiempo, se observan importantes diferencias a nivel sectorial. Adicionalmente, si se consultan otras fuentes como estudios de Forrester, Gartner, etc. se aprecia como este dato sigue variando dependiendo de la muestra, la industria y la fuente.

- Existe una relación directa muy pronunciada que muestra como a mayor inversión en ciberseguridad menos ciberincidentes.

  A pesar de que este dato parece algo evidente, es de destacar como llega a verse variaciones de 5 veces más incidentes en unas empresas según la inversión en ciberseguridad. Las empresas que invierten más del 10% del presupuesto de IT/OT en ciberseguridad reportan 0,63 incidentes de seguridad al año de media, mientras que las que dedican menos del 10% experimentan 3,01 incidentes por año.

- Presupuestos elevados para la externalización de servicios y porcentaje elevado del presupuesto dedicado a la operación/mantenimiento, frente a los dedicados a la inversión.

  El presupuesto que se dedica de media a los servicios internos es del 27%, frente a los 73% de los externalizados. La tendencia dentro de ambos tipos de servicios (tanto internos, como externos) marca que el 30% se considera CAPEX y el 70% restante OPEX. Se considera una buena práctica seguir estos porcentajes.

- Las empresas deciden invertir mayor cantidad de ingresos en Protección (40,6%), después en Vigilancia (25,9%), y por último en Resiliencia (18,3%) y Gobierno (15,1%).

  Este dato va variando según las empresas alcanzan niveles más altos de madurez en ciberseguridad y también en los sectores más regulados donde se ve un incremento de las partidas presupuestarias para el área de gobierno.

Modelo operativo y políticas

- La mayoría de los CISOs quiere reportar a la dirección y sin embargo en casi todos los casos reportan al CIO.

  Casi el 80% de los CISOs consideran que debería reportar directamente a la alta dirección o al COO/CRO/Comité de Dirección, mientras que el presente estudio de Deloitte muestra que casi el 60% reportan al CIO. Esto refleja una gran disparidad entre el árbol de dependencia actual y el deseado.

- Aproximadamente en la mitad de las multinacionales existe la función de Local information Security Officer.

- La mayoría de las empresas opta por la centralización de su cuerpo normativo de seguridad.

  En el 77% de los casos existen políticas globales Corporativas de Ciberseguridad que han de ser cumplidas por todo el grupo.

  En el caso de empresas más pequeñas (el 33% restante) dichas políticas son de carácter local.

- La función holding/global de seguridad sigue sin estar financiada por cada país en la mayoría de los casos.

  Cabe destacar que en el 70% de los casos se ha observado que el resto de países del grupo empresarial no financian las funciones holding.

- La mayoría de las empresas opta por internalizar la función del DPO.

  En el 75% de los casos la figura del DPO es interna, por lo que se puede deducir que se le otorga la importancia necesaria a las políticas de gobierno del dato de carácter personal, frente al 15% que manifiesta disponer de un DPO externo.

- Normalmente en los comités más relacionados con la ciberseguridad los CISOs están representados en los mismos. El Comité de Dirección, a pesar de ser un aspiracional para muchos CISOs sigue estando fuera de su alcance competencial.

  El CISO tiene un rol activo en el Comité de Continuidad de Negocio en más del 70% de los casos en los que este comité existe.

  Solo 1 de cada 5 empresas encuestadas dispone de un comité específico para dar respuesta a incidentes de ciberseguridad.

Certificaciones, framework y formación

- La mayoría de las empresas siguen sin estar certificadas en la ISO 27001 y la ISO 22301.

  El 72,50% de los CISOs aseguraron que sus empresas no estaban certificadas ni en la ISO 27001 ni en la ISO 22301, ambos estándares relacionados con la seguridad de la información y la continuidad del negocio. Dentro del 72,50% cuya empresa no posee ninguna certificación de ciberseguridad más del 50% de los CISOs afirma que su organización está preparada o bastante preparada ante incidentes de seguridad. No obstante, hay que destacar que estas empresas son de un tamaño más reducido y cuentan con un nivel de madurez menor. Por ello, tienen menos concienciación en ciberseguridad, al mismo tiempo que, no son un objetivo frecuente de atacantes.

- Es habitual que las empresas estén certificadas al mismo tiempo en la ISO 27001 y en la ISO 22301.

  Por otro lado, el 66,67% de las empresas que poseen la ISO 22301, están certificadas también en la ISO 27001, lo cual demuestra que gran parte de las empresas cuando entran en procesos de certificación, tienden a optar a varias certificaciones en materia de Seguridad de la Información.

- La mayoría de los CISOs tienen al menos una certificación de seguridad y suelen optar por CISA, CISM y CISSP.

  El 75,00% de los CISOs encuestados posee al menos una certificación. Existe un patrón de certificaciones que vendría a cubrir su "carrera formativa" empezando por el CISA y CISM, para posteriormente acabar con el CISSP. Se puede observar como existen diferencias significativas entre las certificaciones del CISO y las de sus equipos. Mientras que los CISOs buscan certificaciones más enfocadas en las capas altas de gestión y liderazgo en ciberseguridad (como CISSP y CISM), sus equipos se certifican además en certificaciones más técnicas (como CCNA y CEH).

- La ISO 27001 se usa el doble de los que se usa la NIST CSF como marco de referencia en ciberseguridad, mientras que el Deloitte CSF alcanza una cuota del 18% del mercado.

  El 80% de las empresas utiliza la ISO 27001 como marco de referencia en ciberseguridad. Muy por debajo se encuentra la NIST CSF con un 37,50%. Cerca del 18% de las empresas utiliza el CSF (Cyber Strategy Framework) de Deloitte, el cual engloba los controles y requisitos establecidos por el resto de marcos (ISO, SANS, NIST, etc.). Por este motivo, indirectamente las empresas que utilizan el CSF de Deloitte están utilizando indirectamente el resto de marcos y los números de estos frameworks aumentarían.

- La formación en ciberseguridad a los empleados de la compañía sigue siendo una asignatura pendiente en la mitad de las compañías.

  El 50% de los encuestados no proporciona formación presencial a sus empleados y los que sí lo hacen el 65,00% apuesta por la formación online, puesto que permite mayor flexibilidad horaria a los empleados y puede abaratar los costes.

Revisiones de seguridad, entornos cloud y tendencias tecnológicas

- Las aplicaciones críticas son revisadas, al menos, anualmente, aunque sigue siendo insuficiente.

  Se observa que las aplicaciones críticas son revisadas, al menos, una vez al año en la mayoría de los casos. Los sectores que más realizan revisiones periódicas los sectores tecnológicos o con infraestructura OT como son el sector de las Telecomunicaciones, Media y Tecnología, Infraestructuras y el sector de Fabricación.

- Blockchain sigue siendo un ausente en casi todos los departamentos de ciberseguridad de las empresas.

  Se ha verificado que el 95% de los sectores tienen poca o ninguna implicación de la tecnología Blockchain en la ciberseguridad en su empresa.

- Solo el 30% de los sectores está apostando por la IA para potenciar su ciberseguridad.

  El 70% de los sectores cuenta con una implicación baja o muy baja de las tecnologías como Inteligencia Artificial, Machine Learning y Algoritmos Predictivos en la ciberseguridad.

- IoT, la tendencia tecnológica más implantada en las empresas.

  A diferencia de otras tecnologías más disruptivas, IoT sí que está presente en la estrategia de ciberseguridad de las empresas.

- El cloud computing, a pesar de su clara tendencia, aun no representa la opción prioritaria para las empresas para alojar su infraestructura e información, especialmente la crítica. Menos del 20% de los servicios que son imprescindibles/críticos para la empresa están alojados en la nube.

  Sólo el 10% de las empresas tiene más del 80% de su infraestructura en cloud, solo un 5% tiene entre el 60% y el 80% y un 20% de las empresas mantiene entre el 40% y el 60%.

Incidentes de seguridad

- Las grandes empresas son las que más ciberincidentes sufren, excepto las que son líderes en su sector, que son capaces de gestionar los ciberataques evitando que estos se transformen en ciberincidentes o crisis.

  Se ha comprobado que según las empresas van disponiendo de mayores ingresos, estas sufren mayores ciberataques, al ser un objetivo con mayor retorno/impacto para el atacante. No obstante, a partir de un punto elevado de ingresos (más de 5.000 millones de euros) estos descienden gracias a las medidas preventivas y una mayor inversión en ciberseguridad.

- Las empresas con entornos OT son la que más ciberincidentes reciben.

  Se ha verificado que los dos sectores con más incidencias son el de energía y recursos con un 41,67% y el de consumo y distribución con un 16,67% respecto al total de incidencias.

- Si tu empresa no cumple con la ISO 27001 y la ISO 22301 es probable que sufras un ciberincidente.

  Las empresas que no tienen ninguna certificación tienen un 72,22% de incidentes mientras que las que tienen la ISO 27001 tienen un 13,89%. La obtención de certificaciones de ciberseguridad no previene a la empresa ante ciberincidentes, pero estas sí que asientan las buenas prácticas que facilitan la obtención de niveles de madurez en ciberseguridad superiores.

- La gran mayoría de las empresas sufrieron un ciberincidente hace menos de 6 meses.

  El 76,19% de las empresas han tenido un incidente con consecuencias significativas en los últimos 6 meses, frente al 23,81% que han registrado el último incidente hace más de 6 meses.

  El 62,50% de las empresas han tenido menos incidencias en 2018 que en 2017, debido a la gran afectación de los ataques masivos lanzados ese año.

- Muy pocas empresas han hecho uso del ciberseguro, a pesar de la alta tasa de ciberincidentes.

  El 89% de las empresas que tienen un ciberseguro no lo han tenido que utilizar nunca y solamente el 10,71% de las empresas que tienen un ciberseguro han tenido que hacer uso del él en algún momento.

Percepción del CISO

- Los CISO siguen percibiendo que sus empresas están muy poco preparadas para hacer frente a un ciberincidente.

  Se puede concluir que 1 de cada 3 empresas se consideran que están poco o nada preparadas para hacer frente a un incidente de seguridad. Al mismo tiempo que, del 50% de las empresas energéticas y recursos se siente preparadas para afrontar un incidente de estas características. Por otro lado, el 86% del sector financiero sí se siente preparado ante un incidente. Lo cual es un claro reflejo de como a mayor nivel de madurez en ciberseguridad los CISOs se sienten más preparados.

- Las empresas energéticas y recursos están muy preocupadas ante incidentes que supongan una interrupción de sus operaciones.

  El 93% de las energéticas y recursos consideran la interrupción de las operaciones de negocio como su principal preocupación.

- Cuando la fuga de información es la principal preocupación de los CISOs suele haber un DPO interno.

  Los CISOS que consideran la fuga de información confidencial como primer o segundo riesgo tiene internalizado el DPO, exactamente en un 83% de los casos.

- Los CISOs consideran que lo más importante es estar involucrados en los proyectos más importantes. Al mismo tiempo se preocupan mucho por la estrategia y el negocio, a pesar de no estar en contacto constante con los responsables de estos.

  Se puede apreciar como contrasta que los CISOs a pesar de considerar la alineación de la estrategia de ciberseguridad con el negocio como uno de los aspectos más importante en el 64,1% de los casos, luego esto no se refleja en su agenda. Muchos de ellos a pesar de involucrarse en la estrategia, solo ponderan en su agenda las reuniones con otros líderes de negocio en el 15,79% de los casos como algo prioritario.

  El 95% de los CISOs considera que lo más importante en su agenda es estar involucrado en los proyectos más importantes de ciberseguridad.

- La alta dirección en el sector bancario está altamente concienciada en la ciberseguridad, mientras que el sector energético aún tiene un largo recorrido en este campo.

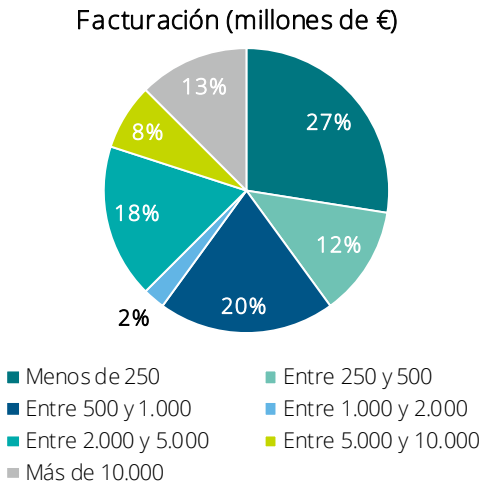
  El 100% en el sector Banca considera la ciberseguridad como un tema clave desde la alta dirección. Mientras que en el sector de Energía y Recursos esta cifra baja hasta el 25%, lo cual es un dato a mejorar debido al carácter crítico que representan estas infraestructuras para la estabilidad del país.


Muestra tomada
para el estudio

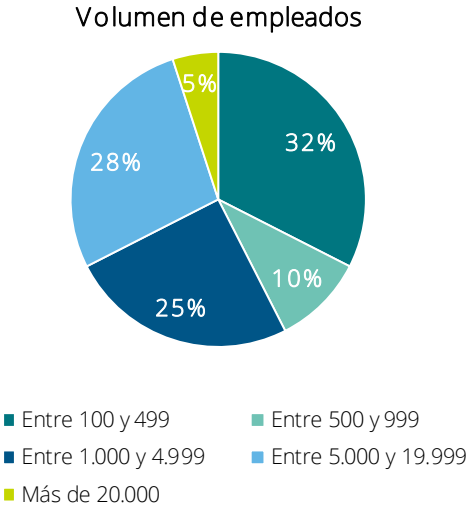
Muestra tomada para el estudio

Para ilustrar brevemente el perfilado de la muestra empleada en el presente estudio, se analizan los datos desde tres dimensiones fundamentales: facturación, número de empleados o "headcount" y sector en el que opera la empresa. Por sencillez y con fines estadísticos, se han diseñado horquillas de valores capaces de agrupar los datos de una manera comprensible y homogénea, como veremos a continuación.

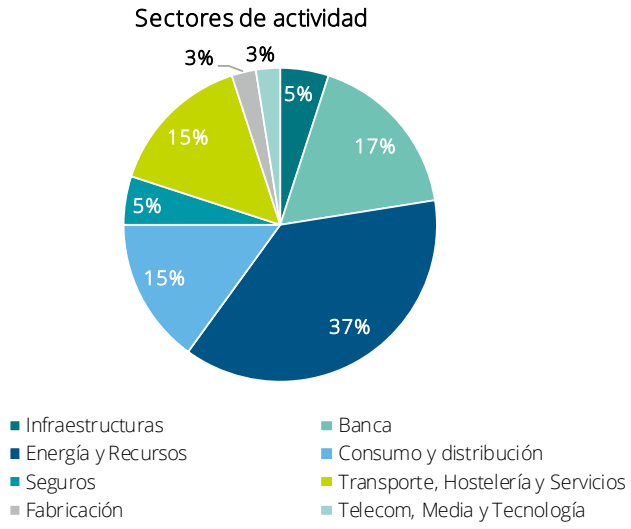
Facturación. Se puede apreciar que casi un 40% de las empresas encuestadas factura menos de 500 millones de euros, frente a un 40% que se mueve en la horquilla de los 500 hasta los 5.000 millones de euros de facturación anual. El resto de la muestra, **casi el 20%, son empresas con una facturación superior a los 5.000 millones**. Se observa que el segmento más numeroso es el de las empresas con facturaciones inferiores a 250 millones, y **una mediana de facturación anual que se sitúa en el segmento de las empresas con facturación entre 500 y 1.000 millones**.



Headcount. La segunda perspectiva es el **número de empleados** en plantilla que disponen las empresas. En esta perspectiva, podemos ver que un 32% de las empresas encuestadas tienen entre 100 y 499 empleados en plantilla, lo que rondaría la consideración de pyme en términos de empleados (250 empleados aproximadamente, según los criterios europeos). Un 35% de la muestra se sitúa entre los 500 y los 5.000 empleados y el 33% restante incluye aquellas empresas con más de 5.000 empleados en plantilla, siendo aquellas empresas con un volumen superior a 20.000 empleados muy residuales en la muestra, pues suponen solamente el 5% de la muestra total. Como en el caso anterior, **la mediana respecto al número de empleados se sitúa en las empresas que disponen de entre 1.000 y 5.000 empleados.**



Sectores. Por volumen de empresas son, en orden descendente: Energía y Recursos, con un 37% de las empresas, Banca, con el 17% de los datos de la muestra y Consumo y distribución y Transporte, Hostelería y Servicios, ambos con un 15%. El resto de sectores en conjunto suponen un 16% del total de las empresas representadas.



