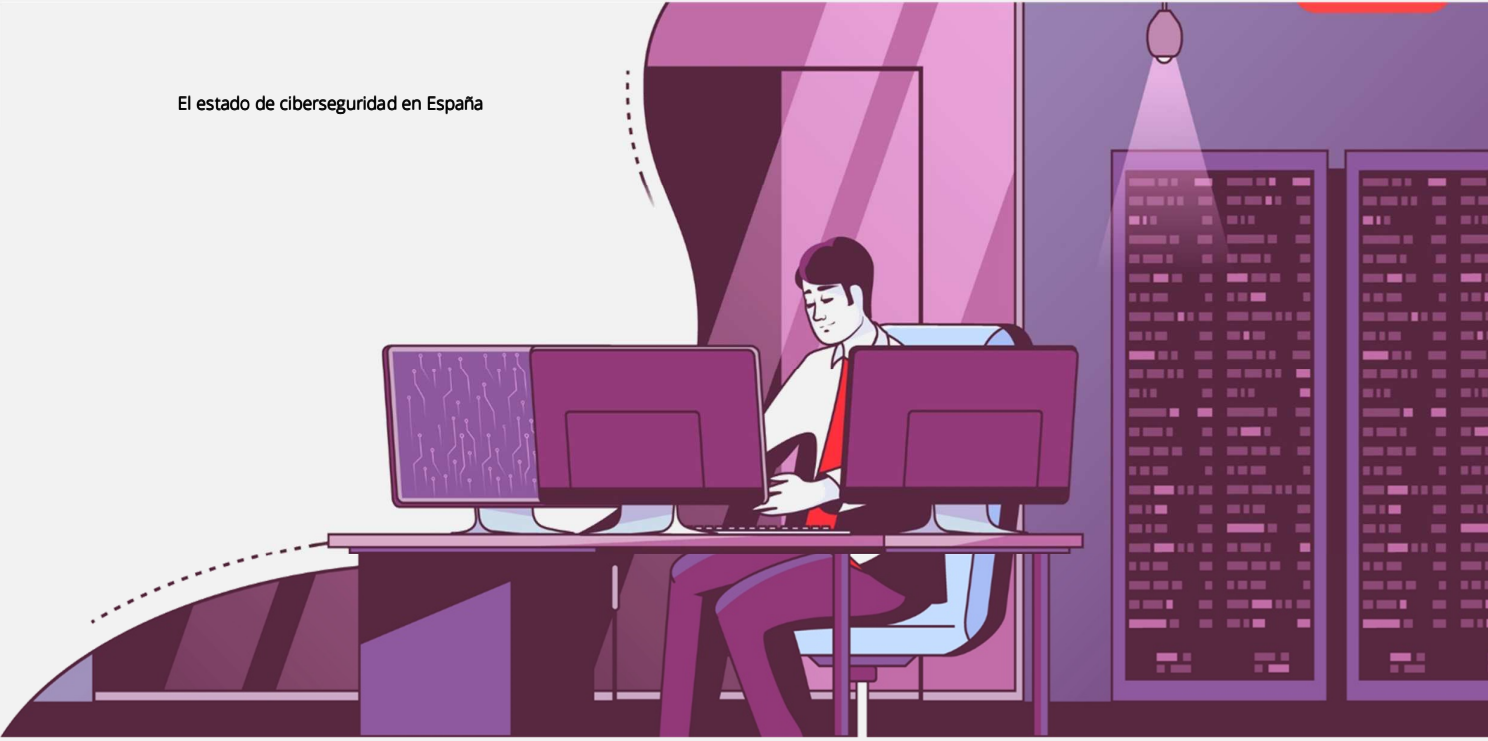
Deloitte.

El estado de la ciberseguridad en España

Digitalización, teletrabajo y ciberataques en tiempos de pandemia

Cyber Strategy Transformation and Assessment

Contenido



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 CISO[1]s 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, en el perfecto equilibrio entre el conocimiento técnico y estratégico, así como en nuestra propia fuente de conocimiento. Gracias a ello, disponemos del know-how de sectores, tendencias, ciber amenazas, 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

Gracias a esta información, las empresas pueden conocer más de cerca cómo están dimensionadas y cómo están trabajando otras empresas en materia de ciberseguridad, en muchos casos a nivel sectorial.

Esta segunda edición del estudio nace con la aspiración de poder resolver algunas dudas que son objeto de preocupación de los CISOs españoles en el 2020.

En el proceso de toma de decisiones, la dirección de las compañías debe realizar un ejercicio de análisis interno de fortalezas y debilidades, pero también tener una referencia externa sobre las tendencias y lo que están haciendo el resto de los competidores para poder tener una base comparativa.

Nuestro objetivo es el de compartir con la sociedad el estado de la ciberseguridad en las empresas españolas.

El equipo de Cyber Strategy, Transformation and Assessment de Deloitte ha realizado un ejercicio de entendimiento sobre una muestra de más de 100 empresas españolas y/o cuya base de operaciones de seguridad reside en España.

[1] Chief Information Security Officer or Cybersecurity Officer

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 CISOs en diferentes foros:

01 Headcount [2] y SOC [3]

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.

02 Presupuesto y servicios

Sin lugar a duda, el aumento de los ciber ataques y la necesidad de mayor ciberseguridad obligan a los CISOs a demandar mayores presupuestos año a 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 futuro ahorro de costes (al evitar y gestionar eficazmente los posible ciber incidentes) y no solo como un puro gasto más para el negocio.

03 Target Operating Model [4]

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.

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. Que certificaciones y *frameworks* abordar suele ser objeto de debate y discusión entre los diferentes CISOs, al no haber un verdadero consenso sobre cuáles son los más útiles o demandados en el mercado.

05 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 debido a su relevancia actual. En este dominio o tema 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 el IoT [5].

[2] Número de personas

[3] Security Operation Center

[4] Modelo operativo y organigrama

[5] Internet of Things

06 Entorno regulatorio

La sociedad, en general, y los gobiernos en particular se han dado cuenta de la necesidad de regular cada vez más acerca las medidas de ciberseguridad que las entidades deben implementar.

Un problema muy común en ciertas organizaciones es el hecho afrontar el cumplimiento normativo como una necesidad impuesta, en vez de una oportunidad para revisar en profundidad los modelos y procesos de ciberseguridad implantados en la organización de forma periódica.

07 Incidentes de seguridad

Probablemente la mayor preocupación de los CISO es saber cuándo y cómo recibirá el siguiente ciberataque o ciber incidente. Para facilitar una respuesta, se analizarán cuáles son las estadísticas de incidentes en los últimos años de diferentes empresas y qué papel jugó el ciberseguro entre otros para, de esta manera, tener una referencia comparativa del mismo.

08 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.

09 Percepción del CISO en tiempos de pandemia

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 estrés para los CISOs, puesto que el contexto de la empresa ha cambiado lo suficiente como para adaptar y replantear rápidamente los modelos de ciberseguridad ante esta nueva realidad.

La COVID-19 ha supuesto todo un reto para las organizaciones en términos de digitalización y ciberseguridad.

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.

En cuanto a la calidad del dato hay que tener en cuenta que este estudio se realizó en una muestra de más de 60 empresas a nivel nacional.

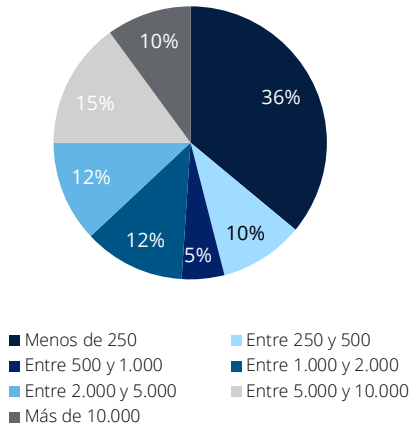
Facturación

Se puede apreciar que un 46% de las empresas encuestadas factura menos de 500 millones de euros, frente a un 29% que se mueve en la horquilla de los 500 hasta los 5.000 millones de euros de facturación anual. El resto de la muestra, **25%, son empresas con una facturación superior a los 5.000 millones.**

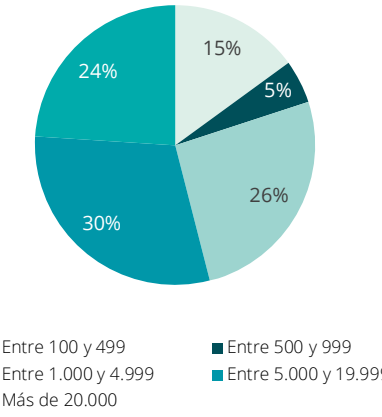
Headcount

La segunda perspectiva es el **número de empleados** en plantilla que disponen las empresas. En esta perspectiva, podemos ver que un 15% 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 31% de la muestra se sitúa entre los 500 y los 5.000 empleados y el 54 % restante incluye aquellas empresas con más de 5.000 empleados en plantilla.