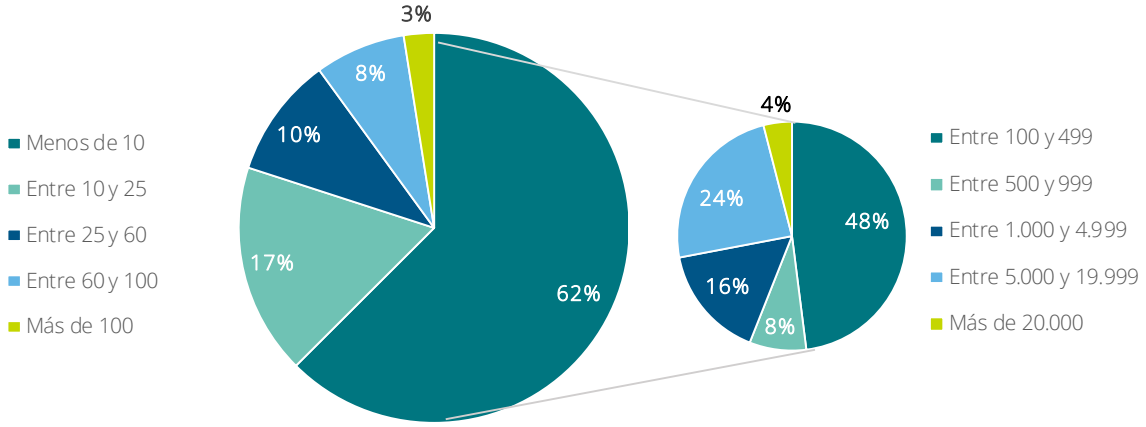
Principales conclusiones del estudio

El estudio en detalle

Headcount y SOC

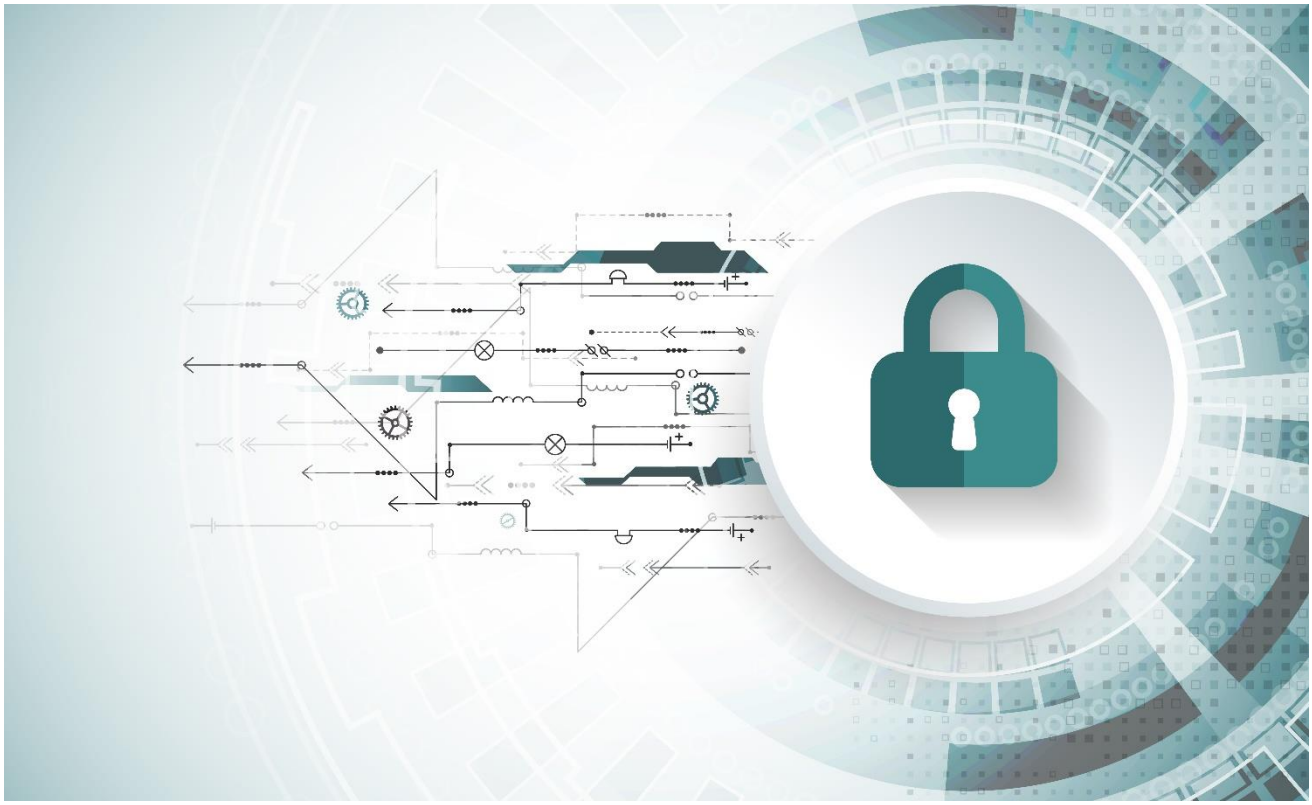
¿Cuál es el número de empleados dedicados en exclusiva a tareas de ciberseguridad?

Se ha verificado que cerca del 60% de las empresas encuestadas destinan menos de 10 empleados a la ciberseguridad y tan solo el 3% de las empresas dedican más de 100 empleados a la ciberseguridad. Por otro lado, más del **40% de empresas con menos de 10 empleados cuentan con más de 1000 empleados en plantilla, lo que representa un porcentaje bajo.**



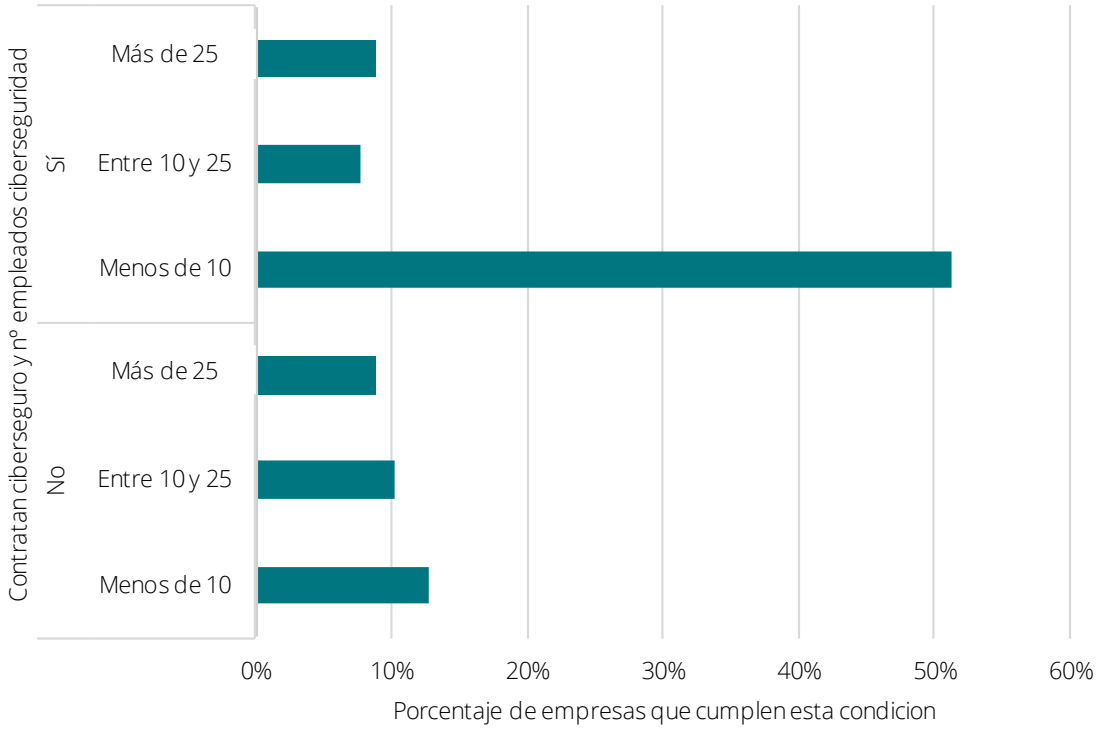
Empleados totales destinados a ciberseguridad

Cuántos empleados en total tienen las empresas que dedican menos de 10 empleados a ciberseguridad



Adicionalmente, se ha observado que **el 50% de las empresas** que cuentan **con un número reducido** de empleados disponen de un **ciberseguro** para mitigar los riesgos derivados de la seguridad de la información. A menor número de empleados mayor contratación del ciberseguro, es decir, se intenta transferir el impacto económico en caso de ciberincidente en aquellas compañías con menor nivel de madurez de ciberseguridad.

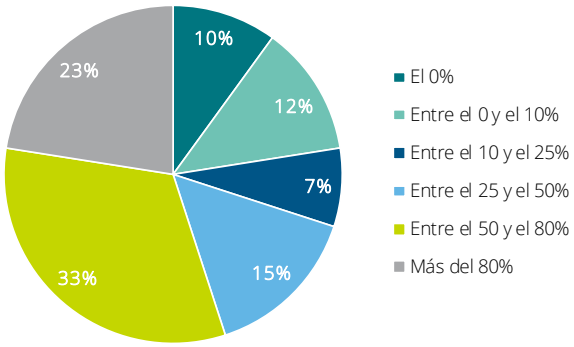
Número de empleados en ciberseguridad que tienen las empresas que, al mismo tiempo, contratan un ciberseguro



¿Qué porcentaje del personal de ciberseguridad es externo?

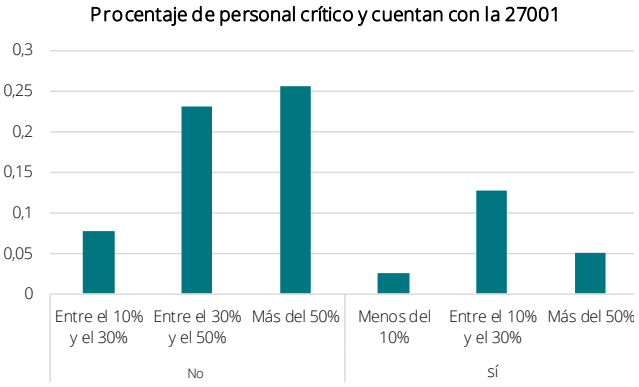
Se ha identificado que en la mayoría de los sectores la dependencia con terceras empresas en materia de ciberseguridad es superior al 50% de la plantilla, **en muchos casos todo el personal dedicado a ciberseguridad procede de proveedores.** Se observa una tendencia elevada en la externalización del personal de ciberseguridad para ser más flexibles a la hora de afrontar cambios y dar respuesta al entorno impredecible del mercado.

Porcentaje de personal externalizado en ciberseguridad



¿Qué porcentaje de empleados de ciberseguridad son imprescindibles (personal crítico)?

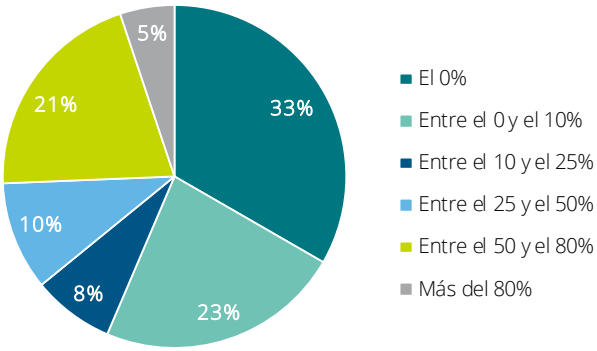
Se observa que en los sectores más regulados se ha hecho mayores esfuerzos en ciberseguridad y el porcentaje de empleados críticos es menor al tratarse de empresas más maduras y, por tanto, se ha sabido diversificar el riesgo de forma más efectiva. Por ello, sectores como la Banca y la energía reducen sus roles críticos diversificando el riesgo de esta manera. Esta situación se puede evidenciar al observar que las organizaciones que cuentan con la ISO 27001 cuentan con un porcentaje reducido de personal crítico, en contraposición a las organizaciones que no cuentan con ella.



¿Qué porcentaje del personal imprescindible (personal crítico) es externo?

Las empresas siguen teniendo de forma general una elevada concentración de responsabilidades críticas en materia de ciberseguridad sobre personal externo. Esto genera una alta dependencia de proveedores clave. En muchos casos, resulta difícil conseguir un equilibrio razonable entre la externalización de servicios de ciberseguridad para reaccionar de forma ágil a las necesidades del mercado sin perder el control de las funciones clave. A pesar de que se recomienda la externalización de determinadas funciones, en cualquier caso, se debe mantener el *know-how* de forma interna de aquellas consideradas críticas para no tener estas dependencias con terceros.

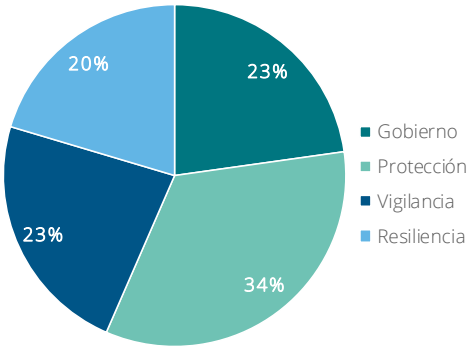
¿Qué porcentaje del personal imprescindible (personal crítico) es externo?



¿Cuál es el número de empleados según las siguientes líneas de ciberseguridad? Gobierno (estrategia), Protección, Vigilancia, Resiliencia (respuesta ante incidentes).

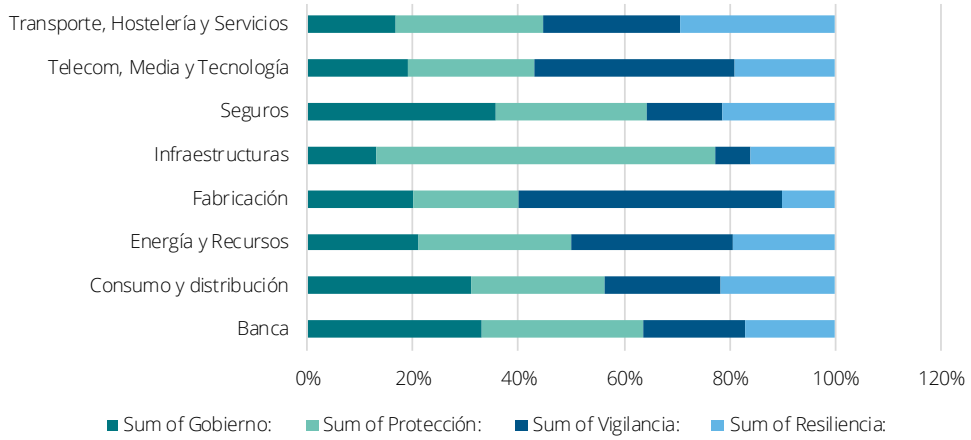
En el porcentaje de empleados destinados a ciberseguridad destacan los dedicados al área de protección con un 34%.

La dedicación por áreas parece responder a las necesidades actuales en ciberseguridad. No obstante, las necesidades de estar cada vez más cerca del negocio y hacer frente al número creciente de ciberataques, hace que cada vez las organizaciones puedan ampliar su ponderación hacia el gobierno y la resiliencia.



A continuación, vemos que la distribución del personal en función de las industrias. En línea con el punto anterior los distintos sectores se alinean con las medias de cada área, sin embargo, en el sector de Banca destaca por el gran número de personal dedicado al área de Gobierno, esta situación puede deberse debido a ser uno de los sectores con más presión regulatoria, lo que obliga a las organizaciones a adaptarse a los nuevos cambios con mayor rapidez y poder tener más control sobre la estrategia y el estado del ciberriesgo organizacional para dar respuesta a diferentes autoridades. Este dato también puede invitar a la siguiente reflexión: ¿Son las empresas más maduras en ciberseguridad las que cuentan con una mayor presencia de personal en estrategia y gobierno de ciberseguridad? Aunque no se dispone de datos suficientes para tener evidencias que afirmen la anterior cuestión, es cierto que las empresas más maduras en ciberseguridad se preocupan más en entender el negocio, cuales son los activos críticos, las prioridades de protección y son capaces de medir de forma más realista el ciberriesgo.

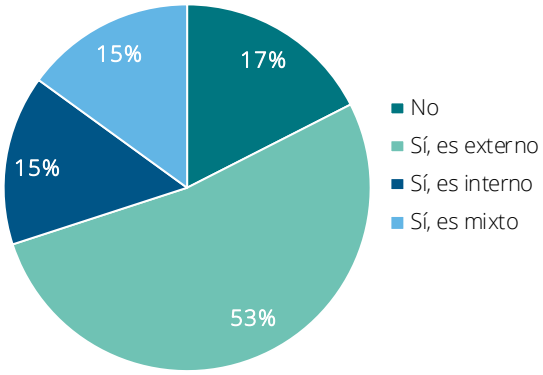
Reparto del número de empleados por industrias y áreas



¿Se dispone de un SOC/CSIRT propio?

Debido al impacto que supone sufrir un ciber ataque, la mayor parte de las organizaciones cuentan con un centro de operaciones y respuesta ante incidentes. Debido a la complejidad y coste de disponer de un centro propio el 53% de las organizaciones optan por externalizar el servicio en organizaciones especializadas.

¿Se dispone de un SOC/CSIRT propio?

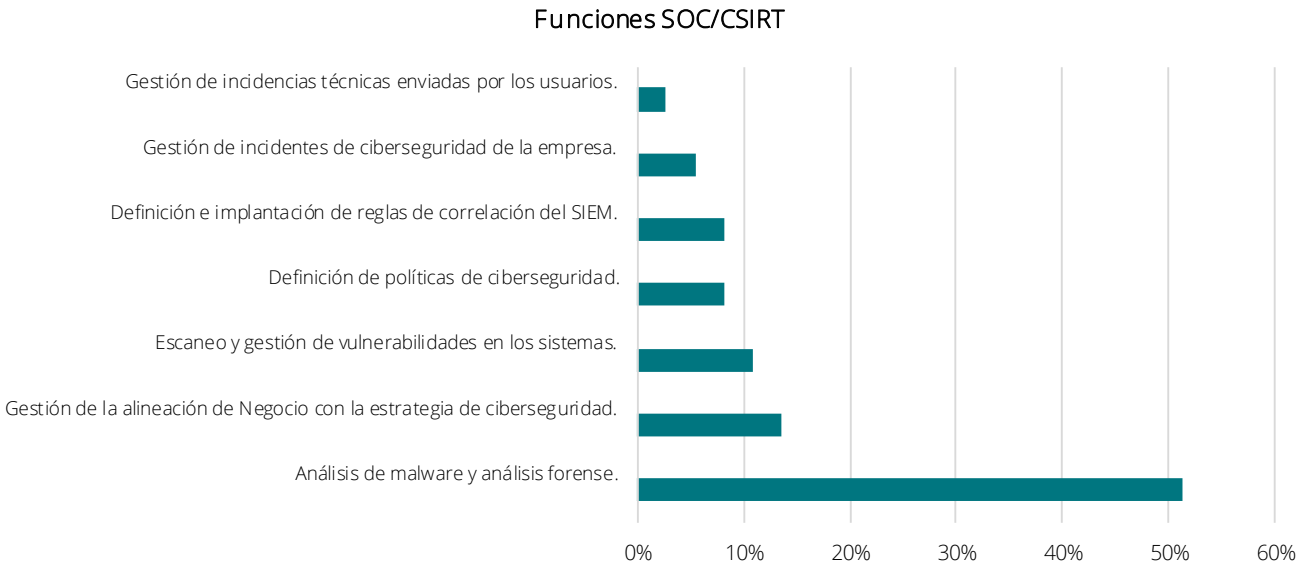


¿Cuáles de estas funciones recaen sobre el SOC/CSIRT?