Facturación
(Millones de Euros)



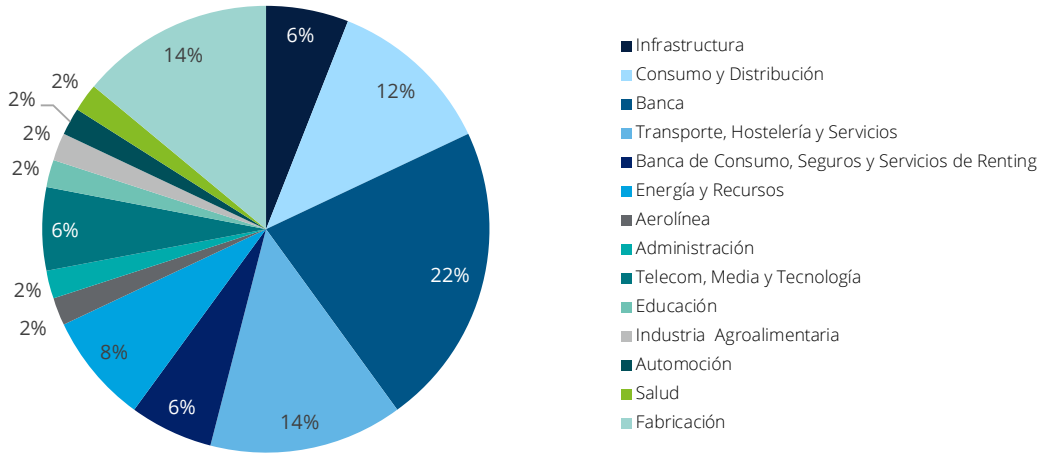
Volumen de empleados



Sectores

Por volumen de empresas, en orden descendente, son: Banca, con un 22% de las empresas; Transporte, Hostelería y Servicios y Fabricación, cada uno con un 14% de participación; y, finalmente, Consumo y Distribución, con un 12%. El resto de los sectores en conjunto suponen un 38% del total de las empresas representadas.

Sectores de actividad



Principales conclusiones del estudio

Headcount y SOC

Más del 70% de las empresas encuestadas destinan menos de 10 empleados a la ciberseguridad. De ellas, casi un 60% está por encima de 1.000 empleados en su organización.

Es evidente que un año más continúa la **tendencia a la externalización de los servicios de ciberseguridad, como se ha observado en el 76% de las organizaciones analizadas**.

Más del 70% de las organizaciones que ha participado cuenta con un Centro de Operaciones de Seguridad (SOC), y de estas, un 60% ha optado por un modelo de servicio totalmente externalizado o híbrido.

Presupuesto y servicios

La tendencia al alza en las empresas españolas a invertir en ciberseguridad de IT[6]/OT[7], que se ha observado en ocasiones anteriores, se cumple también este año, pasando de un 8,5% sobre el total de IT/OT de sus presupuestos [8]en 2018, al 9% en 2019. A su vez, las organizaciones, dedican más de un 60% a servicios externos y, de estos, más de la mitad a operaciones.

Se ha encontrado una relación entre las empresas que destinan menos de un 3% de su presupuesto de IT/OT a ciberseguridad y una mayor cantidad de incidentes significativos de ciberseguridad, pudiendo llegar hasta dos al año de media. Por tanto, se evidencia la necesidad de destinar mayor porcentaje del presupuesto IT/OT si se quiere minimizar los ciber incidentes.

Se puede observar que la tendencia general en España es que **el CISO, en el 60% de los casos, percibe un salario bruto anual menor de 80.000€**.

Más del 70% de las empresas encuestadas destinan menos de 10 empleados a la ciberseguridad. De ellas, **casi en la mitad de las empresas (46%) el CISO tiene una dependencia directa del CIO**.

Cabe destacar que solo el 6% de los CISOs encuestados afirma que percibe un salario de más de 120.000€ brutos.

Target Operating Model

En relación con el modelo de gobierno de ciberseguridad, el estudio arroja unos resultados concluyentes donde **casi en la mitad de las empresas (46%) el CISO tiene una dependencia directa del CIO**.

En segundo lugar, se aprecia todavía una dependencia directa del responsable de Tecnología e Información, donde el 20% de las empresas muestra que la seguridad sigue formando parte de las áreas de tecnología e información. Esto evidencia aun la falta de visibilidad y reporte del CISO a la alta dirección.

[6] Information Technology

[7] Operation Technology, típicamente de los entornos industriales

[8] Excluyendo empleados internos e incluyendo el licenciamiento de herramientas exclusivas de ciberseguridad

La preocupación y concienciación sobre la ciberseguridad en las empresas se aprecia en que **el 91% de las mismas cuenta con un Comité de Seguridad.**

No obstante, todavía es necesario empoderar el rol del CISO, ya que solo el 69% de ellos acude a dicho comité. Este es un dato preocupante.

Desde la perspectiva de la capacidad de reacción y la toma de decisiones ante un incidente de ciberseguridad, se observa un descenso en la tendencia de formalizar comités específicos para la respuesta a incidentes, dado que **solo el 44% de las empresas cuenta con un Comité de Respuesta a Incidentes específico**. Esto pone de manifiesto que, ante tales escenarios, más de la mitad de las empresas encuestadas consensúa las acciones que deberán llevarse a cabo para contener un incidente en comités con objetivos distintos, o en estructuras intermedias no formalizadas.

En cuanto a la coexistencia con otros comités, se observa que el 46% de las empresas que cuenta con un Comité de Seguridad dispone también de un Comité de Respuesta a Incidentes y de un Comité de Crisis, dejando clara la creciente apuesta por un gobierno efectivo de la seguridad y por una buena capacidad de resiliencia.

Los sectores enfocados en el transporte, como aviación y automoción, y en consumo y distribución, son los que actualmente presentan una menor formalización en la gestión ejecutiva de la seguridad, ya que el 32% de las empresas de estos sectores no dispone de ningún comité específico relacionado con la seguridad.

Con respecto a las responsabilidades del CISO, destaca en primer lugar la definición y gestión de políticas de seguridad, y en segundo, la gestión de las operaciones de seguridad de la empresa.

Por otra parte, tanto la privacidad como la seguridad física siguen fuera de las responsabilidades del CISO en muchos casos, reflejándose el hecho de que las empresas optan preferiblemente por el nombramiento de figuras independientes para asumir esos roles específicos.

Certificaciones, framework y formación

En lo que respecta a las certificaciones, cabe mencionar que **el 60% de las organizaciones indica no poseer ninguna específica en el ámbito de ciberseguridad**. Este dato pone de manifiesto uno de los grandes problemas con respecto a los procesos de certificación: se ve de forma negativa el esfuerzo que suponen, a pesar de que permiten mejorar la gestión y la madurez de la ciberseguridad, además de aumentar el valor de los servicios y productos de las compañías.

De las empresas que poseen certificaciones, solo el 30% de ellas está certificada en ISO/IEC 27001, y de estas, el 67% posee además la ISO 22301. Esta fuerte relación entre ambas ISOs simplemente refleja la relativa "facilidad" con la que se puede implantar un sistema de gestión una vez se está familiarizado con su metodología.

Otra de las grandes preocupaciones de los CISOs es su propia formación. **El 70% de los CISOs posee algún tipo de certificación relacionada con alguno de los aspectos de la ciberseguridad, siendo las tres más habituales CISM (40%), CISA (32%), e ISO 27001 Lead Auditor (23%).**

El 60% de las organizaciones indica no poseer ninguna específica en el ámbito de ciberseguridad.

Por otra parte, las certificaciones centradas en las partes más técnicas de la ciberseguridad como son CISSP, CEH o CCSP, cobran más importancia en los equipos de gestión de operaciones que reportan al CISO.

Aunque con anterioridad se ha comentado que un 30% de las organizaciones posee una certificación ISO/IEC 27001, cuando se pregunta el *framework* que se utiliza para la gestión de la ciberseguridad, casi el 75% de los encuestados sigue la ISO como estándar para el desarrollo de su función de seguridad. Esto evidencia que sigue siendo un estándar de referencia, a pesar del bajo porcentaje de entidades que ostentan dicha certificación.

Es de resaltar cómo el 28% de las empresas utiliza el Deloitte CSF como marco de ciberseguridad, aumentando en un 10,5% respecto al año anterior.

En cuanto a sectores que hacen uso de entornos industriales (Energías y Recursos, Fabricación, Automoción, Consumo y Distribución, etc.) pese a la existencia de marcos especializados como ISA 62443 o NIST 800-82, estos solo se utilizan por el 5% de las organizaciones. Este dato evidencia el **bajo nivel de madurez en ciberseguridad industrial**.

Con respecto a formación y concienciación de los empleados de las organizaciones en materia de ciberseguridad, se observa que se realizan una media de **25 horas anuales por empleado en formación y unas 130 en concienciación**. Con respecto al formato en el que se imparten tanto la formación como la concienciación, domina el **formato online o mixto** online-presencial. Debido a la pandemia sufrida este 2020 estos datos han aumentado y se prevé que sigan aumentando en el futuro.

Se debe destacar también que solo 1 de cada 4 empresas no realiza ningún tipo de actividad de formación.

Los empleados, y su gestión del email, son uno de los vectores de entrada de software más utilizados, por lo que se entiende que su falta de formación puede provocar en el medio y largo plazo más incidentes de ciberseguridad.

Revisiones de seguridad, entornos *cloud* y tendencias tecnológicas

En lo que respecta a las revisiones de aplicaciones, un 59% de las organizaciones las realiza solo sobre la mitad de aquellas aplicaciones de su negocio consideradas como críticas; **solo el 20% de las organizaciones afirma realizar revisiones de seguridad en la totalidad de sus aplicaciones críticas**.

Preocupa el hecho de que la mayoría de las organizaciones revisa menos de la cuarta parte de sus aplicaciones, dado que no ofrecen un respaldo de seguridad a un porcentaje elevado de su negocio.

En cuanto a la periodicidad con la que se realizan dichas revisiones, la más habitual, en un 42% de los casos, es cada doce meses o menos. En este rango, destacan sectores como el de Seguros, en los que el 100% de ellos tiene esa periodicidad; Transporte, Hostelería y Servicios, con un 80%; y Banca y Fabricación, ambos con un 75%.

La fuerte tendencia en los últimos años a migrar servicios a la nube se refleja en el **96% de las organizaciones que tienen aplicaciones en *cloud***.

Algunos sectores están muy concienciadas, a tener de cómo se realiza este cambio de paradigma, como es el caso de Energía y Recursos, donde se afirma en el 100% de los casos que poseen una estrategia definida para migrar a *cloud*; destaca también el sector de Fabricación, en el que el 83% de las organizaciones posee una estrategia en este contexto.

Si vamos más allá de la estrategia y nos centramos en la existencia de un marco de controles específicos para cloud, vemos que solo un 65% de la totalidad de las organizaciones posee uno. De hecho, **de las empresas que poseen una estrategia para *cloud*, solo en el 77% de los casos dicha estrategia se ha traducido en un marco de controles**.

Con respecto a otros sectores, como “Energía y Recursos” y “Consumo y Distribución” en el 80% de los casos se dispone al mismo tiempo de una estrategia y un marco de controles específico para *cloud*.

Siguiendo con las tendencias de los últimos años, vemos que un **87% de las organizaciones tiene dispositivos IoT, pero solo el 56% de las mismas contempla en su estrategia de ciberseguridad las necesidades específicas de estos dispositivos, las amenazas y sus vulnerabilidades**. Dado que muchos de estos dispositivos no suelen estar diseñados desde el punto de vista de la seguridad, las organizaciones deben centrarse en desarrollar sus capacidades de gobierno, protección, vigilancia y resiliencia, de tal forma que abarquen este tipo de elementos cuyo uso está en aumento.

Analizando los resultados desde el punto de vista sectorial, vemos que, según las respuestas dadas por el sector de Fabricación, el 100% incluye las particularidades de IoT en su estrategia de ciberseguridad y el 60% en el caso de los sectores de Consumo y Distribución y de Energía y Recursos. En la parte baja, nos encontramos a la Banca, en la que la mitad de las organizaciones utiliza dispositivos de IoT y solo el 14% de ellas diseña estrategias de ciberseguridad para ello.

Entorno Regulatorio

El entorno regulatorio tanto a nivel nacional como internacional ha estado aumentando en los últimos años.

Según se deduce de los resultados, la regulación no tiene buena acogida en las empresas españolas. **Solo el 25% de las empresas considera que la regulación que les aplica es necesaria y, del resto, el 23% matiza que esta es demasiado generalista.**

Por otra parte, con respecto a la apreciación de la efectividad de dicha regulación, solo un 11% considera que es eficaz, mientras que un 17% la califica directamente de ineficaz.

Cuando se ha pedido a los encuestados que valoren la oferta de servicios de ciberseguridad del mercado, un 34% la ha considerado madura, frente a un 22% que la cataloga en el polo opuesto. Por otra parte, el 13% opina que los servicios tienen un coste excesivo, lo que coincide con las organizaciones que menos facturan en la encuesta (menos de 500 millones de euros al año).

Incidentes de seguridad

El análisis sectorial de los incidentes revela que **Administración, Salud y Seguros son los que reportan mayor número de incidentes en el último año**. Si unimos esto a los datos de que el 75% de las empresas posee un CSIRT y que el 100% dispone de un SOC, nos puede estar indicando un aumento de ataques hacia estos sectores.

Si tenemos en cuenta **las empresas con un promedio más alto de ciberincidentes anuales, el 77% de ellas no posee ningún tipo de certificación**. Este dato nos indica la necesidad de definir una adecuada gestión tanto de la ciberseguridad como de la continuidad de negocio, lo que tendrá como consecuencia la mitigación de los riesgos, la mejora de la formación y concienciación de los empleados y el análisis de las causas de los ciberincidentes para intentar evitar que ocurran en el futuro.

Con respecto a las amenazas, las empresas españolas consideran el impacto, de mayor a menor: *malware, phishing, web application attacks, web based attacks y data breaches*. El malware destaca notablemente de entre el resto de las amenazas, con un 68%, quedando en segundo lugar y, muy por debajo, el phishing con un 18%. Las apreciaciones de los encuestados están en línea con los resultados de los estudios sobre ciberamenazas de reputados organismos internacionales.

Percepción del CISO

Con respecto al análisis sectorial, hay que destacar que, **en el sector Banca, el 80% de las organizaciones considera que está preparada para afrontar un ciberincidente.**

Cuando se compara la preparación de las empresas con su número de empleados dedicados a la ciberseguridad, se observa que aquellas que tienen menos de 25 empleados son las que consideran que su organización no está suficientemente preparada para afrontar un ciberincidente.

Siguiendo con otras preocupaciones los CISOs**, los riesgos que les generan mayor inquietud son, en este orden: interrupción de las operaciones, riesgo reputacional y fuga de información confidencial**.

En el 75% de los casos, la tarea bajo la responsabilidad del CISO es la alineación de la estrategia de ciberseguridad con el negocio. En el caso del sector de Energía y Recursos esta tarea es, de manera unánime, la más importante. No obstante, en el sector Transporte, Hostelería y Servicios este porcentaje se reduce al 57% de los casos.

Otras preocupaciones que tienen son la comprensión de su entorno de amenazas y manejo efectivo del programa de amenazas, implementación de las medidas de seguridad y el desarrollo y gestión del cumplimiento de las políticas de ciberseguridad, teniendo todas ellas porcentajes de relevancia mucho más bajos, menos del 20%.

En contraposición a lo anterior, cuando se pide a los CISOs que identifiquen las labores más importantes en su agenda, salta a la vista las discrepancias con respecto a las preocupaciones anteriores, ya que destaca que la implementación de las medidas de seguridad, su implicación en los proyectos de ciberseguridad más relevantes, las reuniones con otras áreas de negocio y la revisión del presupuesto de ciberseguridad ocupa la mayoría de su tiempo. **Las reuniones con otras áreas de negocio solo supone el 22% de las tareas del CISO, lo que pone de manifiesto que este no dedica mayoritariamente su tiempo a sus verdaderas preocupaciones, que es el alineamiento con el negocio.**

Dado que la implicación de Alta Dirección en ciberseguridad y el reporte directo desde esta área es el medio principal para empoderar al CISO a lo largo de la organización para desarrollar sus tareas, se ha analizado la relevancia con la que se tratan los temas de ciberseguridad en los comités de dirección. **Para un 75% de las empresas, la ciberseguridad es considerada un tema importante y se trata de forma periódica en los comités de la alta dirección**.

Es llamativo el caso del sector de Fabricación, en el que hay un 33% de las organizaciones en las que solo se considera la ciberseguridad cuando hay un incidente grave, pese a ser organizaciones en las que una de sus preocupaciones es la interrupción de sus operaciones.

Percepción del CISO en tiempos de pandemia

Dada la situación mundial actual, se consideró de relevancia volver a contactar con las empresas que participaron en este estudio para poder ahondar en cómo se ha gestionado esta crisis dentro de las responsabilidades del CISO.

El 77% de las organizaciones consideraban el teletrabajo, con anterioridad en sus Planes de Continuidad, como una de las alternativas a la actividad presencial. Esto se traduce en que el 79% de las organizaciones se consideraba, al menos, bastante preparada o más, frente a los riesgos que plantea esta modalidad de trabajo.

Desde el punto de vista de la continuidad de las operaciones en entornos no presenciales, el 43% de las empresas considera que el teletrabajo no le ha facilitado el desarrollo de sus tareas.

Por otra parte, **el 62% de las empresas indica que su infraestructura tecnológica ha sufrido más ataques de lo normal desde el comienzo de la pandemia.**

El dato más preocupante, sin lugar a duda, ha sido que para el 57% de las empresas la pandemia ha supuesto la disminución de sus presupuestos de ciberseguridad. Este dato es entendible por la crisis económica que se ha desencadenado, pero puede desencadenar una crisis de ciberseguridad que ponga en riesgo la viabilidad del propio negocio.

El 62% de las empresas indica que su infraestructura tecnológica ha sufrido más ataques de lo normal desde el comienzo de la pandemia.

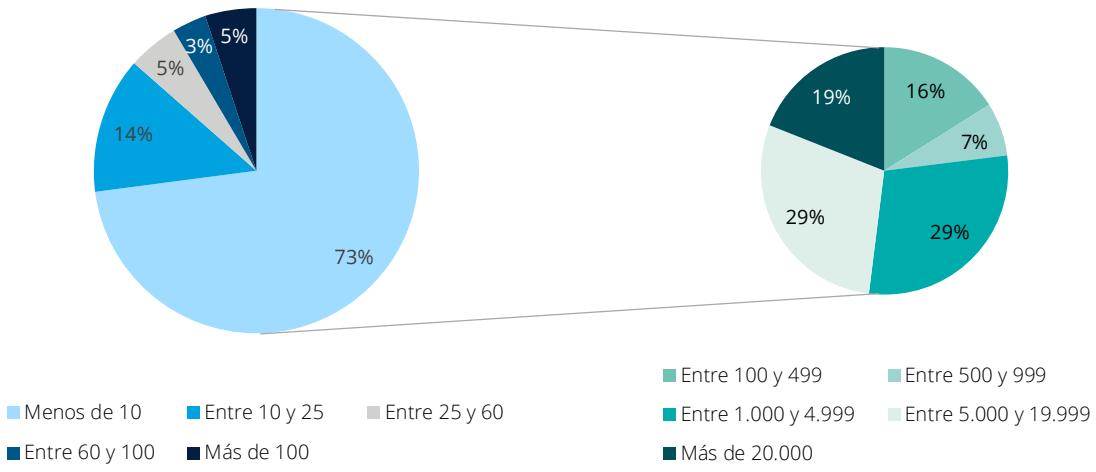
El 57% de las empresas la pandemia ha supuesto la disminución de sus presupuestos de ciberseguridad.