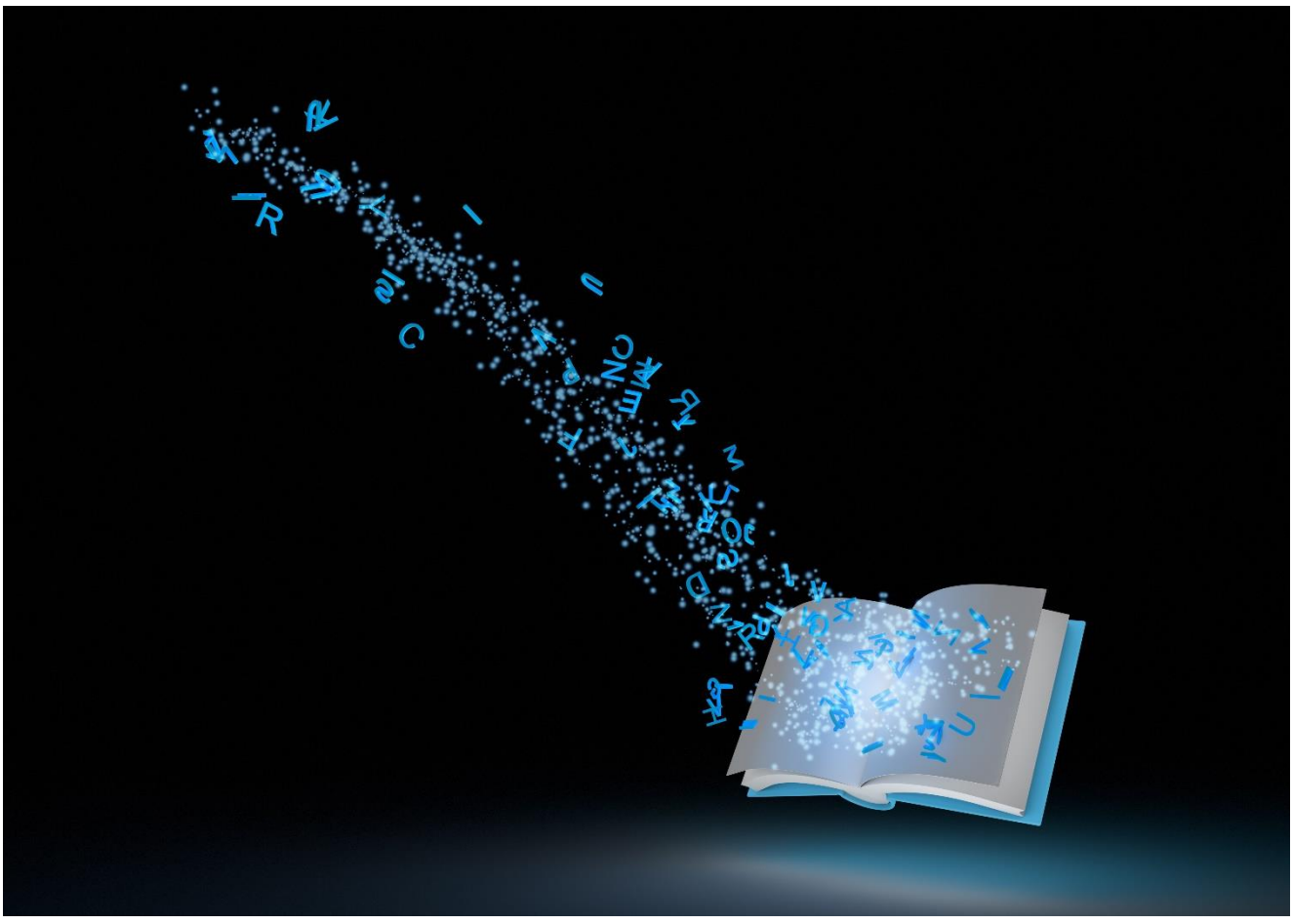
No existe un consenso alto sobre qué servicios deben estar bajo un SOC y CSIRT, así como cuál es la diferencia exacta entre ambos. Por ese motivo, es interesante conocer que servicios prestan cada uno según la muestra del estudio.

Las principales funciones de los SOC/CSIRT se distribuyen en:

- Análisis de **malware** y análisis **forense con un** 51%.
- Gestión de la alineación de Negocio con la estrategia de ciberseguridad con un 14%.
- **Escaneo** y **gestión** de **vulnerabilidades** en los sistemas con un 11%.



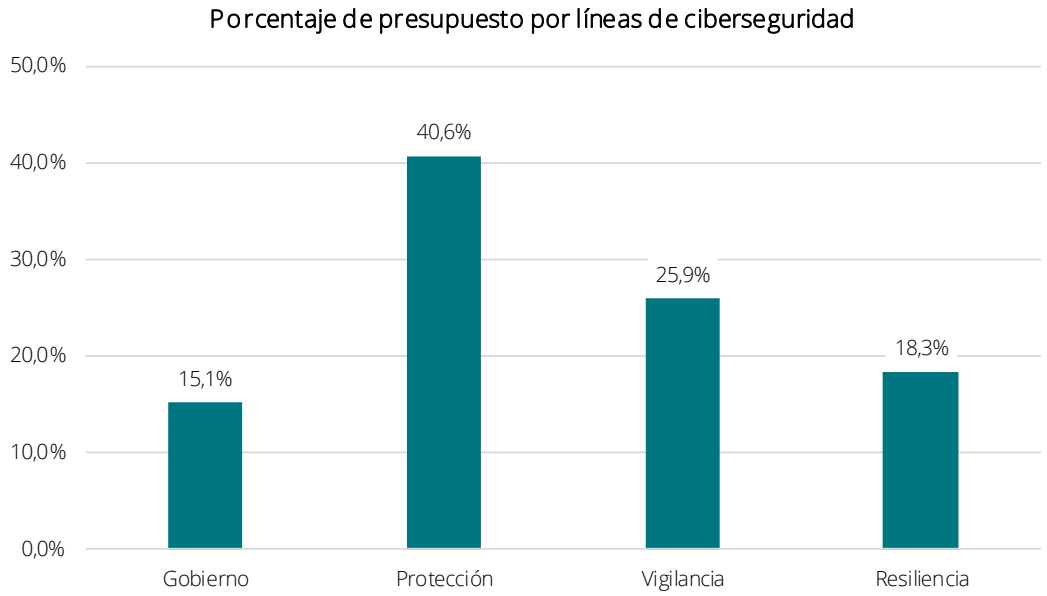
Se puede apreciar en la gráfica que hay un consenso respecto a la función de análisis de malware y análisis forense, puesto que al menos el 51% de las empresas sí que lo incluyen dentro de las funciones de su SOC/CSIRT. No obstante, el resto de funciones no siempre están incluidas. La capa de definición e implantación de políticas de ciberseguridad queda normalmente fuera, así como la propia respuesta de incidentes. Ello no significa que no se estén realizando estas tareas, sino que estas pueden estar dentro de otras áreas como puede ser la de Arquitectura de Ciberseguridad, Respuesta ante Incidentes, etc.



Presupuesto y servicios

¿Cuál es el presupuesto (incluyendo la tecnología y licencias de soluciones de ciberseguridad) disponible para ciberseguridad? Excluyendo empleados internos y según las líneas de ciberseguridad.

Gracias a los datos recogidos, podemos tener una imagen general de la distribución del presupuesto a lo largo de las cuatro líneas principales de ciberseguridad. Las empresas deciden invertir mayor cantidad de ingresos en Protección (40,6%), después en Vigilancia (25,9%), y por último en Resiliencia (18,3%) y Gobierno (15,1%).

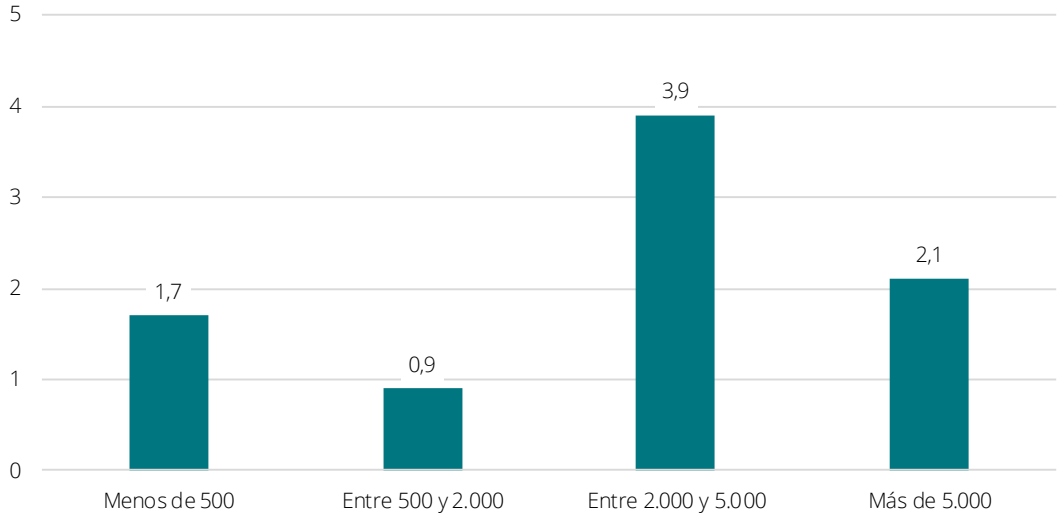


Esta distribución no es del todo realista si nuestro objetivo es mantener una estructura de ciberseguridad robusta, puesto que se observa una clara deficiencia en el presupuesto dedicado a Gobierno. El porcentaje recomendado estaría entorno a no menos de un 20%, con valores inferiores a este, no es posible construir modelos eficaces y realistas de análisis de riesgos y amenazas, ni estrategias completas que permitan alcanzar un nivel de seguridad adecuado, así como una relación fluida y continuada con negocio e IT.

Se ha realizado un análisis combinado del número de incidentes que ha recibido cada empresa durante el 2018 y su presupuesto en ciberseguridad, destacándose que las empresas que facturan entre 2.000 y 5.000 millones de euros son las que experimentan un mayor número de incidentes al año, prácticamente 4 al año. Esto se debe a que se encuentran en un nivel alto de facturación, por lo que al mismo tiempo, son con mayor frecuencia un objetivo de los atacantes. Sin embargo, los del rango superior de facturación sufren menos ciberincidentes al tener más medidas preventivas.

Se ha comprobado que según las empresas van disponiendo de mayores ingresos, estas sufren mayores ciberataques, al ser un objetivo con mayor retorno/impacto para el atacante. No obstante, a partir de un punto elevado de ingresos (más de 5.000 millones de euros) estos descienden gracias a las medidas preventivas y una mayor inversión en ciberseguridad.

Número de incidentes graves de seguridad al año por rango de facturación en Millones de euros



En el segundo rango (entre 500 y 2.000 millones de euros) se encuentran las empresas que solo reciben un ciberataque al año. Es el menor número de ataques de toda la muestra. Este dato se debe a que aún siguen siendo un objetivo poco frecuente para los atacantes, al mismo tiempo que, estas empresas ya disponen de unas medidas mínimas para empezar a mitificar de forma razonable, fallos básicos de seguridad y estar preparados ante *script-kiddies* o ataques poco sofisticados.

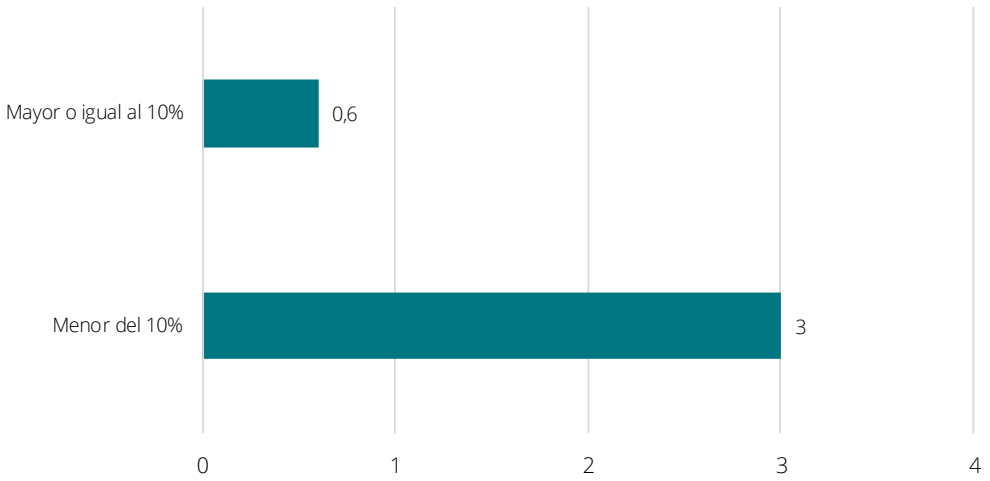
Gracias al análisis combinado de varias preguntas del estudio se puede apreciar que las empresas que consideran sus defensas y procedimientos contra incidentes adecuados, dedican en torno a 5 veces de media más presupuesto que las compañías que no se ven suficientemente preparadas

¿Qué porcentaje representa el presupuesto de ciberseguridad respecto al de IT/OT? Excluyendo empleados internos.

Si se analizan los resultados obtenidos se puede comprobar que de media se dedica a ciberseguridad un 8,5% del presupuesto de IT/OT.

Contrastando los datos obtenidos del estudio, podemos comprobar que las empresas que invierten más del 10% del presupuesto de IT/OT en ciberseguridad reportan 0,63 incidentes de seguridad al año de media, mientras que las que dedican menos del 10% experimentan 3,01 incidentes por año.

Incidentes al año según el porcentaje del presupuesto de IT/OT dedicado a ciberseguridad

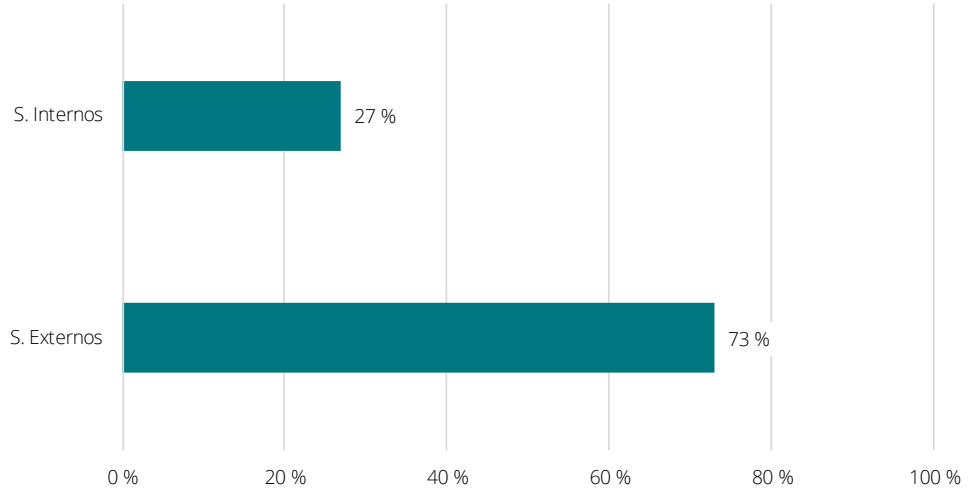


La diferencia entre ambos rangos es bastante notable, llegando a cuadruplicar el número de incidentes, lo cual recalca la importancia de establecer un presupuesto adecuado para levantar defensas y procedimientos seguros, y así mantener la información de los sistemas a niveles aceptables y proteger la reputación de la compañía.

¿Qué porcentaje del presupuesto* anual de ciberseguridad se dedica a los servicios externalizados y cuál a los servicios internos? Excluyendo personal interno y dividiendo entre CAPEX y OPEX.

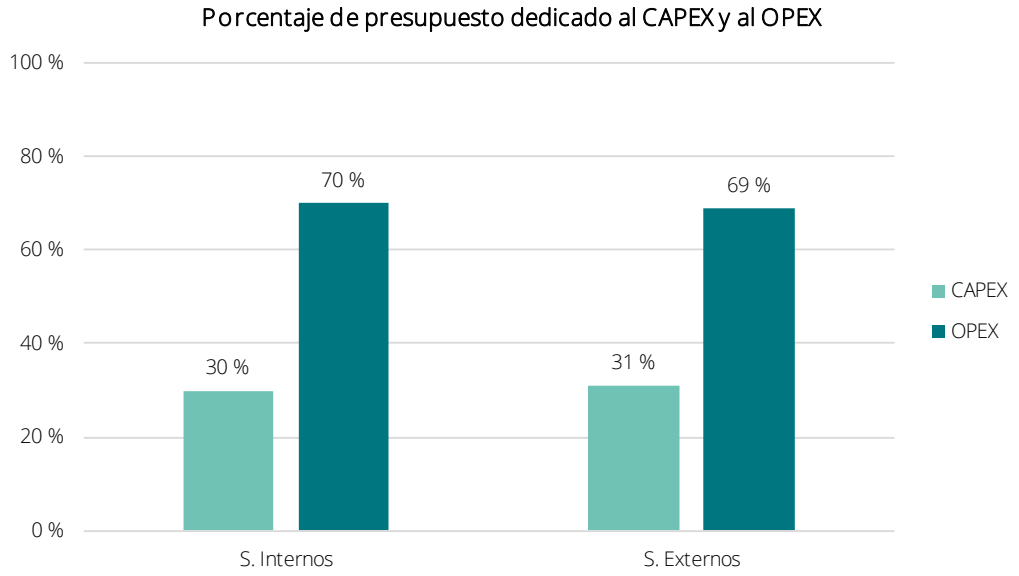
Tras examinar las cifras extraidas del estudio, se puede obtener el presupuesto que se dedica de media a los servicios internos (27%) frente a los externalizados (73%).

Porcentaje del presupuesto dedicado a los servicios internos y externos



El aumento de los servicios necesarios para mantener la seguridad de la información de las compañías y el incremento de la complejidad de dichos servicios, han provocado que cada día sea más rentable y necesario externalizar ciertas funciones a pesar de que esto implique delegar la seguridad en manos de otros proveedores.

Asimismo, la tendencia dentro de ambos tipos de servicios marca que el 30% se considera CAPEX y el 70% restante OPEX. Se considera una buena práctica seguir estos porcentajes.



Por otro lado, un dato interesante es que prácticamente coinciden los valores de CAPEX y OPEX para los servicios internos y externos.

Target Operating Model y políticas

Jerárquicamente, ¿De quién depende el CISO?

La figura del CISO principalmente tiene una responsabilidad focalizada en la seguridad dentro de la empresa reportando en la mayoría de los casos al CIO o al departamento de IT en su caso.

Según estudios anteriores ("El Rol del CISO" de ISMS en colaboración Deloitte), casi el 80% de los CISOs consideran que debería reportar directamente a la alta dirección o al COO/CRO/Comité de Dirección, mientras que el presente estudio de Deloitte muestra que casi el 60% reportan al CIO. Esto refleja una gran disparidad entre el árbol de dependencia actual y el deseado.

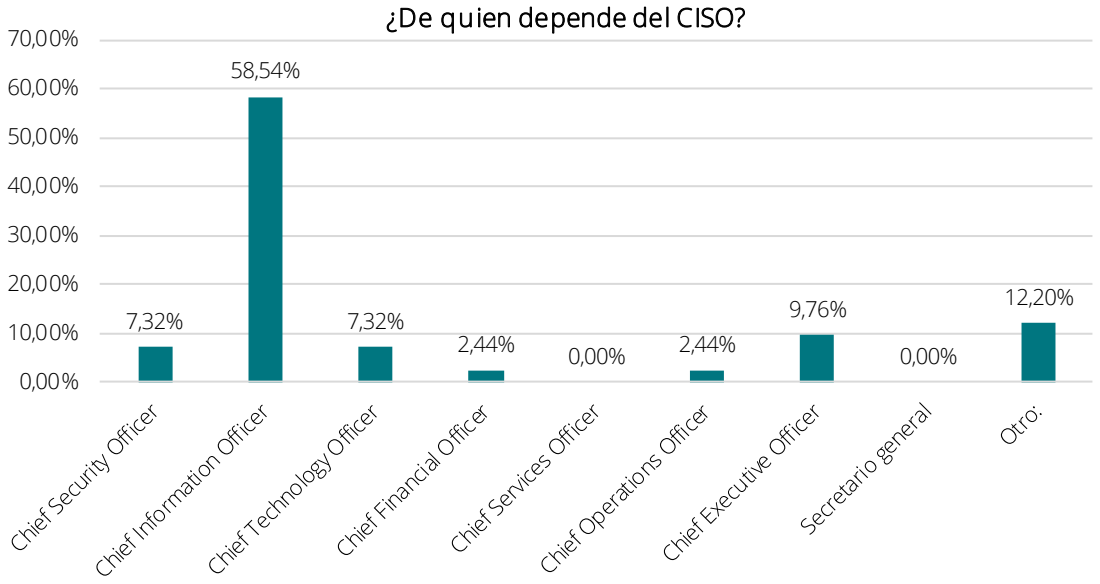
La ubicación organizativa del CISO depende de los siguientes factores principales:

- Complejidad de la empresa.
- Requisitos de leyes y regulaciones.
- Sector de actividad.
- Factor humano del equipo de dirección.

En las grandes organizaciones el área de Seguridad de la Información está generalmente ubicada dentro del departamento de IT. Es dirigida por el CISO que reporta directamente a los altos directivos de sistemas o al CIO.

Actualmente existe una tendencia en separar la seguridad de la información de la división de IT.

El desafío está en diseñar una estructura de reporte para los programas de Seguridad de la Información que equilibre los requerimientos de cada una de las partes interesadas.



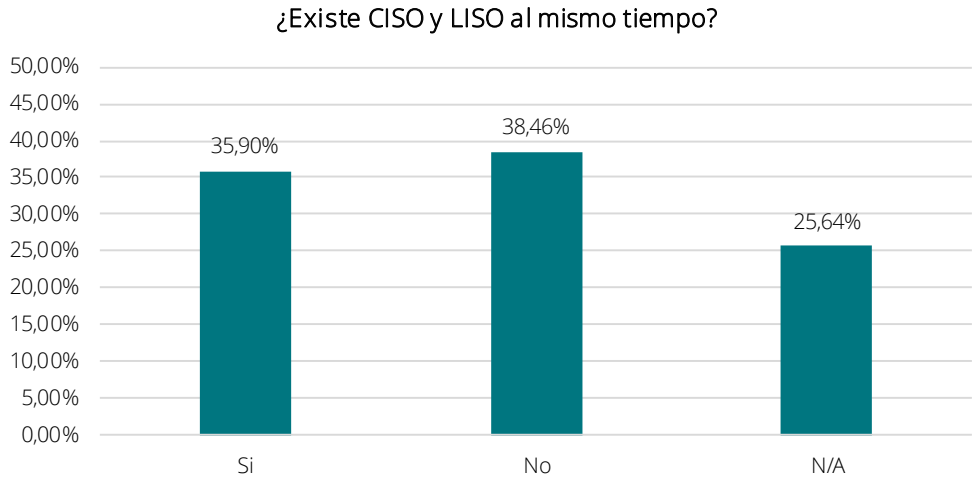
¿Existe un Global CISO y al mismo tiempo LISO's en cada país?

Se ha observado que en el 36% de los casos existe un CISO y LISO (Local Information Security Officer) simultáneamente. Es el caso de las multinacionales o empresas de gran tamaño, donde el LISO reporta al CISO. En el 38% de los casos solo existe la figura del CISO y en el 26% de los casos restantes no aplica. Es decir, aproximadamente en la mitad de las multinacionales existe la función de Local information Security Officer. En muchas multinacionales, la implantación de controles, la monitorización de la operación de ciberseguridad y respuesta ante incidentes, así como la estrategia global se realiza de forma centralizada. No obstante, a pesar de que gracias a la transformación digital esta centralización es cada vez más fácil de realizar, existe el riesgo de perder el control en cada país sobre el cumplimiento de los controles procedimentales, normativas locales, así como gestión de una correcta cultura y concienciación sobre el ciberriesgo. Por este motivo, a medida que estas compañías van creciendo en cada región empieza a ser necesaria la función de un responsable de ciberseguridad en cada una de ellas.

Los principales motivos que justifican la inversión en la figura del LISO están relacionados con la complejidad de la organización:

- Dispersión geográfica
- Dispersión funcional

- Dispersión societaria
- Alto volumen de transacciones de negocio

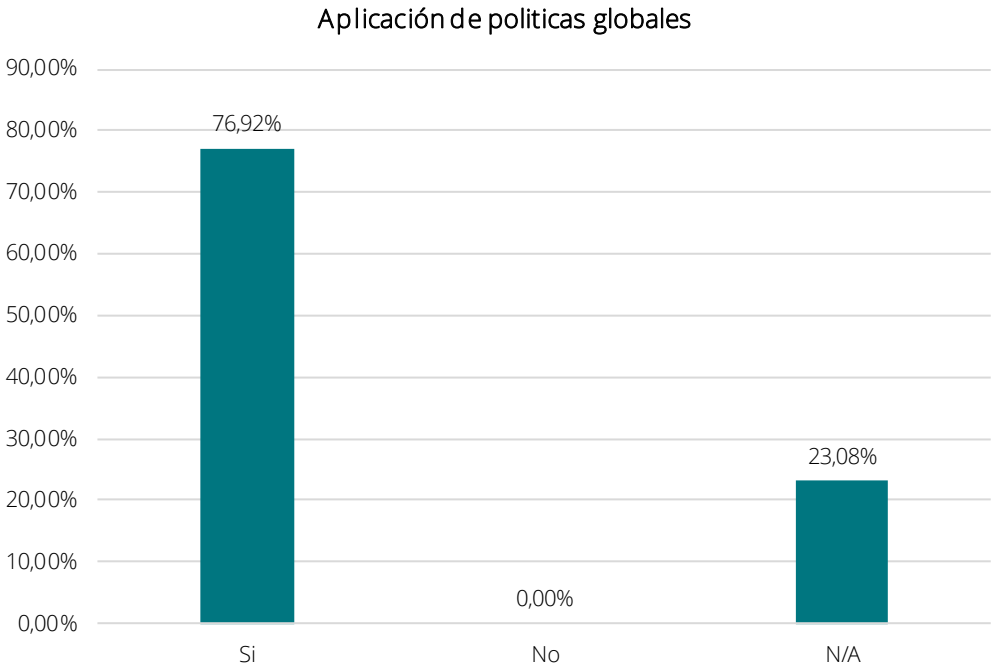


¿Se definen políticas de ciberseguridad a nivel global que deben ser cumplidas por todos los países?

En el 77% de los casos existen políticas globales Corporativas de Ciberseguridad que han de ser cumplidas por todo el grupo.

En el caso de **empresas más pequeñas (el 33% restante) dichas políticas son de carácter local.**

En la totalidad de los casos, independientemente de que exista un LISO en aquellas compañías multinacionales, las políticas siempre se definen desde la figura de "Global o Holding".



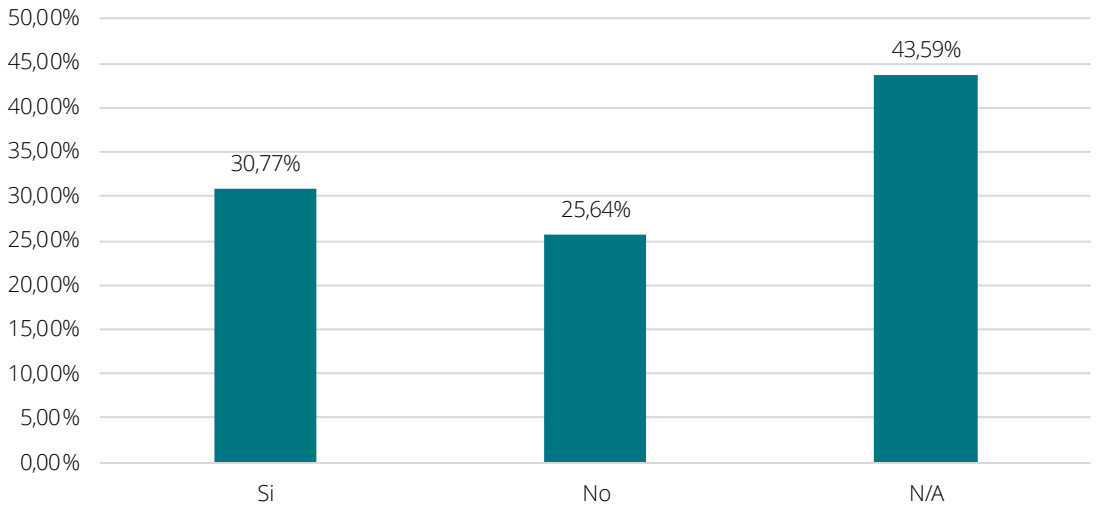
¿El resto de países financian las funciones holding?

Cabe destacar que en el 45% de los casos se ha observado que el resto de países no financian las funciones holding.

En el 55% de los casos restantes sí se financian las funciones de Holding donde la matriz, posee la totalidad (o al menos, la mayoría) de participaciones de otras entidades dependientes o filiales. **Son fundamentalmente las grandes multinacionales las empresas que se estructuran de tal forma.**

Según nos encontramos ante organizaciones más grandes y maduras, se observa que, este suele ser un debate importante de discusión y preocupación para los CISOs. Mientras que en los presupuestos de la organización, la ciberseguridad es percibida como un coste (no inversión) residual, los CISOs se enfrentan ante la complejidad de justificar mayores presupuestos para hacer frente a un servicio multipaís y que supone un retorno de mayor beneficio para la empresa (al descontar los gastos del menor número de incidentes, como se ha visto anteriormente).

Países que financian la función global/holding en ciberseguridad



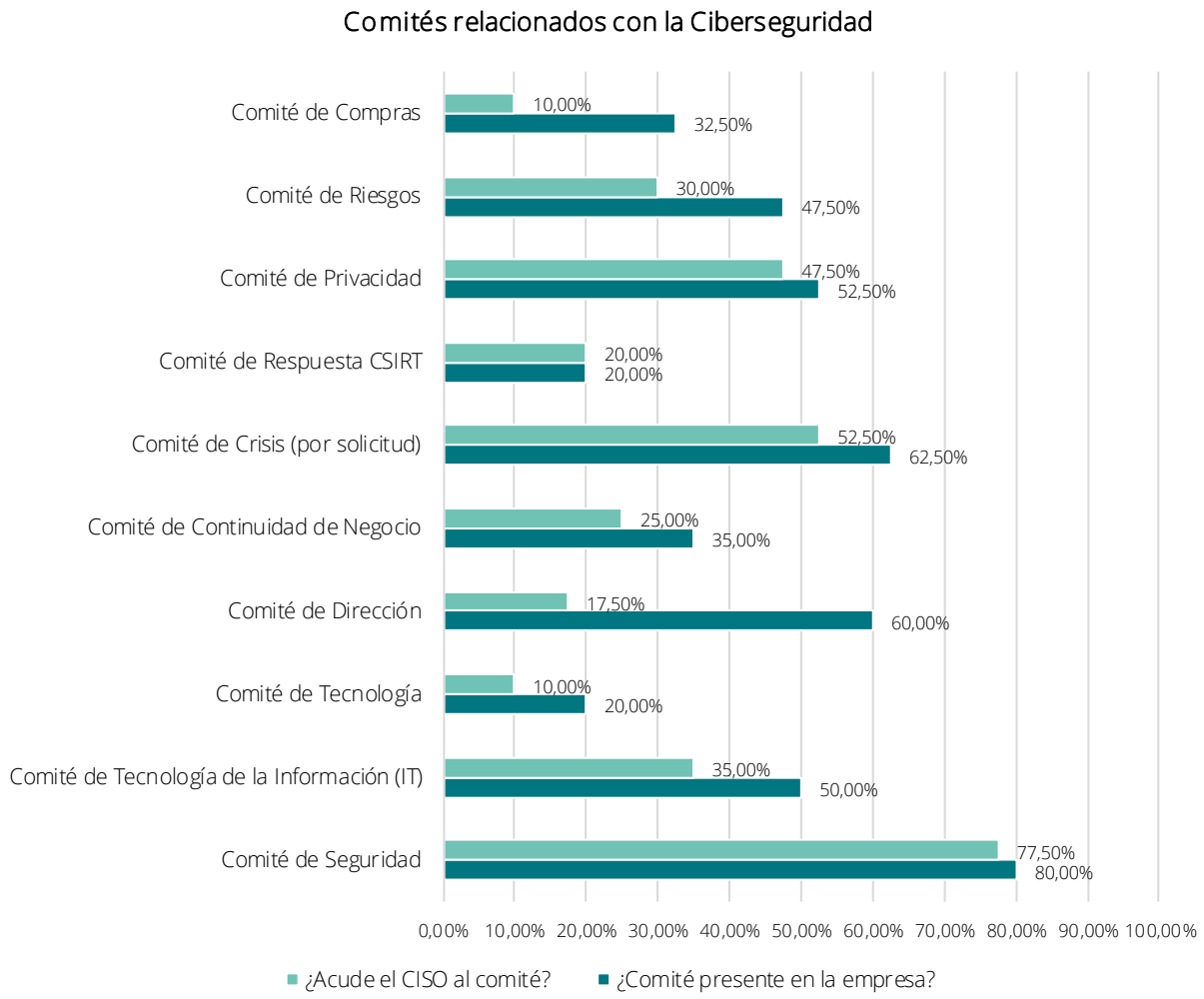
¿Cuáles de estos comités de ciberseguridad están formalizados en su empresa? ¿Y en cuáles de ellos acude el CISO al comité?

Los comités que tiene mayor relevancia para las funciones de un CISO y, por tanto, estos tienen una participación activa son el Comité de Seguridad, el Comité de Privacidad y el Comité de Crisis.

Por el contrario, el comité de dirección está presente en la mayoría de las empresas, pero los CISOs siguen sin tener una aportación mayoritaria en él, aunque la tendencia es al alza.

El rol del CISO es, sin embargo, tan imprescindible como aun insuficientemente conocido o reconocido por la propia organización.

Según estudios precedentes (Encuesta del Rol del CISO de ISMS, en colaboración con Deloitte), el tiempo que el CISO dedica a las funciones relacionadas con la Dirección estratégica y planificación, la Elaboración de políticas, y la Gestión de los presupuestos concuerda con la prioridad que este mismo les da a estas tareas. Sin embargo, a pesar de que la **gestión de los empleados y las actividades técnicas son dos tareas con menor prioridad** según lo indicado por los propios CISOs, **también son dos de las tareas que conllevan mayor implicación de tiempo por su parte**. Esto indica un **conflicto entre lo que el CISO considera que debe hacer y lo que el CISO hace en su día a día.**



De la anterior gráfica se rescatan varios datos interesantes:

- Normalmente en los comités más relacionados con la ciberseguridad los CISOs están representados en los mismos. El Comité de Dirección, a pesar de ser un aspiracional para muchos CISOs sigue estando fuera de su alcance competencial.
- El CISO tiene un rol activo en el Comité de Continuidad de Negocio en más del 70% de los casos en los que este comité existe.
- Los CISOs empiezan a tener un papel relevante en los Comités de Crisis.
- Solo en el 64% de los casos en los que existe un comité de riesgos, el CISO está representado ahí. Con lo que contrasta los datos del World Economic Forum que apunta al ciberriesgo como unos de los riesgos de mayor impacto y probabilidad, al mismo tiempo que estos están relacionados con muchos otros de diferente naturaleza.
- El Comité de Seguridad está más presente que los de Tecnología y Tecnología de la Información. También entendible por el tipo de urgencia y criticidad de los temas a tratar.
- Solo 1 de cada 5 empresas encuestadas dispone de un comité específico para dar respuesta a incidentes de ciberseguridad.

En relación a la figura del Delegado de Protección de Datos según la GDPR, ¿Se dispone de un DPO interno o externo?

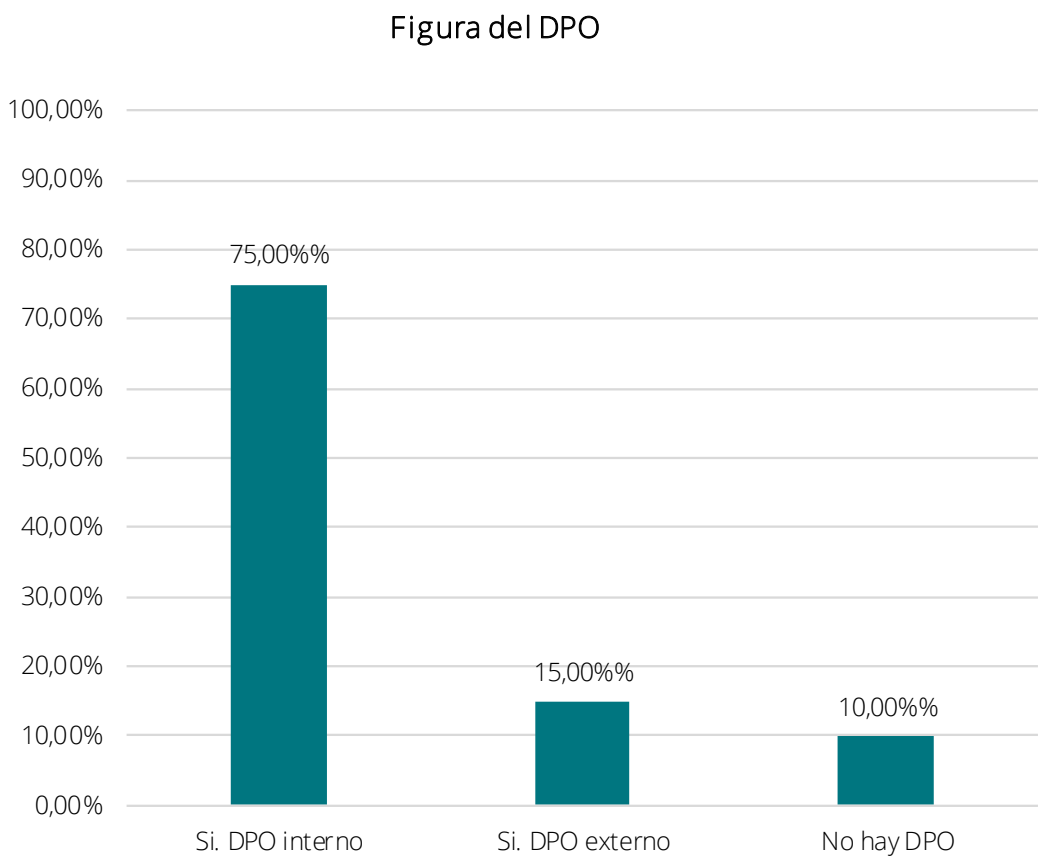
En el 75% de los casos la figura del DPO es interna, por lo que se puede deducir que se otorga la importancia correspondiente a las políticas de gobierno del dato de carácter personal. La principal función que debe desempeñar el Delegado de Protección de Datos o DPO es gestionar y supervisar el cumplimiento de la GDPR. Entorno a esta función se desarrollan todas sus actividades.

Asimismo, existen una serie de casos en los que es obligado contar con un DPO:

- Si los datos son tratados por una autoridad o un organismo público. A no ser que se trate de tribunales, durante un proceso judicial.
- Si las actividades de los encargados del tratamiento son operaciones en las que se observan de forma sistemática y habitual los datos de interesados a gran escala.
- Si se lleva a cabo un tratamiento, en grandes niveles de categorías extraordinarias, de datos personales que hagan referencia a condenas o infracciones penales.