Headcount y SOC

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

La creciente preocupación por la seguridad ha hecho que las empresas busquen contar con personal especializado en ciberseguridad dentro de su estructura, independientemente de si se trata de personal externo o interno. Desde la perspectiva del número de personas dedicadas a la ciberseguridad, se observa que la mayoría de las empresas consultadas (el 73%) cuenta con menos de 10 de estos perfiles y que tan solo un 5% de las empresas cuenta con una estructura de ciberseguridad compuesta por más de 100 personas.

Empleados dedicados en exclusiva a la ciberseguridad



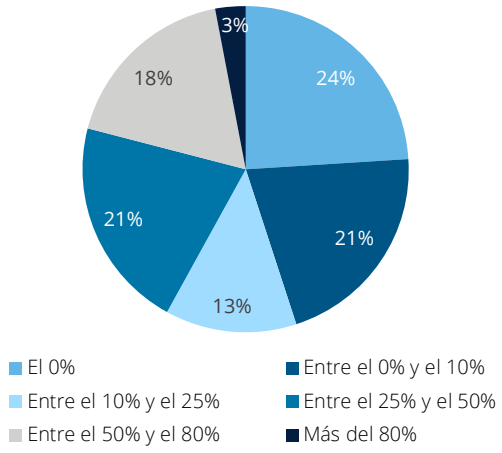
Empleados totales destinados a ciberseguridad

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

¿Qué porcentaje del personal de ciberseguridad es externo?

La externalización del personal de ciberseguridad por la que se decantan la mayoría de las empresas que buscan cierta flexibilidad ante los cambios de un mercado impredecible, continúa siendo tendencia ya que **el 76% de las empresas encuestadas cuentan con personal externo en sus equipos de ciberseguridad**, donde además, para el 21% de empresas que optan por la externalización, dicha plantilla está compuesta en más del 50% por empleados externos.

Porcentaje de empleados externos en la empresa

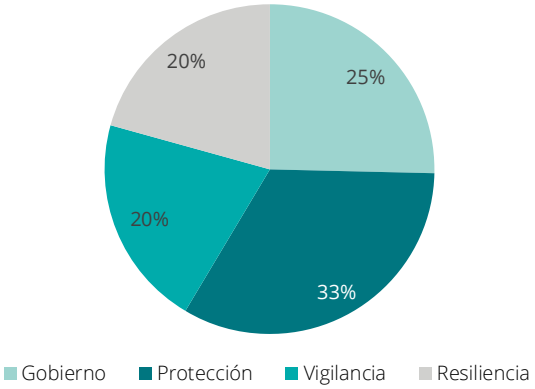


¿Cuál es el número de empleados según las siguientes líneas de ciberseguridad: Gobierno, Protección, Vigilancia, Resiliencia?

Se puede observar cierto equilibrio en la distribución del personal en las diferentes líneas de ciberseguridad, no obstante, la protección sigue siendo la línea predominante, con un 33% de personal de ciberseguridad destinados a la protección de los sistemas de la empresa.

Cabe destacar también, que dada la necesidad de alineamiento entre la ciberseguridad y el negocio en un mercado en constante cambio, la línea de Gobierno va cobrando mayor protagonismo.

Número de empleados según las líneas de ciberseguridad

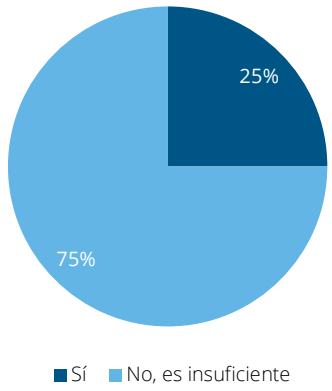


La externalización del personal de ciberseguridad por la que se decantan la mayoría de las empresas que buscan cierta flexibilidad ante los cambios de un mercado impredecible, continúa siendo tendencia ya que **el 76% de las empresas encuestadas cuentan con personal externo en sus equipos de ciberseguridad**.

¿Considera que cuenta con el número de empleados necesarios?

Aunque se observan grandes esfuerzos en materia de ciberseguridad por parte de la industria, **la mayoría de las empresas tiene la percepción de que el número de recursos dedicados a Ciberseguridad es aún insuficiente**, como se muestra en la siguiente gráfica, donde solo un 25% cree disponer del personal necesario, tanto externo como interno, para realizar las tareas destinadas a la defensa y seguridad de la organización.

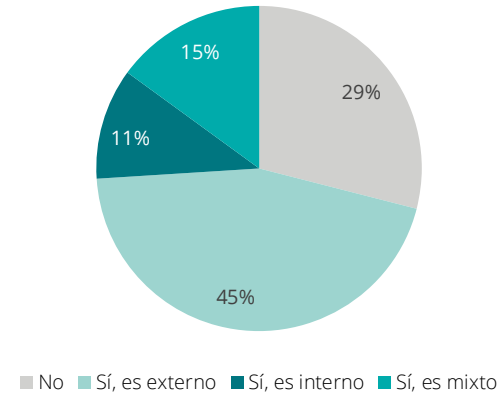
Número de empleados necesarios



¿Se dispone de un SOC/CSIRT propio?

Las empresas son cada vez más conscientes de la necesidad de ser capaces de detectar y gestionar de forma rápida y eficaz los incidentes de seguridad, minimizando así los impactos que estos puedan tener sobre el negocio. Esto se ve reflejado en que **el 71% de las empresas participantes cuentan con los servicios especializados de un Centro de Operaciones de Seguridad (SOC)**.

¿Se dispone de un SOC/CSIRT propio?



El 71% de las empresas participantes cuentan con los servicios especializados de un Centro de Operaciones de Seguridad (SOC).

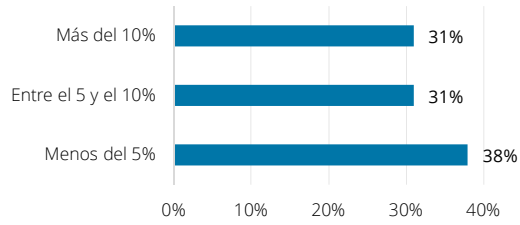
No obstante, debido a la complejidad y el coste de disponer de un SOC propio, la externalización de dichos servicios en empresas especializadas es la modalidad con mayor adopción por parte de las empresas participantes (45%), seguida, aunque de lejos, por la modalidad mixta (15%), donde confluyen recursos internos y externalizados.

Presupuesto y servicios

¿Qué porcentaje representa el presupuesto [9]de ciberseguridad respecto al de IT/OT? Excluyendo empleados internos

Se observa que **las empresas dedican de su presupuesto de IT/OT una media de 9,33% de estos a la ciberseguridad**. En este sentido, se puede apreciar, **con respecto al año pasado, un notable incremento del 0,8%** en la inversión dedicada a esta materia.

Porcentaje del presupuesto de ciberseguridad respecto de IT/OT

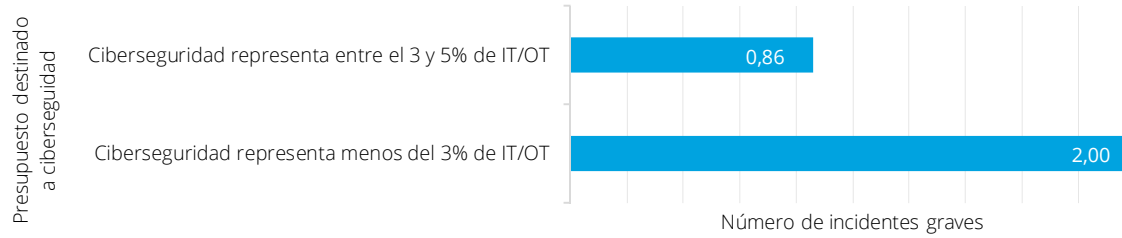


Las empresas dedican de su presupuesto de IT/OT una media de 9,33% de estos a la ciberseguridad.

Se observa también que existe cierta relación entre los presupuestos dedicados a la ciberseguridad y el número de ciber incidentes sufridos, ya que **el 80% de las empresas que dedican a la ciberseguridad menos del 3% de su presupuesto de IT/OT, sufrió de media 2 incidentes graves al año, mientras que para aquellas que dedican entre el 3% y 5% de sus presupuestos, la media se reduce a 0,86 incidentes significativos por año**.

El 80% de las empresas que dedican a la ciberseguridad menos del 3% de su presupuesto de IT/OT, sufrió de media 2 incidentes graves al año, mientras que para aquellas que dedican entre el 3% y 5% de sus presupuestos, la media se reduce a 0,86 incidentes significativos por año.

Incidentes de seguridad graves vs presupuesto invertido



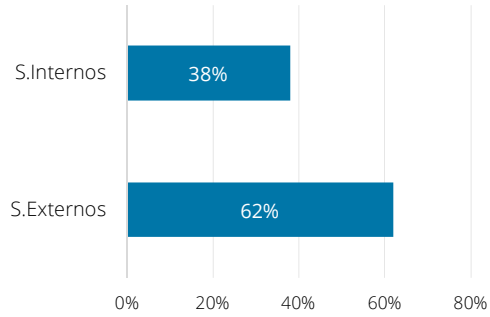
La diferencia entre ambos rangos es notable y recalca la importancia de una inversión adecuada en ciberseguridad, donde un mayor presupuesto permite a las empresas levantar y mantener las líneas de defensa necesarias para reducir la probabilidad de ocurrencia de incidentes de ciberseguridad.

[9] Excluyendo empleados internos e incluyendo el licenciamiento de herramientas exclusivas de ciberseguridad.

¿Qué porcentaje del presupuesto anual de ciberseguridad se dedica a los servicios externalizados y cuál a los servicios internos?

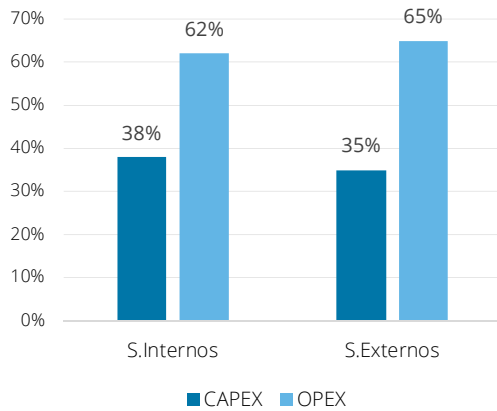
La necesidad de contar con servicios especializados en materia de ciberseguridad, en un escenario cada vez más complejo, hace que la externalización de estos servicios siga siendo el elemento al que las empresas dedican el mayor porcentaje de sus presupuestos de ciberseguridad (62%), en contraposición al dedicado a servicios internos (38%).

Porcentaje del presupuesto dedicado a los servicios internos y externos



Haciendo un desglose de los presupuestos en términos de CAPEX y OPEX, se observa que existe cierta similitud en la distribución económica en los servicios internos y externos. Asimismo, se observa también **que más de la mitad del presupuesto se dedica al OPEX** en ambos casos.

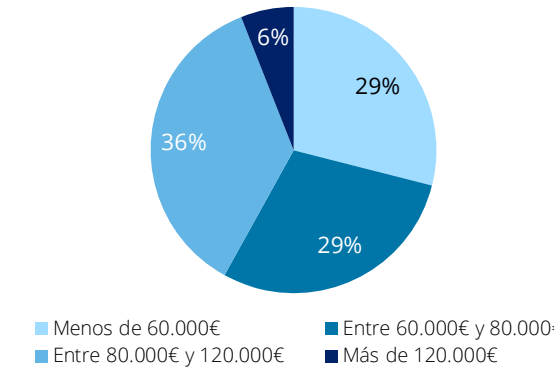
Porcentaje de presupuesto dedicado al CAPEX y al OPEX



¿Cuál es salario bruto anual medio del CISO?

Un 29% de los CISOs perciben un salario bruto inferior a 60.000€, mientras que otro 36% percibe un salario bruto anual de entre 80.000€ y 120.000€. Solo un reducido porcentaje de los CISOs (6%) afirman percibir un salario superior a 120.000€.

Salario del CISO



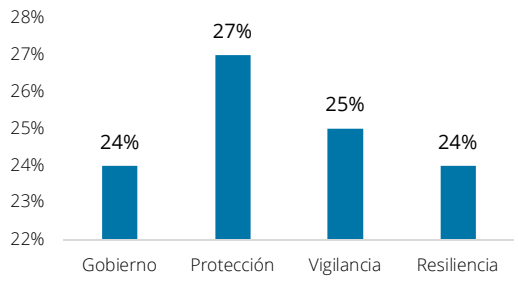
Se ha comprobado cómo los salarios más altos de los CISOs se corresponden con las empresas con un mayor EBITDA.

A pesar de que estos datos están obtenidos sobre una muestra muy diversa de empresas, es cierto que siguen siendo salarios bastante por debajo del resto de países de la Unión Europea. Además, de manera general, son salarios que se encuentran por debajo de la media de responsables que ostentan cargos de responsabilidad similar en la misma empresa.

¿Cuál es el presupuesto en euros disponible según las siguientes líneas de ciberseguridad? Excluyendo empleados internos e incluyendo licenciamiento: Gobierno, Protección, Vigilancia y Resiliencia

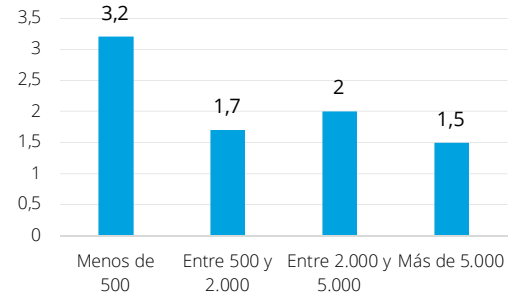
En línea con los resultados obtenidos en cuanto a la distribución del personal de ciberseguridad en las cuatro principales líneas de ciberseguridad, se observa que también existe una distribución relativamente equitativa del presupuesto de ciberseguridad. Asimismo, y al igual que ocurre con el personal, "Protección" es la línea que mayor inversión de recursos recibe con un 27% del total del presupuesto.

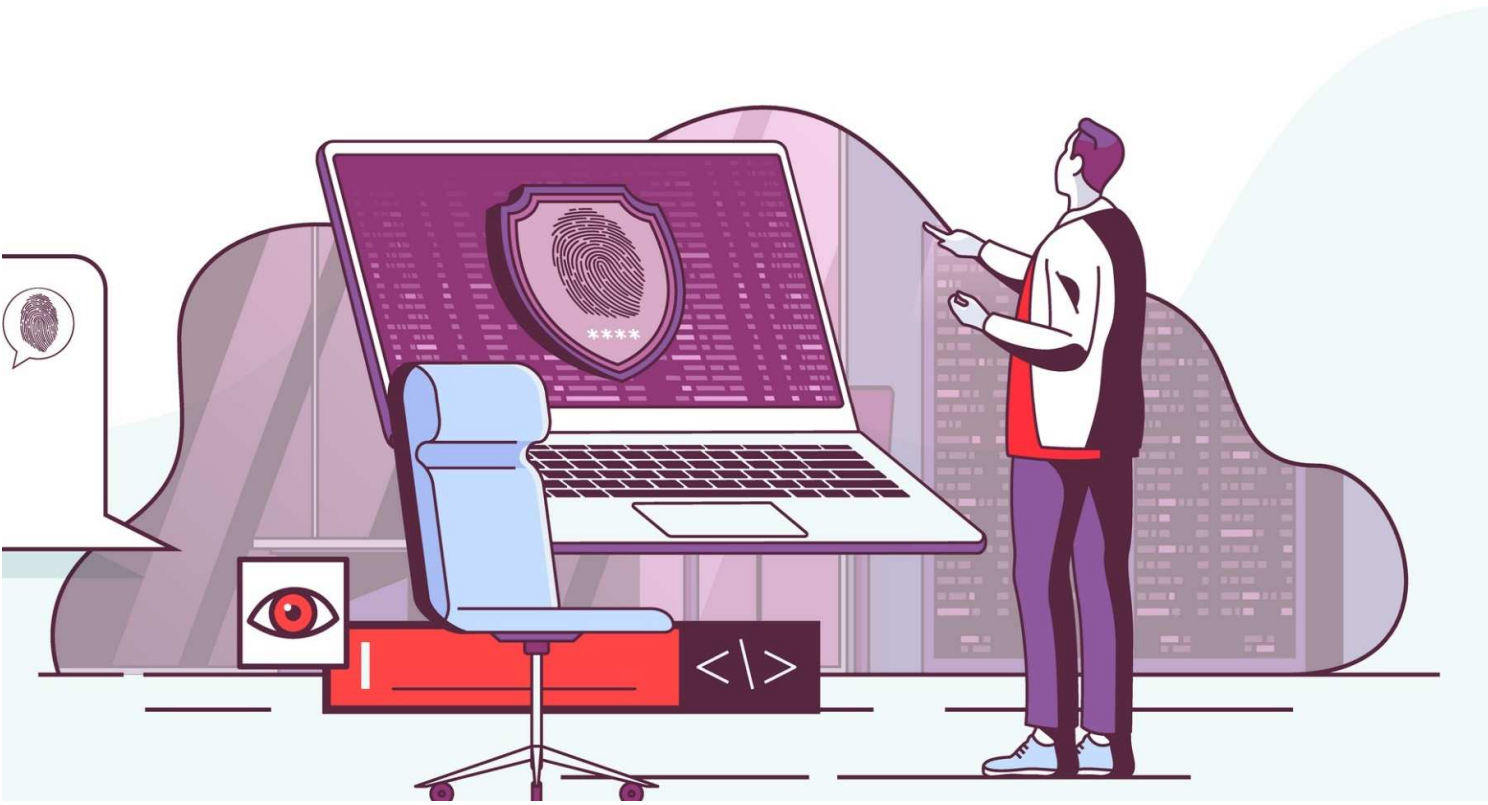
Porcentaje de presupuesto por líneas de ciberseguridad



Se ha realizado un análisis combinado del número de incidentes que ha recibido cada empresa durante el 2019 y su presupuesto en ciberseguridad, destacándose que las empresas que facturan menos de 500 millones de euros son las que experimentan un mayor número de incidentes al año, 3.2 incidentes. Sin embargo, los del rango superior de facturación sufren menos ciber incidentes 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.