El 15% de los encuestados manifiesta disponer de un DPO externo en sus empresas, esto se debe fundamentalmente al tamaño de las mismas.

En el 10% de los casos no se dispone de la figura de un DPO, lo cual nos indica que las políticas de Gobierno del dato y el control de los mismos no tienen un nivel de madurez suficiente.



Certificaciones, framework y formación

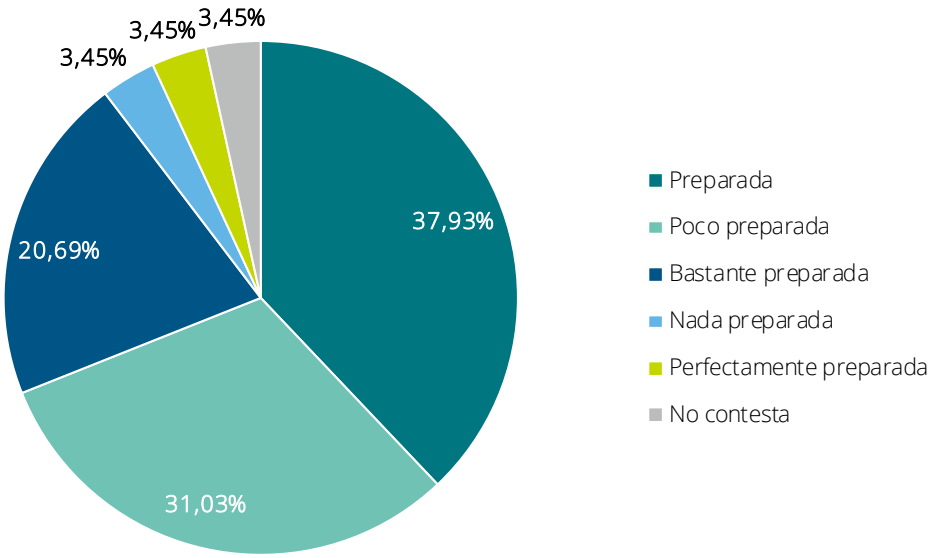
¿Qué certificaciones relacionadas con la ciberseguridad posee la empresa?

Se ha evidenciado que solamente el **22,5% de las empresas** que participan en la encuesta poseen la certificación **ISO 27001**. Los sectores en los que más encontramos dicha certificación son: **Energía y Recursos, Banca y Consumo y Distribución.**

El **15%** de las empresas que participan en la encuesta poseen la certificación **ISO 22301** relacionada con la continuidad del negocio, perteneciendo estas a sectores como: **Banca, Energía y Recursos, Consumo y distribución, Transporte, Hostelería y Servicios y Telecom, Media y Tecnología.**

El 72,50% de los CISOs que participaban en la encuesta, aseguraron que sus empresas no estaban certificadas ni en la ISO 27001 ni en la ISO 22301, ambos estándares relacionados con la seguridad de la información y la continuidad del negocio. Poseer la ISO 22301 suele traducirse en que la organización está razonablemente preparada ante un incidente que pueda suponer la interrupción del negocio. El hecho de que solamente el 15% de las empresas encuestadas posean la ISO 22301 señala que el resto podría no estar preparadas para dar respuesta en caso de incidente de seguridad, pudiendo producir interrupciones en el servicio prestado sin llegar a garantizar un nivel mínimo de servicios o productos.

¿Cómo de preparadas se ven las empresas que no tienen certificaciones de seguridad ante incidentes?



Dentro del **72,50%** cuya empresa **no** posee ninguna **certificación** de **ciberseguridad** más del **50%** de los **CISOs afirma** que su **organización** está **preparada** o bastante preparada ante incidentes de seguridad. Un porcentaje tan alto puede deberse a que empresas de tamaño reducido, aunque no posean ninguna certificación en materia de Seguridad de la Información se sienten confiadas ante la preparación frente a un ataque de seguridad. No obstante, dicha **confianza** en numerosos casos proviene de una **falta** de **concienciación** y se traduce en una escasez de **preparación** real.

Por otro lado, el 66,67% de las empresas que poseen la ISO 22301, están certificadas también en la ISO 27001, lo cual demuestra que gran parte de las empresas, una vez entran en procesos de certificación, tienden a optar a varias certificaciones en materia de Seguridad de la Información. Esta predisposición a obtener varias certificaciones en parte viene porque las empresas perciben el valor que les retorna poseer una certificación y deciden continuar con ello. Al mismo tiempo, parte del esfuerzo en la obtención de una certificación si este se hace para aumentar el nivel de madurez real y, no solo para obtener dicho "título", se traduce en una mayor facilidad en la obtención de futuras certificaciones.

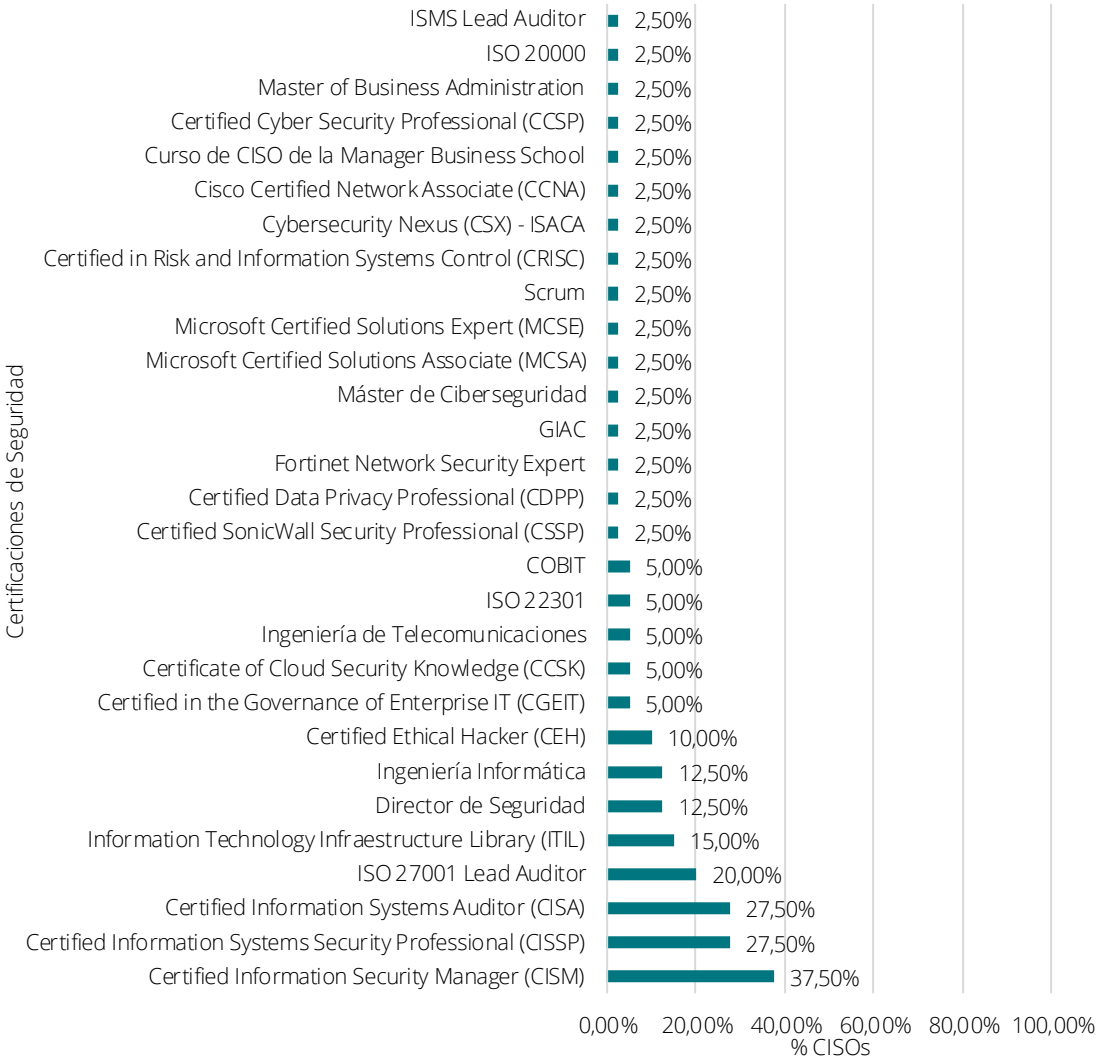
¿Qué certificaciones/formación posee el CISO de la empresa?

El 75,00% de los CISOs encuestados posee al menos una certificación en materia de Seguridad de la Información. Esto se debe, en parte, a que para desempeñar la figura del CISO en la empresa se necesitan tanto conocimientos de negocio como técnicos, por lo que, a menudo los **CISOs complementan sus conocimientos con certificaciones que cubren sus áreas de conocimiento pendientes.**

Si bien hasta ahora las certificaciones más comunes entre los CISOs eran la CISM y CISA, se observa que el CISSP ha cobrado relevancia situándose entre las más habituales en los últimos años. La popularidad de la CISSP se debe, en parte, a que cubre ámbitos como la seguridad y gestión de riesgos, la seguridad de activos, comunicación y seguridad de red, la gestión de identidad y acceso o la seguridad en el desarrollo del software en mayor profundidad que las otras dos mencionadas.

Un dato interesante es el hecho de que el 72,73% de los CISOs que poseen la certificación CISSP, están certificados a su vez en la CISM y en el 64% de las veces están certificados en el CISA. Esto se puede deber a la **tendencia** actual de mayor **concienciación** en la formación de los CISOs y que existe un patrón de certificaciones que vendría a cubrir su "carrera formativa" empezando por el CISA y CISM, para posteriormente acabar con el CISSP.

Certificaciones que posee el CISO de la empresa

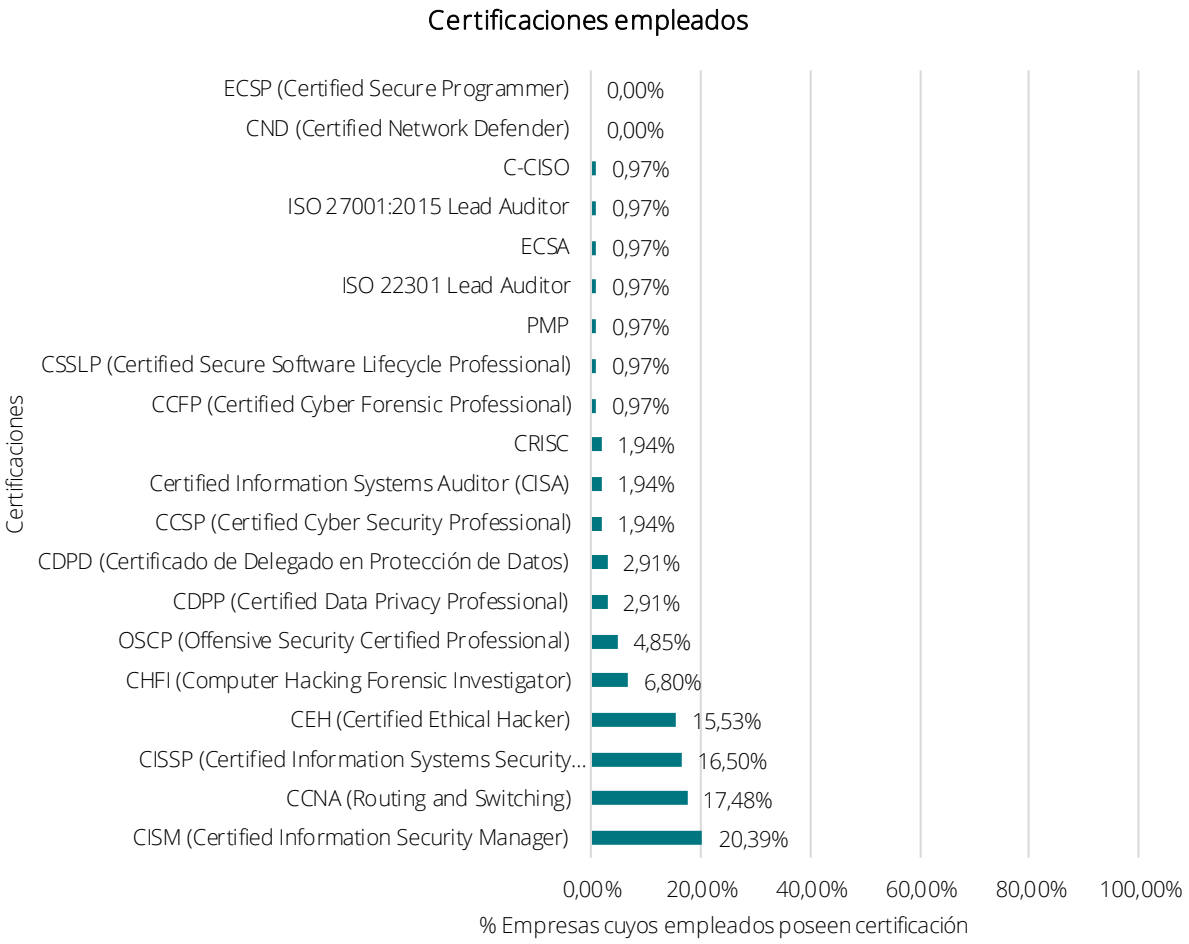


¿Cuáles de estas certificaciones de seguridad están en posesión de algún empleado de la empresa?

Una forma de mejorar el nivel de Seguridad de la Información de la empresa es a través de la **formación y concienciación de los empleados**, por lo que, es importante analizar qué certificaciones poseen el personal de ciberseguridad de las empresas analizadas.

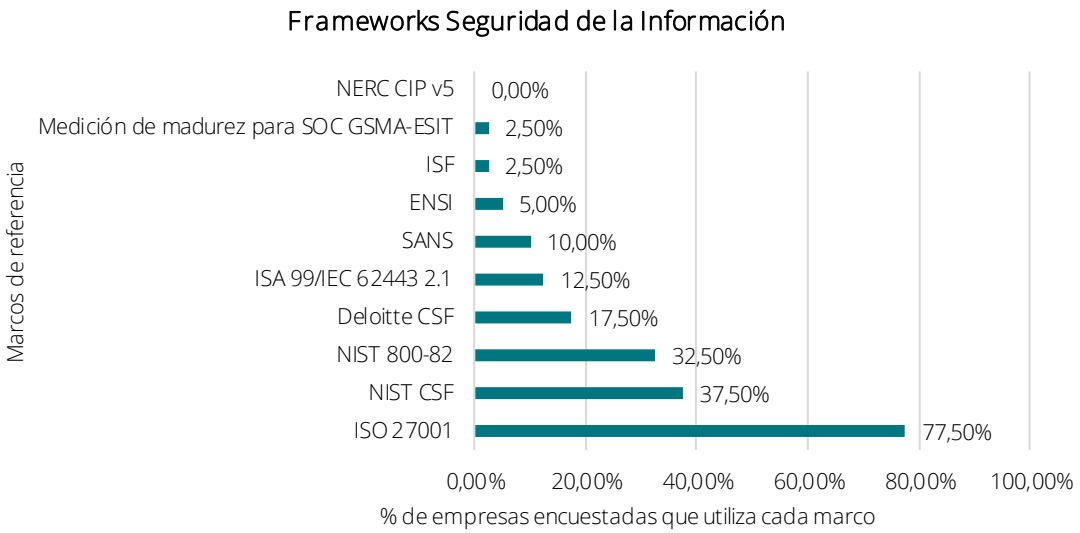
Al igual que en el caso de los CISOs, **la certificación CISM (Certified Information Security Manager) es la más común entre los empleados**, seguida muy de cerca por la **CCNA (Routing and Switching)**, con un enfoque más técnico ya que está orientada a los profesionales que operan equipamiento de red.

Otro dato destacable es que el **10,00% de los CISOs** encuestados afirmó que **no posee ninguna certificación**, así como **ninguno de los empleados de su empresa**. Estas organizaciones pertenecen al sector de Energía y Recursos.



Se puede observar como existen diferencias significativas entre las certificaciones del CISO y las de sus equipos. Mientras que los CISOs buscan certificaciones más enfocadas en las capas altas de gestión y liderazgo en ciberseguridad (como CISSP y CISM), sus equipos se certifican además en certificaciones más técnicas (como CCNA y CEH).

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



Podemos observar que, a pesar de que no todas las empresas están certificadas en la ISO 27001, casi un 80% utiliza dicho estándar como marco de referencia en ciberseguridad. Muy por debajo se encuentra la NIST CSF con un 37,50%. Cerca del 18% de las empresas utiliza el CSF (Cyber Security Framework) de Deloitte, cuyos **controles** para determinar el nivel de madurez de una empresa en materia de Seguridad de la Información **engloban** los controles y requisitos establecidos por el **resto** de **marcos** (ISO, SANS, NIST, etc.). Por ello, las empresas que evalúan su nivel de madurez con el **CSF de Deloitte** están utilizando **indirectamente** el **resto de marcos** en materia de Seguridad de la Información.

Un hecho destacable es que **ninguna empresa** utilice **NERC CIP v5**, puesto que se trata de un marco muy conocido y usado en Estados Unidos para el **sector energético**. Es decir, las empresas españolas no están importando el uso de este marco americano.

En el caso de los marcos **ISA 99** y **NIST 800-82** sus controles están enfocados al **mundo OT**, esto se ve reflejado en el hecho de que el **40%** de las empresas que utiliza la primera y más del **30%** de las que utiliza el segundo pertenecen al **sector de Energía y Recursos**. El resto de sectores entre los que son muy comunes dichos marcos son los de **Consumo y distribución y Fabricación**. Esto demuestra que, en el **mundo OT** se está dando gran **importancia a la Seguridad de la Información** y se utilizan estándares específicos y enfocados a dichas infraestructuras.

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

La Formación y Concienciación en materia de Seguridad de la Información en las compañías es **fundamental** para que los empleados posean las habilidades necesarias para trabajar cumpliendo protocolos de seguridad que protejan a la empresa de amenazas y situaciones críticas. Se ha observado que el 50% de los encuestados no proporciona formación presencial a sus empleados. No obstante, de los que sí lo hacen el 65,00% apuesta por la formación online puesto que permite mayor flexibilidad horaria a los empleados y puede abaratar los costes.

El **15,00%** de los CISOs encuestados asegura **no impartir** u ofrecer **formación y concienciación** a sus empleados.