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





Target Operating Model

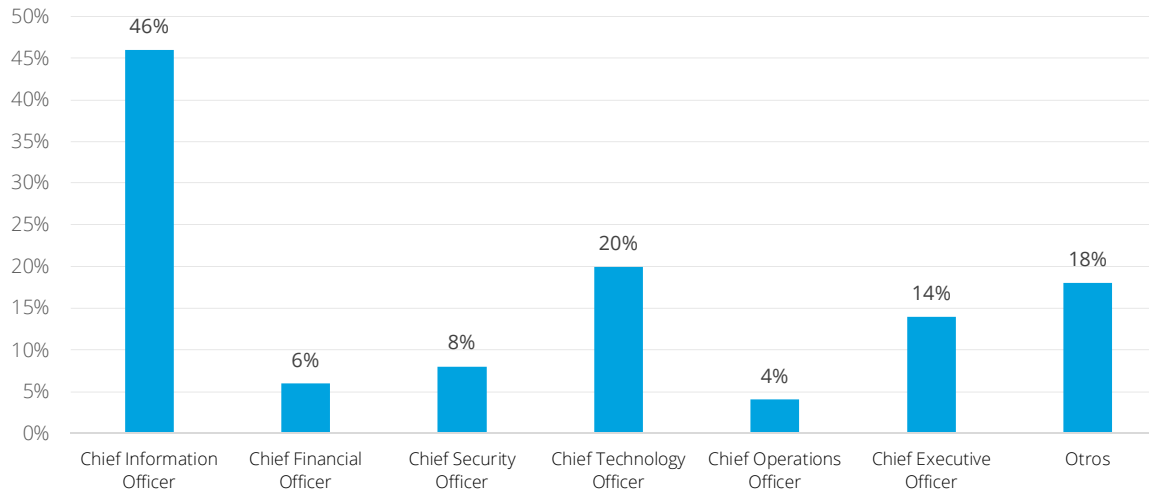
Jerárquicamente ¿de quién depende el CISO?

La ubicación organizativa del CISO es un tema que sigue estando presente en múltiples estudios de ciberseguridad realizados, donde se puede ver que las tendencias y predicciones van variando con el tiempo, al igual que lo hace las necesidades del mercado con empresas cada vez más complejas, nuevas leyes y regulaciones, digitalización de los entornos, demanda de perfiles especializados, etc.

Un creciente 14% se desliga completamente del área de Tecnología con una dependencia directa del CEO.

En relación con el modelo de gobierno de ciberseguridad que predomina actualmente en el conjunto de las empresas encuestadas, se observa que **el 46% de los CISOs depende jerárquicamente del CIO, acorde a la tendencia mantenida tradicionalmente. Sin embargo, se observa que la dependencia empieza a experimentar cambios hacia modelos nuevos, donde el 20% de los CISOs muestra dependencia del CTO, un creciente 14% se desliga completamente del área de Tecnología con una dependencia directa del CEO** y otro significativo 18% se encuadra en otro tipo de estructuras jerárquicas diferentes a las más comunes.

¿De quién depende el CISO?

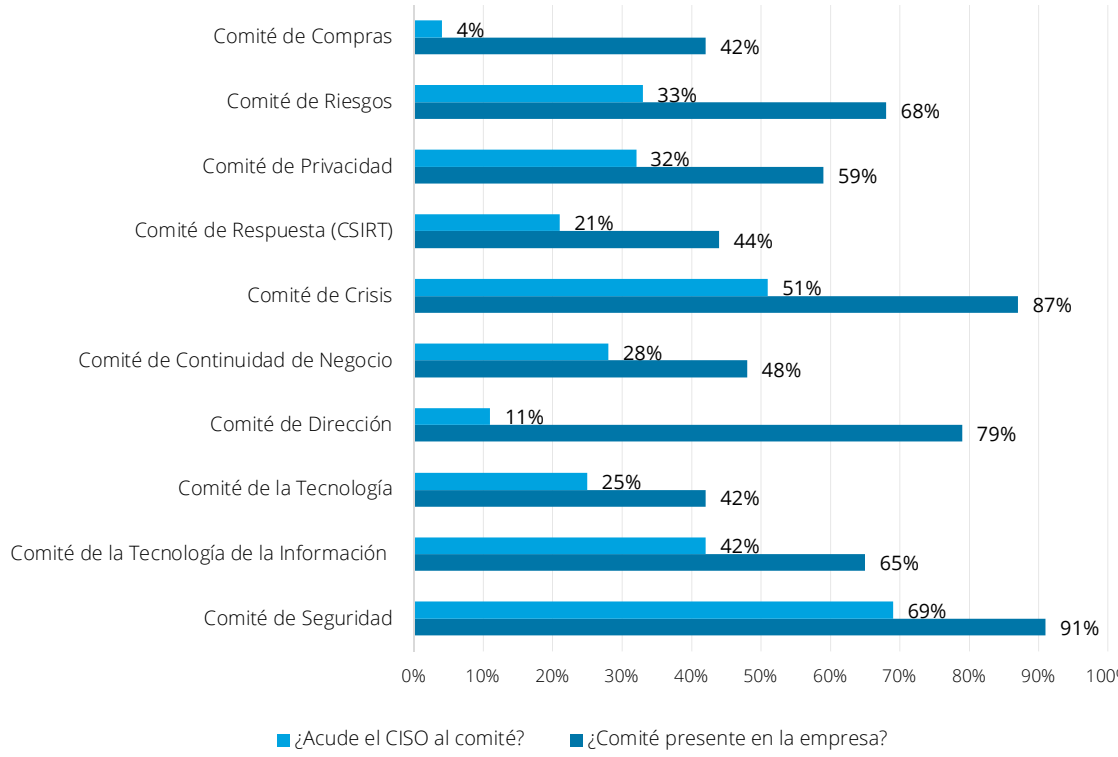


El dato realmente destacable en este aspecto es que respecto al año pasado ha disminuido un 12,54% la dependencia del CIO y ha aumentado la dependencia del CEO en un 4,24%. Esto muestra cómo la dirección de las empresas está cada vez más concienciada en materia de ciberseguridad.

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

Un dato llamativo es que, apenas, el 69% de los CISOs acude al Comité de Seguridad. En este sentido, su participación en el resto de los comités es todavía mucho menor.

Comités relacionados con la ciberseguridad

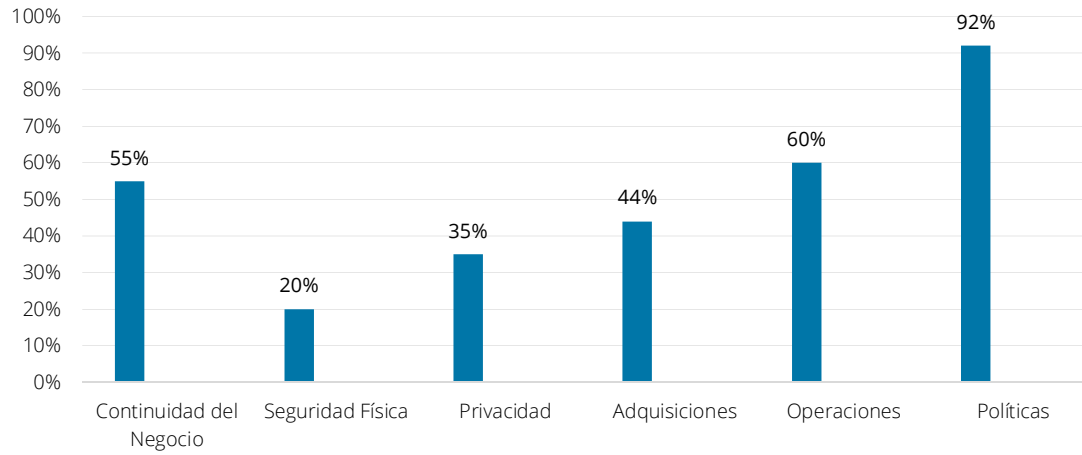


Adicionalmente, de la anterior gráfica se rescatan otros datos interesantes:

- Existe una tendencia clara hacia empresas cada vez más preocupadas por la ciberseguridad que se fortalece con los resultados obtenidos, donde **casi la totalidad de las empresas (91%) cuenta con un Comité de Seguridad**.
- La resiliencia sigue siendo una asignatura mejorable para las empresas, ya que **solo el 44% de las empresas ha formalizado un Comité de Respuesta a Incidentes específico**, lo que pone de manifiesto que, ante tales escenarios, más de la mitad de las empresas gestionan en otros comités las acciones que deberán llevarse a cabo para contener un incidente. No obstante, **un 87% cuenta con un Comité de Crisis, por lo que ante un incidente de ciberseguridad significativo que pudiera derivar en una crisis se contaría con una estructura formalizada para la toma de decisiones requeridas ante tal escenario.**
- Del total de empresas que cuenta con un Comité de Seguridad, el 46% de las mismas cuenta también con un Comité de Respuesta a Incidentes o con un Comité de Crisis, lo que demuestra la creciente preocupación de las empresas por tener estructuras formalizadas que den soporte al gobierno de la seguridad y también a la resiliencia de la empresa ante un incidente o crisis.

¿Qué ámbitos de responsabilidad dependen del CISO?

Responsabilidades del CISO



Adicionalmente a los datos del gráfico anterior, se detecta una tendencia en la **que el CISO es responsable de la primera línea de defensa en un 60% de los casos, al ser responsables de las operaciones de seguridad de la empresa, además de ser la figura clave en la segunda línea. Este dato concuerda con los modelos que sitúan al CISO en la línea 1,5, es decir, entre la primera y segunda línea de defensa**.