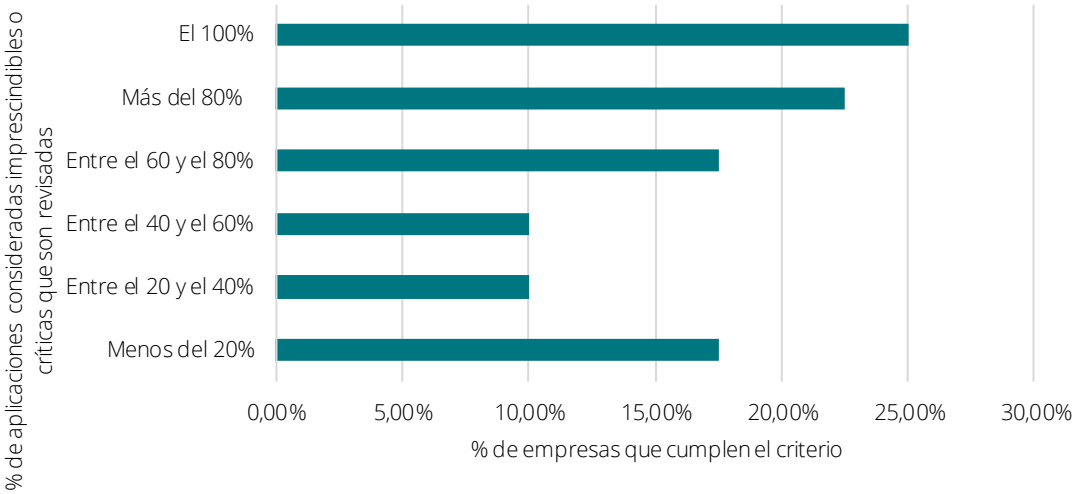
Asimismo, cabe destacar el hecho de que algunos **CISOs** han comentado que la **formación** en sus empresas se imparte **bajo demanda**. En estos casos se recomienda utilizar un enfoque más proactivo y no tan reactivo en materia de formación y concienciación. Esto se lograría con **planes** robustos de **formación y concienciación preestablecidos, aprobados por la dirección**, con un seguimiento formal, así como su **mejora continua** y actualización de los mismos.

Revisiones de seguridad, entornos cloud y tendencias en tecnologías

¿Qué porcentaje de las aplicaciones consideradas imprescindibles/críticas son revisadas?

Se ha evidenciado que la mayoría de los sectores tienen una **alta concienciación** sobre la importancia de realizar **revisiones periódicas sobre las aplicaciones** que son imprescindibles o críticas para su modelo de negocio. No obstante, es llamativo que sigue habiendo un 37% de empresas que no llegan a cubrir con las revisiones el 60% de las aplicaciones críticas.

Porcentaje de las aplicaciones consideradas imprescindibles/críticas son revisadas



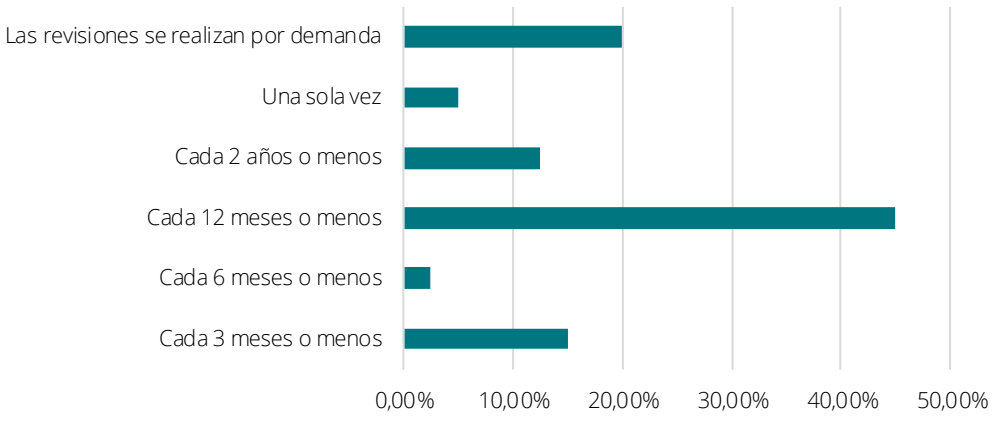
Además, si se hace una revisión por sectores, se aprecia que los más preocupados por el correcto funcionamiento de sus aplicaciones críticas y, por tanto, los que más revisan las funcionalidades y requerimientos de las mismas son los sectores TI, Fabricación y Seguros, y los que menos, Transporte, Hostelería y Servicios e Infraestructura.

¿Con qué periodicidad se revisan las aplicaciones consideradas imprescindibles/ críticas? Elija la respuesta que mejor se ajuste.

Se observa que las aplicaciones críticas son revisadas, al menos, una vez al año en la mayoría de los casos.

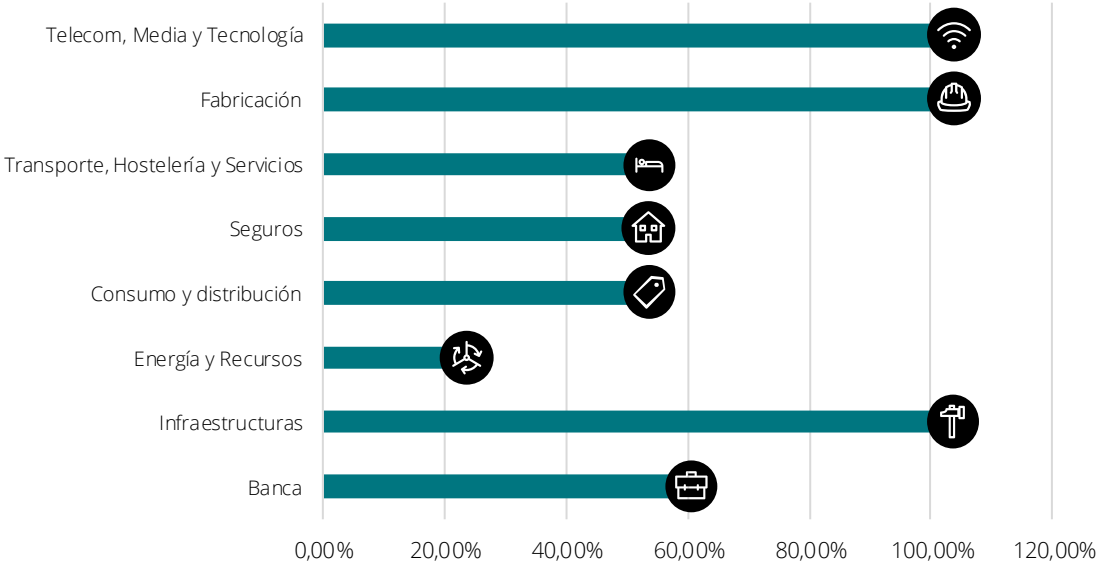
Un dato importante que se puede extraer es que estas revisiones también suelen hacerse bajo demanda, entendiendo la demanda como posibles evolutivos que se realicen en dichas aplicaciones y que por ello necesiten de una revisión. No obstante, realizar estas revisiones cada más de 1 año se considera insuficiente según las buenas prácticas de mercado.

Periodicidad con la que se revisan las aplicaciones críticas



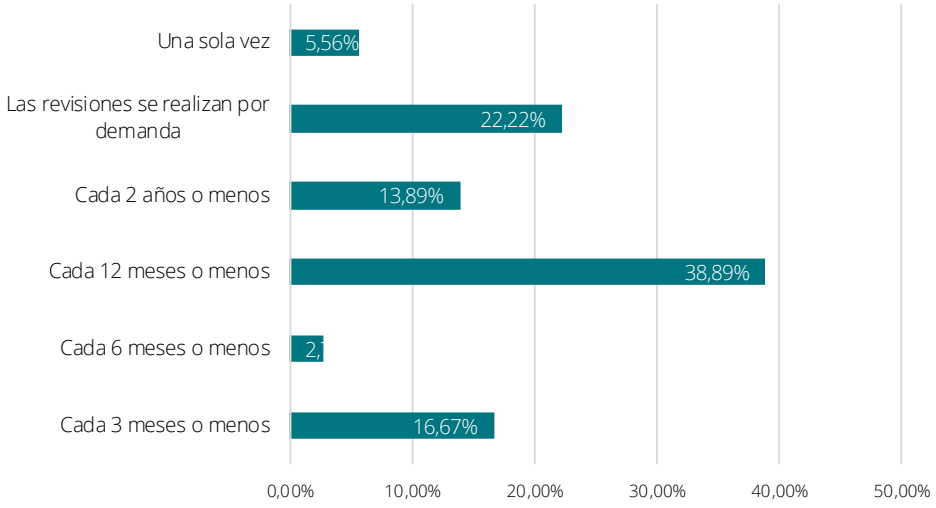
Se puede deducir que los sectores que más realizan revisiones periódicas son los sectores tecnológicos o con infraestructura OT como son el sector de las Telecomunicaciones, Media y Tecnología, Infraestructuras y el sector de Fabricación.

Sectores que revisan sus aplicaciones críticas de forma anual



Además, relacionando esto con el número de incidentes de ciberseguridad que ocurren al año, se extraen las siguientes conclusiones:

Periodicidad con la que se revisan las aplicaciones Vs. Incidentes de seguridad al año



Como era de esperar, el no hacer revisiones de forma periódica puede acarrear que el número de incidentes de seguridad sea más elevado. Por ello la importancia de que las aplicaciones que sean críticas pasen este tipo de revisiones con la máxima frecuencia posible.

¿Qué porcentaje de servicios están soportados por Cloud Computing?

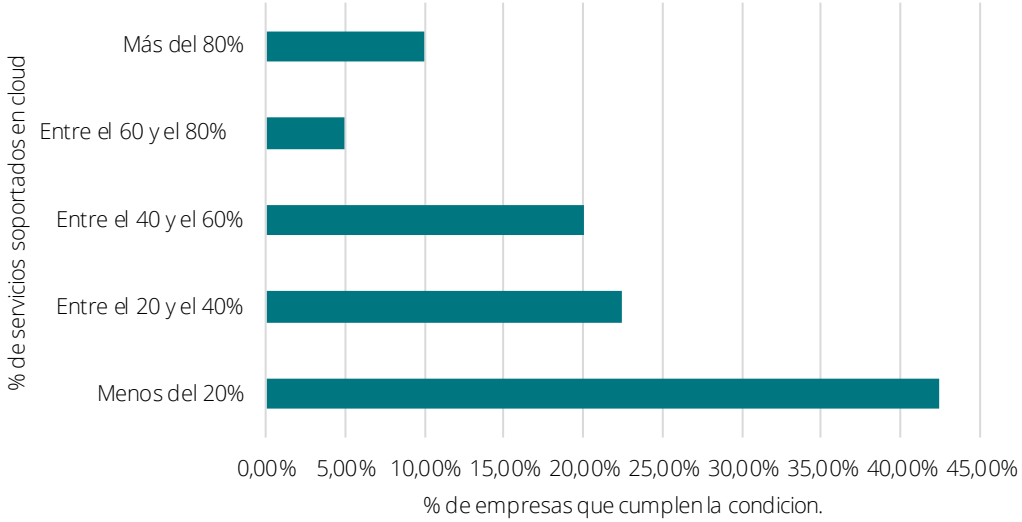
Hoy en día, sigue siendo elevada la cantidad de datos **soportados "In house"** dentro de las propias empresas, debido a que, aunque cada vez el Cloud Computing es una tendencia más al alza, algunas empresas siguen prefiriendo mantener determinados datos y aplicaciones dentro de su infraestructura.

Esto puede ser debido a aún **falta confianza** en cuanto a las medidas de seguridad que pueden ofrecer los servicios Cloud a las empresas en cuanto al tratamiento de sus servicios y de sus datos, así como algunas fugas o brechas de las que se han hecho eco en los medios.

El cloud computing, a pesar de su clara tendencia, aun no representa la opción prioritaria para las empresas para alojar su infraestructura e información.

Solo el 10% de las empresas tiene más del 80% de su infraestructura en cloud, solo un 5% tiene entre el 60% y el 80% y un 20% de las empresas mantiene entre el 40% y el 60%.

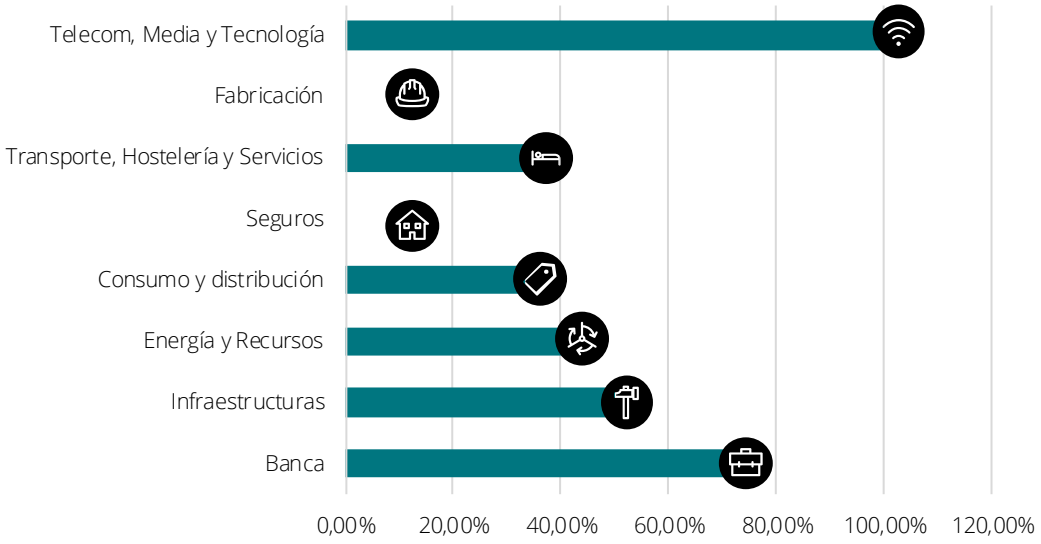
Porcentaje de servicios soportados por Cloud Computing



Los sectores que más confían en entregar sus servicios y almacenamiento y tratamiento de aplicaciones y datos a servicios Cloud son los sectores de Transporte, Hostelería y Servicios. Probablemente, se debe a que se prefiere que sea un tercero quien gestione y mantenga los servicios, puesto que son empresas donde los departamentos de IT no son especialmente maduros y, al mismo tiempo, no se almacena información tan crítica como puede ser la que manejan otros sectores, por ejemplo, la banca.

En contraposición, observamos **que los que menos confían sus servicios al Cloud Computing son los sectores de Telecom, Media y Tecnología y banca. Se entiende que ellos mismos son capaces, por el sector al que pertenecen, de mantener este tipo de infraestructuras "In House".**

Sectores que menos confían en Cloud Computing

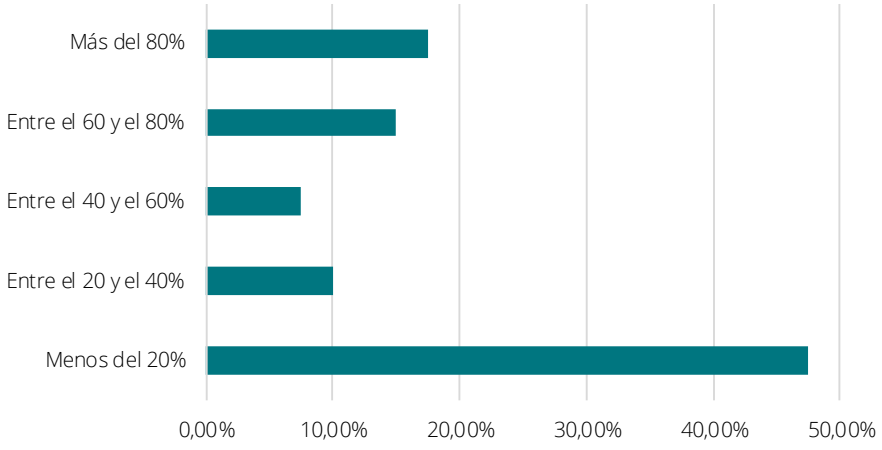


¿Qué porcentaje de ellos son servicios imprescindibles/críticos para la empresa?

Como era de esperar, menos del 20% de los servicios que son imprescindibles/críticos para la empresa están alojados en la nube. Las empresas prefieren mantener los servicios "In House" y no delegar en un tercero Cloud el manejo de estos servicios, a pesar, de que se espera para los próximos años un cambio de tendencia.

Además, las estrictas normativas de protección de datos complican el control de las infraestructuras en la nube. Los datos que se tratan en cada uno de los servicios críticos, en el momento que adquieren un carácter alto de criticidad, adquieren una dificultad adicional en caso de que se quieran sacar fuera de la propia infraestructura.

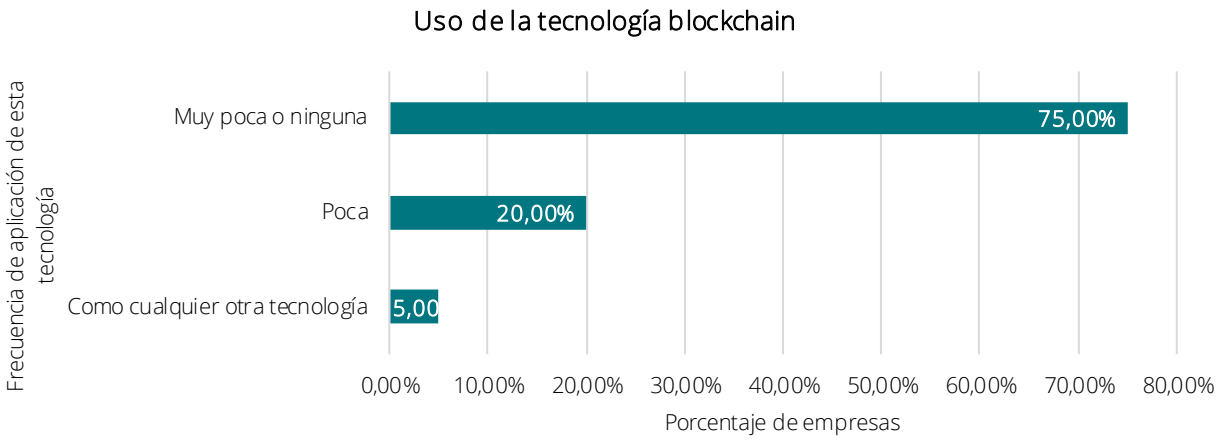
Porcentaje de servicios críticos que están alojados en la nube

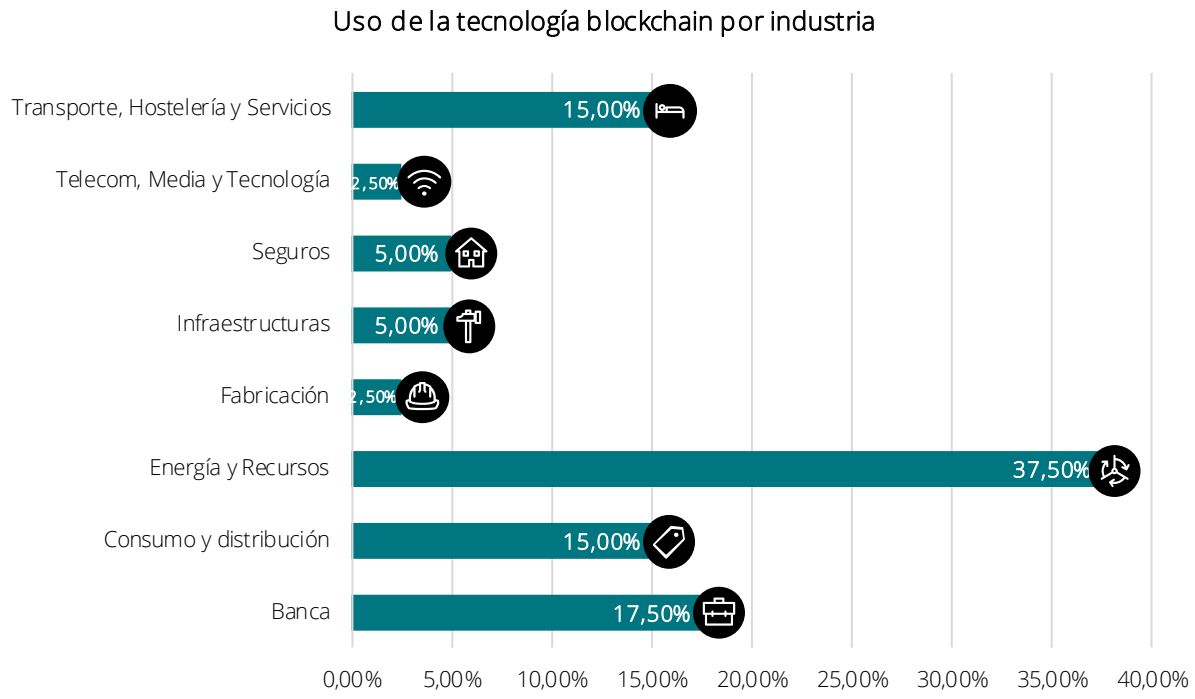


¿Qué implicación tiene la tecnología de Blockchain **en la ciberseguridad** de su empresa actualmente?