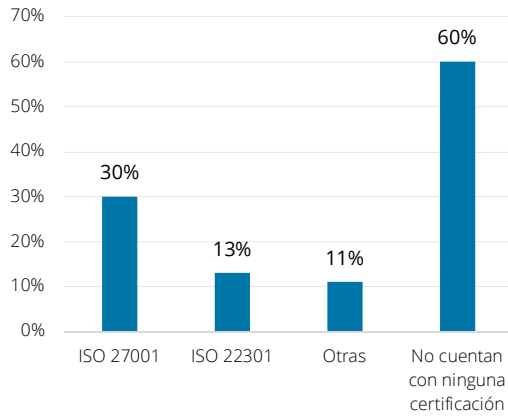
En contraste, las actividades enfocadas en la seguridad física y la privacidad de la información (GDPR) siguen estando fuera del ámbito de responsabilidades de muchos CISOs, ya que estas son normalmente delegadas en el responsable de seguridad física y el responsable de protección de datos (DPO) de la empresa.

Certificaciones, framework y formación

¿Qué certificaciones relacionadas con la ciberseguridad posee la empresa?

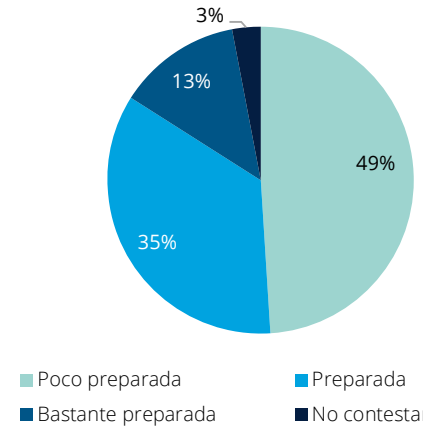
La certificación ISO 27001, cuyo estándar promueve la implementación de un Sistema de Gestión de Seguridad de la Información, sigue siendo el estándar favorito de las organizaciones para su gestión de ciberseguridad. Un 30% de las empresas se ha certificado bajo dicho estándar.

¿Qué certificaciones posee la empresa?



Por otro lado, la certificación ISO 22301, relacionada con la continuidad del negocio, es la segunda más demanda por las empresa. Además, **aproximadamente el 67% de empresas que posee la ISO 22301 están certificadas también en la ISO 27001**. 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, se traduce en una mayor facilidad en la obtención de futuras certificaciones.

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



Dentro del grupo de empresas que no poseen ninguna certificación de ciberseguridad, las percepciones acerca de su nivel de preparación ante incidentes de ciberseguridad se encuentran divididas casi a partes iguales, con un 49% de los CISOs que considera que su empresa está poco preparada y un 48% que cree que sí están preparados, en mayor o menor medida.

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

En el ámbito de las habilidades individuales en materia de seguridad, se observa que existe un gran interés por adquirir y/o complementar dichas habilidades a través de formación especializada obteniendo, a su vez, un reconocimiento oficial de las mismas a través de certificaciones reconocidas. Los datos que apoyan esta conclusión son que **el 70% de los CISOs encuestados posee, al menos, una certificación en materia de Seguridad de la Información**.

Estos mismos datos, permiten ver que **las certificaciones de seguridad enfocadas a la gestión (CISM) y a la auditoría (CISA), siguen siendo las más predominante entre los CISOs, estando presentes en un 40% y 32%, respectivamente, del total de certificaciones que estos poseen**.

Este hecho podría deberse a dos causas:

1. Son las certificaciones más demandadas por los CISOs
2. Fueron las primeras certificaciones relacionadas, de algún modo, con este ámbito de competencia y, por tanto, hay un número mayor histórico de certificados.

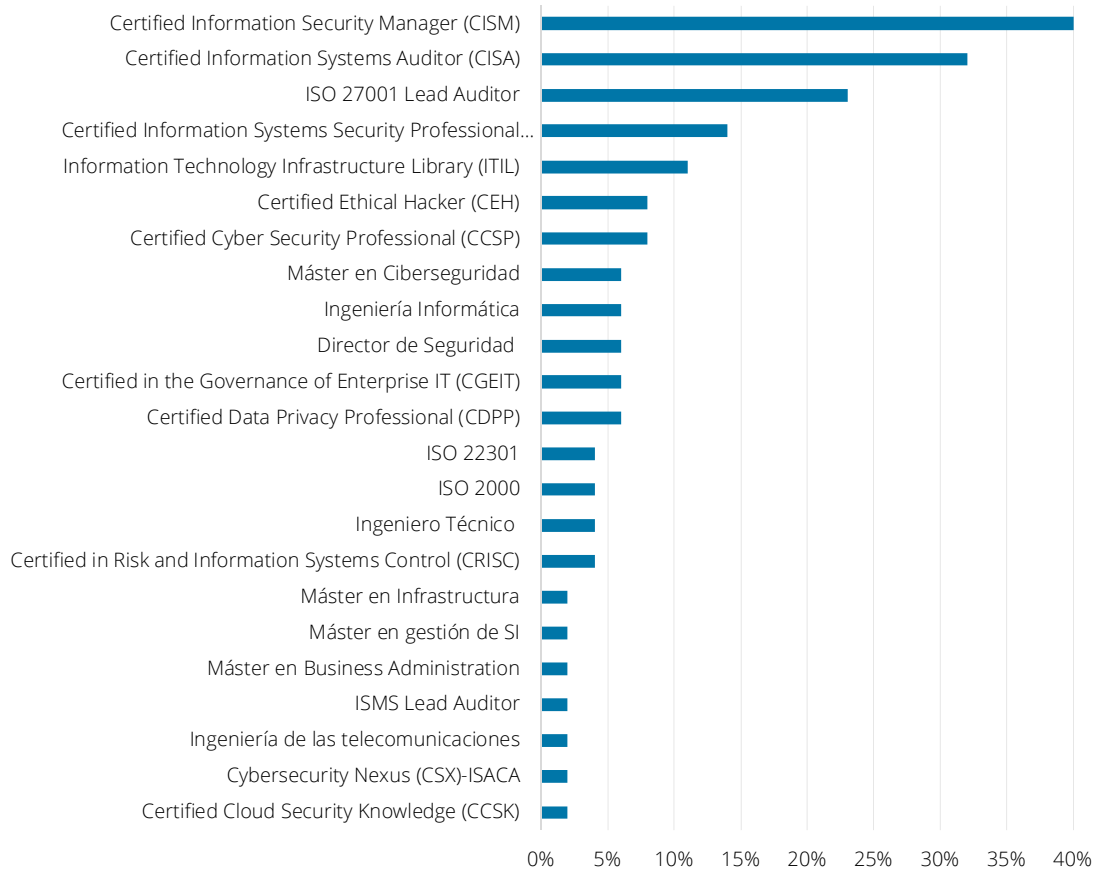
No obstante, si recogemos los datos del año pasado se observa que **la demanda del CISM ha aumentado en un 2,5 % y la del CISA en un 4,5% respecto a los datos del año pasado**.

Otras certificaciones con un enfoque más "técnico", como por ejemplo CISSP, CCSP o CEH, empiezan a tener cada vez más presencia en el plan de formación de los CISOs.

Este dato está alineado con el hecho de que los CISOs son responsables también de las operaciones de seguridad, requiriendo en mayor o menor medida de este tipo de conocimientos.

La demanda del CISM ha aumentado en un 2,5 % y la del CISA en un 4,5% respecto a los datos del año pasado.

Certificaciones que posee el CISO de la empresa



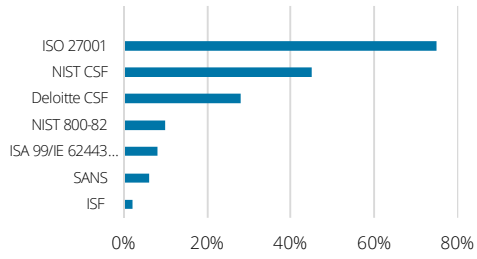
¿Qué frameworks se usan como referencia para la mejora de los procesos de ciberseguridad en las empresas?

A pesar de que no todas las empresas cuentan con la certificación ISO 27001, **casi un 75% del total de empresas utiliza dicho estándar como marco de referencia para la mejora de sus procesos de ciberseguridad. Con menor adopción (45%), el NIST CSF es el segundo marco más referenciado por parte de las empresas participantes. Finalmente, y con un 28%, se sitúa el CSF (Cyber Strategy Framework) de Deloitte.**

Este último, se trata de un marco propio de Deloitte que engloba los controles de seguridad de varios estándares reconocidos (ISO, SANS, NIST, etc.).

Finalmente, cabe destacar que **el uso del Deloitte CSF como marco de referencia ha aumentado en un 10,5% respecto al año pasado.** Un dato favorecedor para este Framework teniendo en cuenta además que el número de empresas participantes en este estudio ha aumentado también respecto al año anterior.

Frameworks Seguridad de la Información



Si se pone foco en sectores donde se cuenta, además de con el tradicional entorno IT, con entornos industriales (Energías y Recursos, Fabricación, Automoción, Consumo y Distribución, etc.), se observa que estándares reconocidos y específicos para dichos entornos, como ISA 62443 o NIST 800-82, no aparecen entre los marcos más utilizados, habiendo sido citados únicamente por el 5% de las empresas pertenecientes a dichos sectores.

Este dato refleja el bajo nivel de madurez en ciberseguridad de la tecnología industrial usada por estas industrias.