Se ha verificado que el 95% de los sectores tienen poca o ninguna implicación de la tecnología Blockchain en la ciberseguridad en su empresa. Esto evidencia que a pesar de ser una tecnología muy potente, actualmente son muy reducidos los casos de uso donde esta se puede aplicar.

Solamente el 5% de los sectores emplea la tecnología Blockchain como una tecnología más para la ciberseguridad de la empresa, destacando entre estos los siguientes: energía y recursos (37,5%) y banca (17,5%).





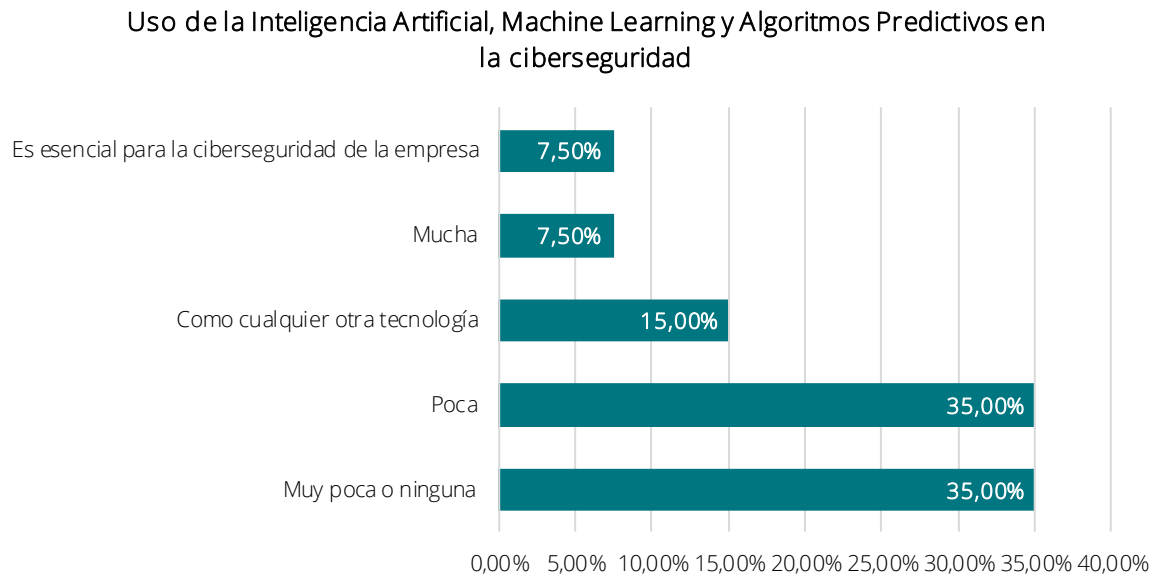
Se puede concluir que, aunque el uso de la tecnología Blockchain haya experimentado un aumento considerable en los últimos años, sobre todo gracias a la aparición de las criptomonedas como Bitcoin, Ethereum, Litecoin, etc. esta tecnología todavía no se adecua a los casos de usos de los procesos de negocio de las empresas de los diferentes sectores. Por otro lado, la falta de profesionales con conocimientos avanzados en esta tecnología, hacen que su despliegue todavía no sea muy elevado.

¿Qué implicación tienen las tecnologías como Inteligencia Artificial, Machine Learning y Algoritmos Predictivos **en la ciberseguridad** de su empresa actualmente?

Se ha contrastado que el 70% de los sectores cuenta con una implicación baja o muy baja de las tecnologías como Inteligencia Artificial, Machine Learning y Algoritmos Predictivos en la ciberseguridad.

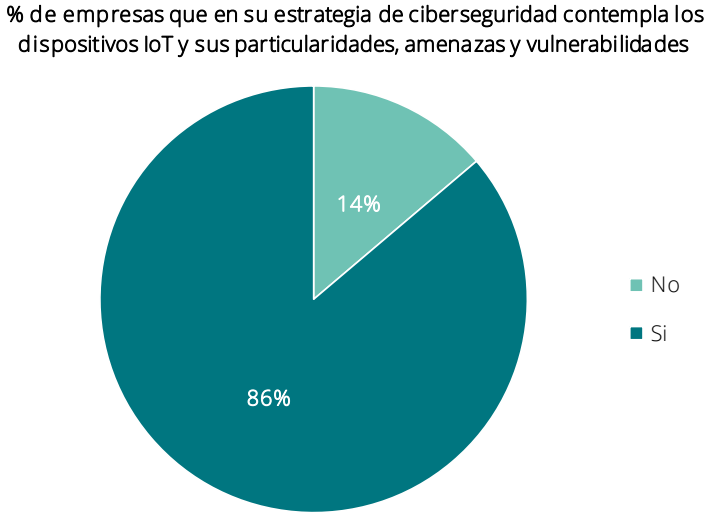
El 15% de los sectores utiliza estas tecnologías como cualquier otra tecnología de las empresas, mientras que solo el 7,5% cuenta con una alta implicación de estas en materia de ciberseguridad.

Solo para el 7,5% de los sectores son esenciales estas tecnologías.

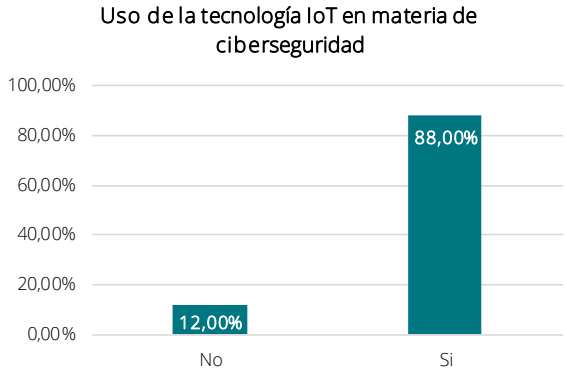


Se puede observar que estas tecnologías **ya tienen implicación en la ciberseguridad** de las empresas y se espera que ésta vaya creciendo en los próximos años. Puesto que ya se usan como herramientas avanzadas para examinar grandes cantidades de información y reconocer así posibles amenazas.

¿Su estrategia de ciberseguridad contempla los dispositivos IoT y sus particularidades, amenazas y vulnerabilidades?

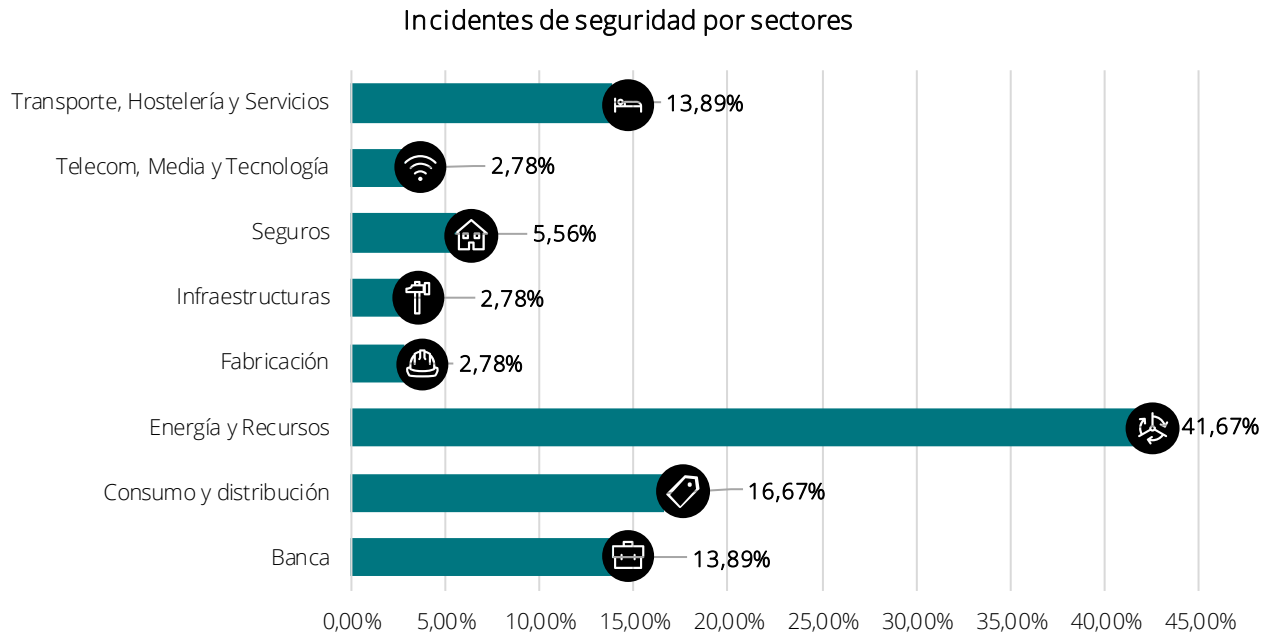


Se ha verificado como el 86% de las empresas contempla los dispositivos IoT en su estrategia de ciberseguridad y el 14% no contempla estos dispositivos. A diferencia de otras tecnologías más disruptivas, IoT sí que está presente en la estrategia de ciberseguridad de las empresas.

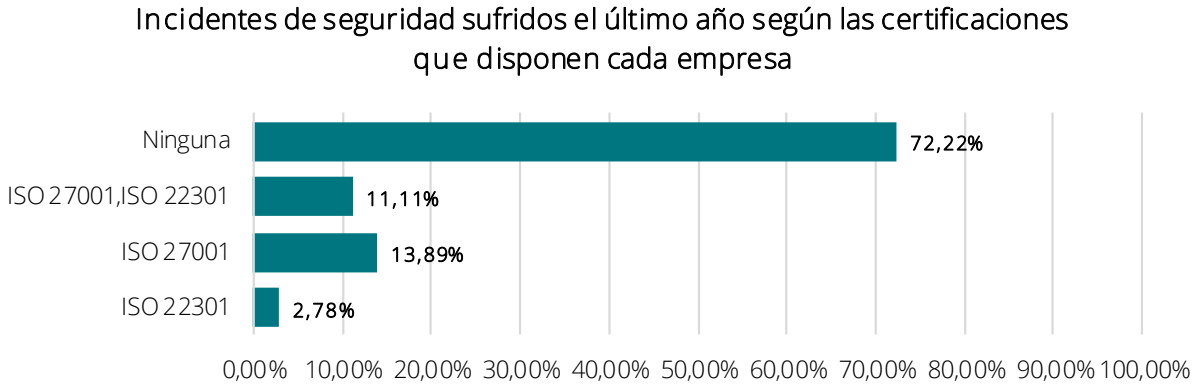


Incidentes de seguridad

¿Cuántos incidentes de seguridad con consecuencias significativas/graves se producen en su empresa al año?

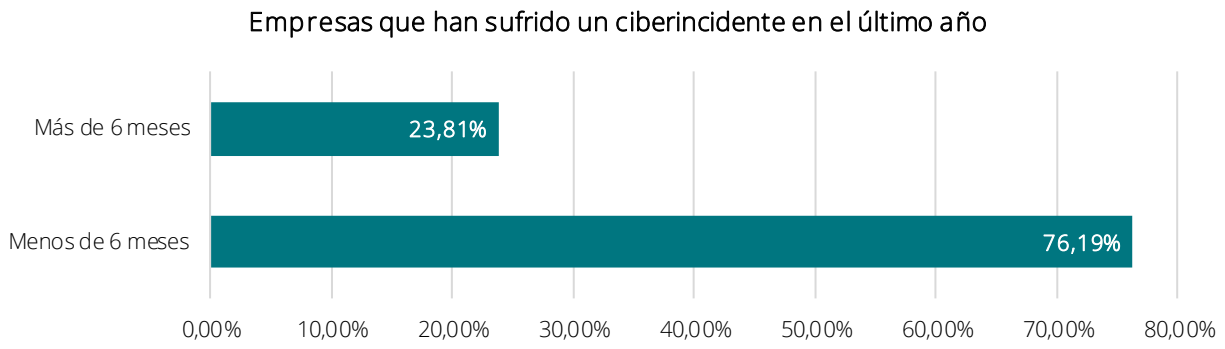


Se ha verificado que los dos sectores con más incidencias son el de energía y recursos con un 41,67% y el de consumo y distribución con un 16,67% respecto al total de incidencias. Esto se debe a que los entornos OT son los más susceptibles a sufrir incidentes debido al bajo nivel de seguridad de dichas infraestructuras.



Como ya se mencionó anteriormente, es más probable sufrir incidentes de seguridad si no se dispone de ninguna certificación. Esto se debe a que normalmente estas certificaciones suelen exigir a las empresas un mínimo de seguridad que, a su vez, minimiza los ciberincidentes o minimiza sus impactos. Las empresas que no tienen ninguna certificación tienen un 72,22% de incidentes, mientras que las que tienen la ISO 27001 tienen un 13,89%, las que cuentan con la ISO 27001 y la ISO 22301 tienen un 11,11% y, por último, las que cuentan con la ISO 2,78% tiene un 2,78% de incidentes

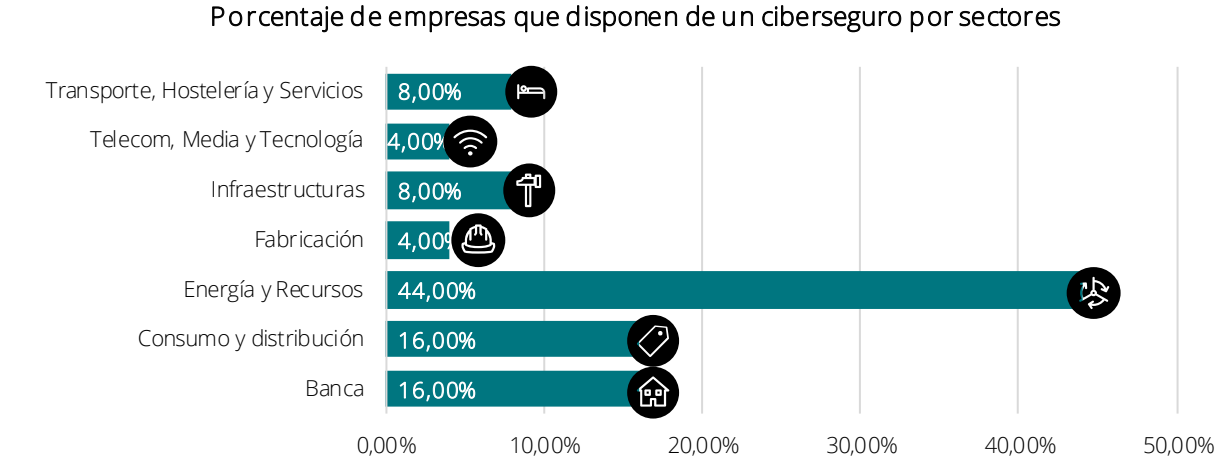
.



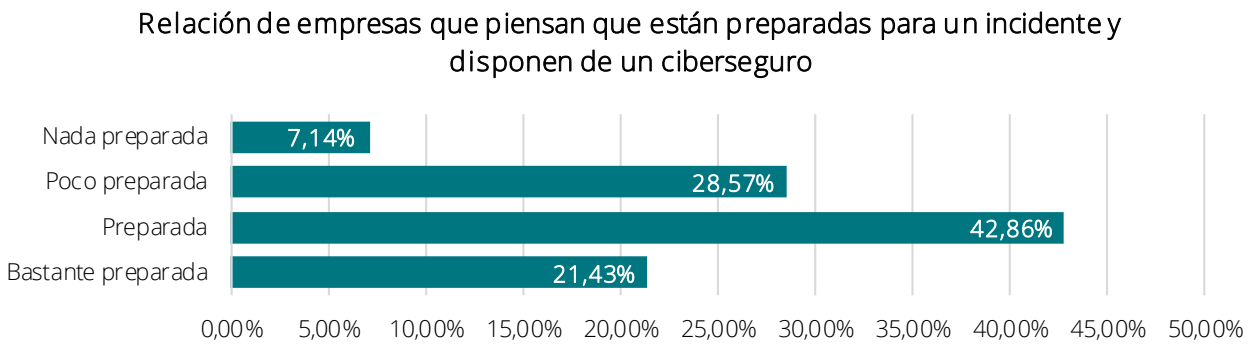
El 76,19% de las empresas han tenido un incidente con consecuencias significativas en los últimos 6 meses, frente al 23,81% han registrado el último incidente hace más de 6 meses.

El 62,50% de las empresas han tenido menos incidencias en 2018 que en 2017, mientras que un 37,5% ha registrado más incidencias en 2018 que en el año 2017. Aunque el número de ciberamenazas ha aumentado con el paso del tiempo, así como su probabilidad e impacto, la muestra de empresas afirma haber sufrido menos incidentes en el 2018 que en el 2017. Esto se debe a qué en el 2017 el conocido Wannacry y el Petya afectaron masivamente a un número elevado de empresas. Por ello, en el 2018 se ha registrado un menor número de incidentes a pesar de que el escenario de riesgos es mayor.

En relación al ciberseguro:

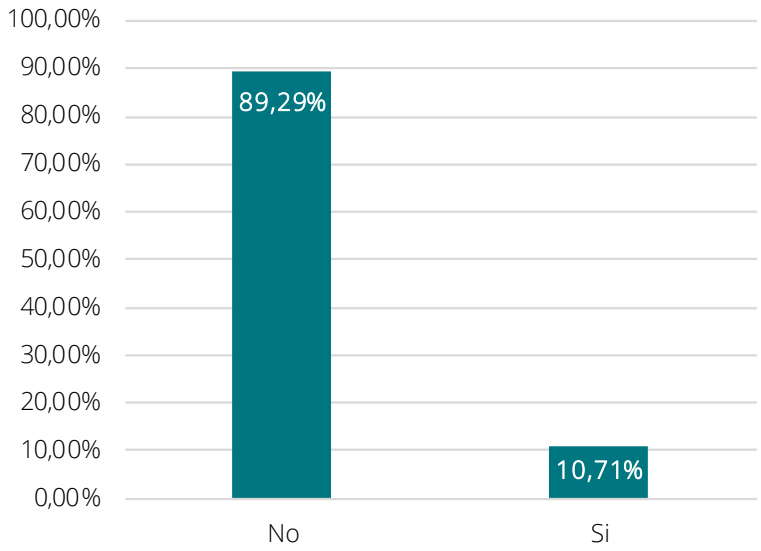


Cabe destacar que el 44% de las empresas del sector de energía y recursos y el 16% de las empresas del sector de energía y recursos y banca cuentan con un ciberseguro.



El 42,86% y el 21,43% de las empresas que piensan que su empresa está preparada y bastante preparada respectivamente, para hacer frente a incidentes de seguridad cuentan con un seguro ante ciberincidentes. Mientras que solamente el 7,14% de las empresas que piensan que su empresa no está preparada para hacer frente a un ataque cuenta con un ciberseguro.

El 89% de las empresas que tienen un ciberseguro no lo han tenido que utilizar nunca y solamente el 10,71% de las empresas que tienen un ciberseguro han tenido que hacer uso del él en algún incidente.



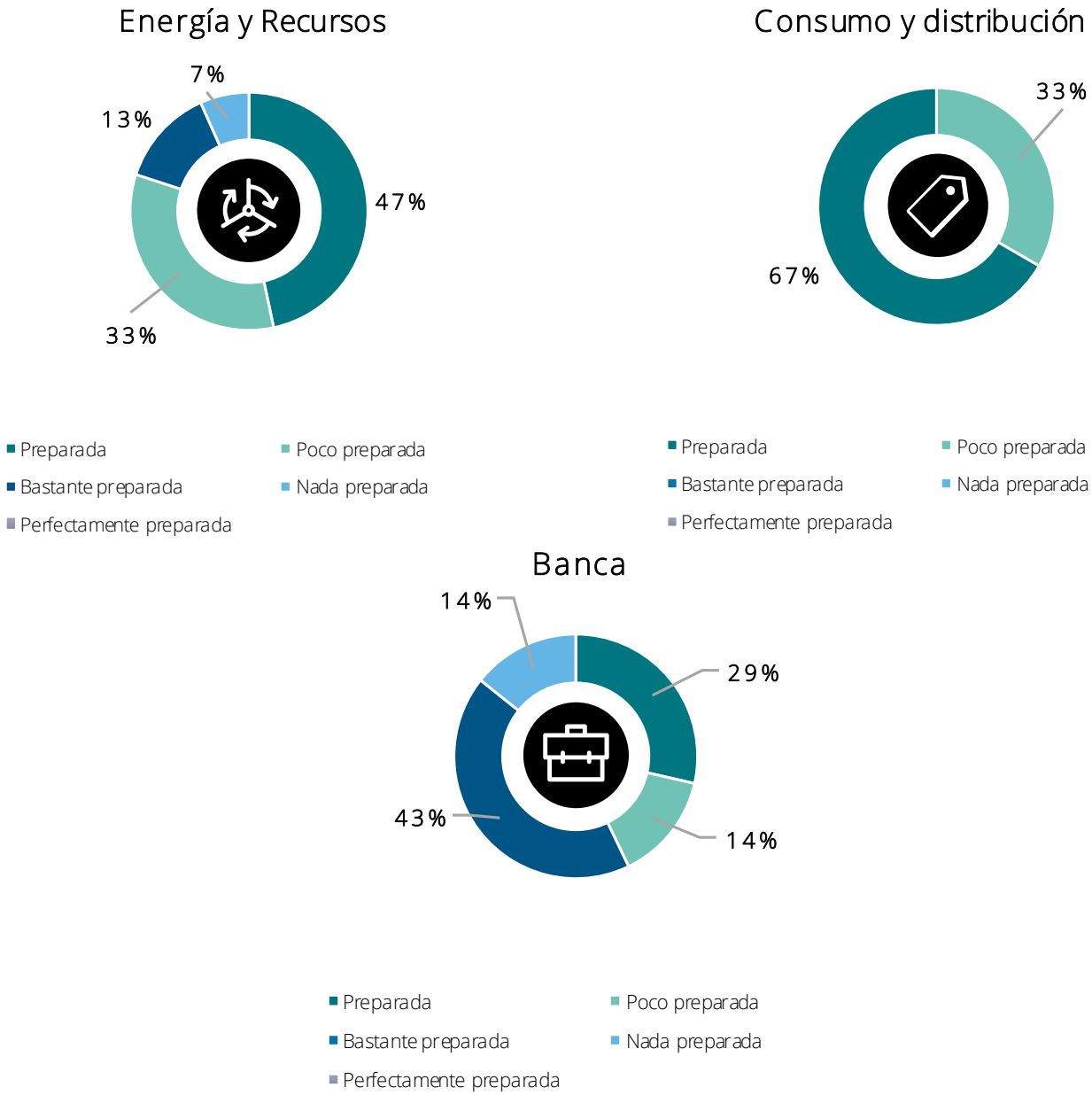
Percepción del CISO

¿Cómo de preparada cree que se encuentra su empresa para hacer frente a incidentes de seguridad?

Se puede concluir que una de cada tres empresas se considera que está poco o nada preparada para hacer frente a un incidente de seguridad.

Si se realiza el análisis por tres de los sectores claves como son: Banca, Energía y Recursos y Consumo y distribución se obtienen los siguientes resultados.

- Energéticas y Recursos:
  - **Menos del 50%** de las empresas Energéticas y Recursos **se siente preparadas** para afrontar un incidente de seguridad. Es un dato bastante destacable al ser uno de los sectores crítico y estratégico para cualquier país.
  - Solo el 13% se siente bastante preparadas, mientras que unas de cada tres empresas están poco preparadas.
- Banca:
  - El 86% se siente preparada, bastante o perfectamente preparada para hacer frente a un incidente de seguridad.
- Consumo y Distribución
  - **Dos de cada tres empresas está poco preparada** y solo una de cada tres se siente preparada.



En conclusión, el sector más preparado es la Banca a mucha diferencia con el sector Energético/Recursos y Consumo/Distribución.

El 71% de las empresas que se sienten poco o nada preparadas para hacer frente a un incidente de seguridad optan por la opción del Ciberseguro.

¿Cómo ordenaría los siguientes riesgos generados por ciberamenazas según la preocupación que genera en su empresa cada una?

A continuación, vemos el porcentaje de CISOS que consideran como principal preocupación:

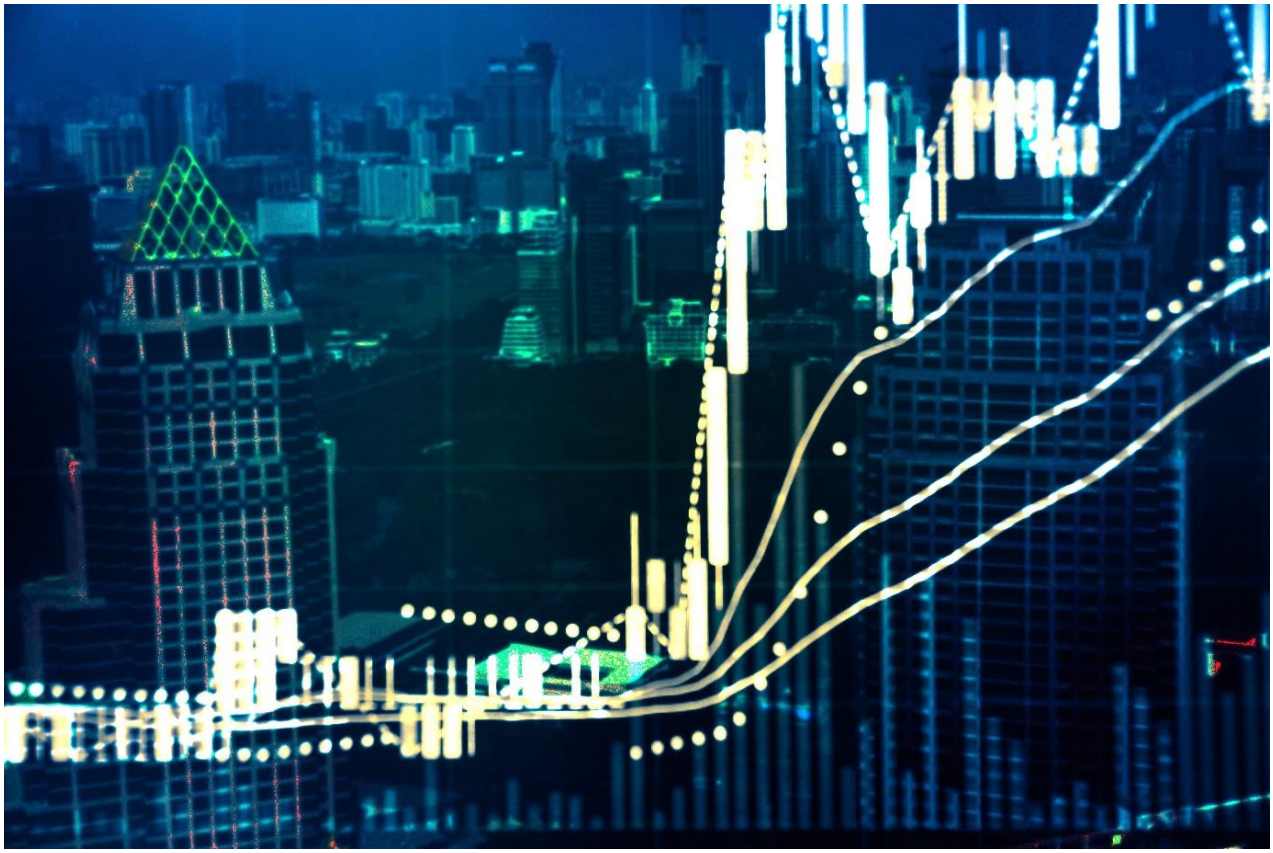
1. Interrupción de las operaciones de negocio. 64,1%
2. Riesgo reputacional. 23,1%
3. Fuga de información confidencial. 33,3%
4. Fraude económico. 23,1%
5. Falta de cumplimiento normativo. 10,3%
6. Riesgo geopolítico 2,6%

- El 93% de las energéticas y recursos consideran la interrupción de las operaciones de negocio como su principal preocupación.
- Los CISOS que consideran la fuga de información confidencial como primer o segundo principal riesgo tiene internalizado el DPO, exactamente en un 83% de los casos.

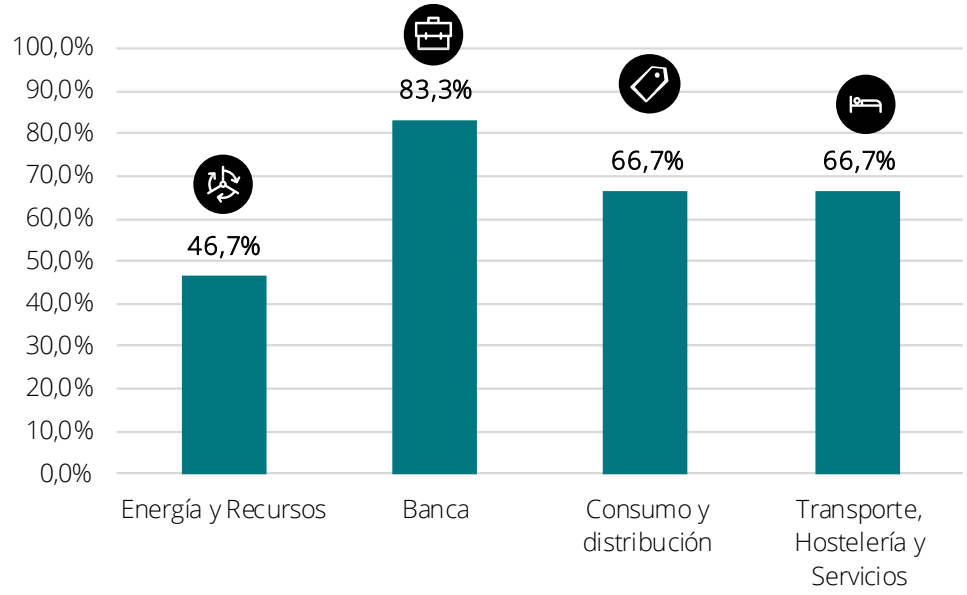
¿Cómo ordenaría las siguientes labores fundamentales del CISO de mayor a menor importancia?

A continuación, vemos el porcentaje de CISOS que consideran como principal preocupación:

- Alinear la estrategia de ciberseguridad con el negocio. 64,1%
- Evaluar e implementar las medidas de seguridad y estándares necesarios. 25,6%
- Entender al completo el entorno de amenazas y manejar con efectividad el programa de Seguridad de la Información. 23,1%
- Desarrollar y gestionar el cumplimiento de las políticas de ciberseguridad. 12,8%



Por **sectores**, el porcentaje de empresas que consideran **alinear la estrategia de ciberseguridad con el negocio** como labor fundamental:



Más del 80% de la Banca alinea la estrategia Cyber con el negocio, muy por detrás del sector Energético y Recursos que no llega al 50%.

¿Cómo ordenaría las siguientes tareas de su agenda ordenadas de mayor a menor prioridad?

A continuación, vemos el porcentaje de CISOS que consideran como principal preocupación:

- **Implicarse en los proyectos de ciberseguridad más relevantes. 94,74%**
- **Evaluar y monitorizar la estrategia de Seguridad de la Información. 73,68%**
- Preparar el material para los comités. 26,32%
- Mantener reuniones con los líderes de otras áreas de Negocio. 15,79%
- Mantener reuniones uno a uno con cada empleado del departamento de ciberseguridad. 10,53%
- Formar al equipo de Formación y Concienciación. 10,53%
- Ajustar el presupuesto de ciberseguridad mes a mes. 5,26%

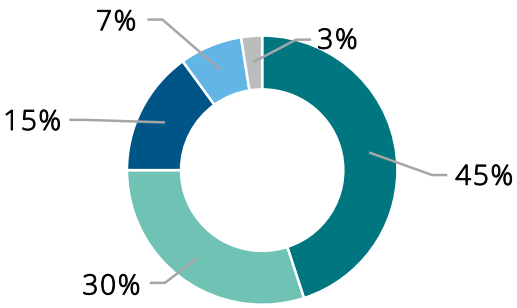
Se puede apreciar como contrasta que los CISOs a pesar de considerar la alineación de la estrategia de ciberseguridad con el negocio como uno de los aspectos más importantes en el 64,1% de los casos, luego esto no se refleja en su agenda, puesto que muchos de ellos a pesar de involucrarse en la estrategia, solo ponderan en su agenda las reuniones con otros líderes de negocio en el 15,79% de los casos como algo prioritario.

El 95% de los CISOs considera que lo más importante en su agenda es estar involucrado en los proyectos más importantes de ciberseguridad.

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

A continuación, se puede observar el nivel de concienciación de las empresas en cuanto a la ciberseguridad:

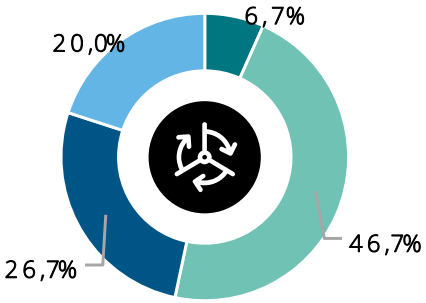
- El 60% consideran un tema clave o importante, mientras que **casi 1 de cada 3 empresas le siguen sin dar demasiada importancia** a la ciberseguridad.
- Casi la mitad de las empresas, un 45%, considera un tema importante y trata de manera periódica la ciberseguridad de la empresa.



- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta, pero no se le da demasiada importancia
- Es un tema clave que se trata semanal o mensualmente
- Sólo se considera cuando hay un incidente grave
- NS/NC

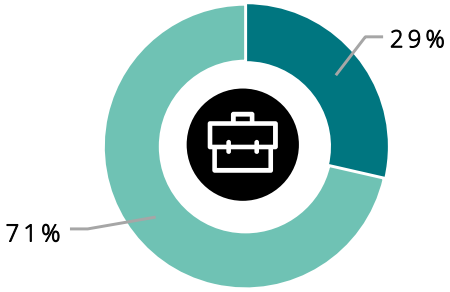
Por sectores:

Energía y Recursos



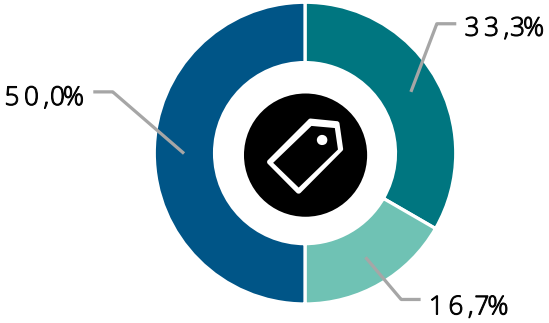
- Es un tema clave que se trata semanal o mensualmente
- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta, pero no se le da demasiada importancia
- Sólo se considera cuando hay un incidente grave

Banca



- Es un tema clave que se trata semanal o mensualmente
- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta, pero no se le da demasiada importancia
- Sólo se considera cuando hay un incidente grave

Consumo y distribución



- Es un tema clave que se trata semanal o mensualmente
- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta, pero no se le da demasiada importancia
- Sólo se considera cuando hay un incidente grave

El **100% en el sector Banca** considera que es un tema **clave** que se trata semanal o mensualmente o considera un tema **importante** y se trata periódicamente.

En Energías y Recursos más de una de cada cuatro empresas lo tiene en cuenta, pero no le da demasiada importancia.

El **100% de las empresas** que se siente **bastante o perfectamente preparadas** para hacer frente a un incidente de seguridad **consideran a la ciberseguridad un tema clave o importante** y tratan de manera periódica (semanal o mensual).

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

Rubén Frieiro
Socio Cyber Risk Advisory
rfrieiro@deloitte.es

Xavier Gracia
Socio Cyber Risk Advisory
xgracia@deloitte.es@deloitte.es

Andrés Bravo
Socio Cyber Risk Advisory
abravosanchez@deloitte.es

Adolfo Pedriza
Socio Cyber Risk Advisory
apedriza@deloitte.es

Nicola Espósito
Socio Cyber Risk Advisory
niesposito@deloitte.es

Juan Antonio Santos
Socio Cyber Risk Advisory
jsantosgonzalez@deloitte.es

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

Deloitte.