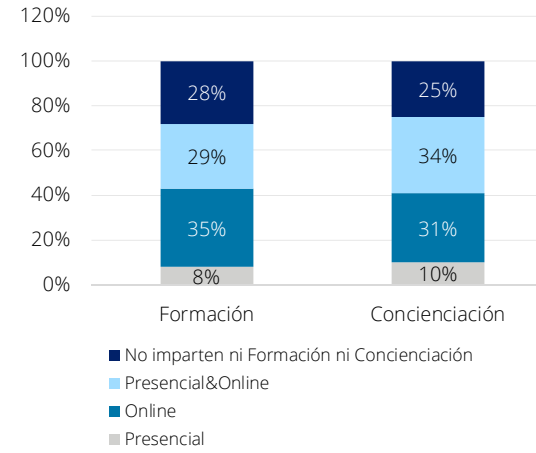
El uso del Deloitte CSF como marco de referencia ha aumentado en un 10,5% respecto al año pasado.

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

Si se cuantifica la inversión en tiempo dedicado a formación en materia de ciberseguridad de los empleados, se observa similitud en el número de horas dedicadas a dichas actividades, siendo la media de, **aproximadamente, 25 horas anuales por empleado en formación y, aproximadamente, 130 horas de concienciación en materias de ciberseguridad**.

En cuanto a la modalidad elegida por las empresas, se aprecia que tanto para la concienciación como para la formación de los empleados, gran parte de ellas se decantan por la facilidad y flexibilidad horaria que proveen la modalidad online, siendo en algunos casos, la única forma de impartición o dentro de una modalidad mixta, donde parte de estas actividades son impartidas también de forma presencial.

Formación y concienciación en materias de seguridad



Por otro lado, es bastante reseñable que **aproximadamente el 25% de las empresas (especialmente las más pequeñas) no realiza actividades de concienciación ni formación de ciberseguridad entre sus empleados**. Siendo los usuarios el eslabón más frágil de la cadena, queda manifiesto que este es un ámbito en el que las empresas deben seguir trabajando.

En cuanto a la modalidad elegida por las empresas, se aprecia que tanto para la concienciación como para la formación de los empleados, gran parte de ellas se decantan por la facilidad y flexibilidad horaria que proveen la modalidad online.

Revisiones de seguridad, entornos *cloud* y tendencias tecnológicas

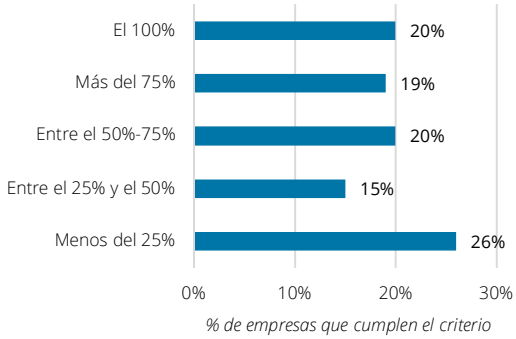
¿Qué porcentaje de las aplicaciones consideradas imprescindibles/críticas son revisadas?

Conocer cuáles son las aplicaciones críticas que soportan los servicios y procesos críticos del negocio es tan importante como el asegurar que estas se encuentran protegidas frente a posibles ataques de ciberseguridad por el impacto que esto supondría para el negocio.

En este sentido, se observa que **un 59% de las empresas consultadas revisa al menos la mitad del total de sus aplicaciones críticas, llegando incluso a ser revisadas en su totalidad por un 20% de las empresas. Por otro lado, un significativo 26% de las empresas no revisa ni la cuarta parte del total de sus aplicaciones críticas, es decir, tres de cada cuatro aplicaciones se quedarían sin revisar** y, por tanto, sin garantizar que cuentan con el nivel de seguridad requerido para un servicio crítico.

Porcentaje de las aplicaciones consideradas imprescindibles/críticas que son revisadas desde ciberseguridad

% de las aplicaciones consideradas imprescindibles o críticas que son revisadas:



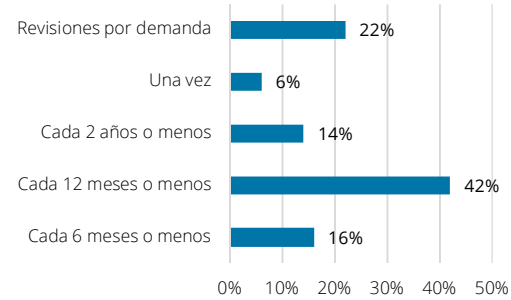
El sector de la Banca es el que revisa en mayor profundidad sus aplicaciones críticas, revisando casi la totalidad de ellas. En el extremo opuesto se encuentran los sectores de Consumo y Distribución e Industria Agroalimentaria, ya que revisan menos del 25% del total de las aplicaciones que consideran imprescindibles o críticas.

En un punto intermedio se encuentran Energía y Recursos, junto con Transporte, Hostelería y Servicios, donde la mitad de las empresas pertenecientes a dichos sectores revisan entre el 50% y el 75% de las aplicaciones consideradas imprescindibles o críticas para su negocio.

¿Con que periodicidad se revisan las aplicaciones consideradas imprescindibles/críticas?

Las buenas prácticas del mercado recomiendan una revisión anual y tras cambios significativos de las aplicaciones consideradas críticas o imprescindibles para el negocio y, acorde a los datos obtenidos, estas parecen ser las pautas que siguen la mayoría de las empresas consultadas:

Periodicidad con la que se revisan las aplicaciones criticas

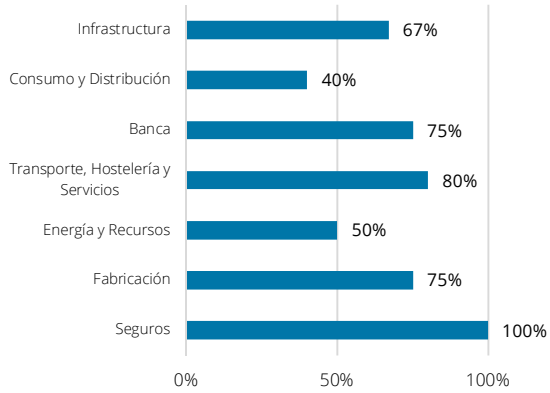


Conocer cuáles son las aplicaciones críticas que soportan los servicios y procesos críticos del negocio es tan importante como el asegurar que estas se encuentran protegidas.

Las buenas prácticas del mercado recomiendan una revisión anual y tras cambios significativos de las aplicaciones consideradas críticas o imprescindibles para el negocio.

Teniendo en cuenta que se trata de aplicaciones críticas para el negocio, destaca que haya un 22% de las aplicaciones que solo se revisan bajo demanda y un 6% que solo se revisan tras su despliegue inicial.

Sectores que revisan como mínimo sus aplicaciones críticas de forma anual



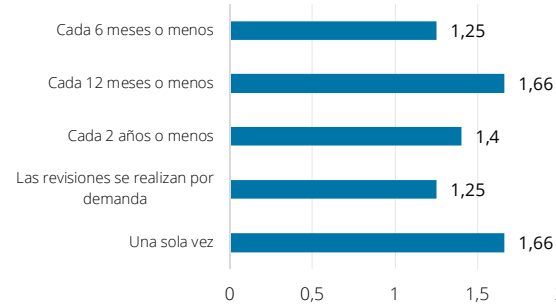
No sorprende el dato del bajo número de revisiones del sector de Energía y Recursos y el de Consumo y Distribución, en los que la tecnología OT suele contar con componentes *legacy* y, en muchos de los casos, todo el soporte recae bajo el proveedor de dicha tecnología. No obstante, cada vez más se busca la forma de gestionar mejor la ciberseguridad de estas aplicaciones y sistemas debido a la convergencia de la tecnología IT y OT, lo que supone un aumento de las probabilidades de sufrir un ciber ataque.

Si se analizan las revisiones bajo demanda, se observa que son los sectores de Consumo y Distribución, Banca y Fabricación, los que mayor índice de revisiones por demanda poseen, abarcando más del 50% del total de empresas que optan por esta modalidad en sus revisiones.

La tecnología OT suele contar con componentes *legacy* y, en muchos de los casos, todo el soporte recae bajo el proveedor de dicha tecnología.

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

Periodicidad con las que se revisan las aplicaciones:



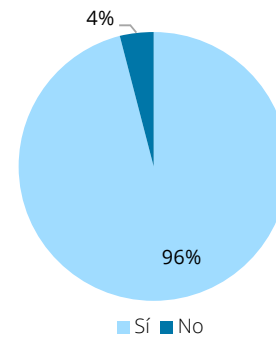
Promedio de Incidentes por año

¿Tienen una estrategia definida en materia de Cloud Computing?

Es evidente que la adopción del Cloud por parte de las empresas es un hecho consolidado, ya que **solo el 4% de las empresas encuestadas no dispone de ningún servicio o aplicación Cloud**.

Este dato puede deberse a varios factores, pero no se descarta que uno de ellos siga siendo la desconfianza depositada en estos terceros, la cual predominaba hace 10-5 años y que poco a poco ha ido disminuyendo.

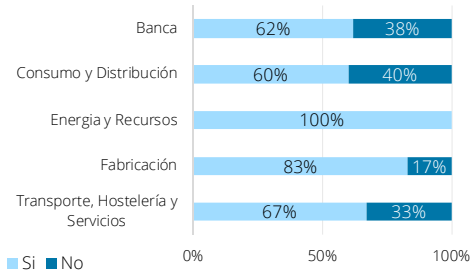
Empresas con aplicaciones cloud



Precisamente, debido a la desconfianza en materia de ciberseguridad que puede suscitar la adopción del Cloud, la mayoría de las empresas que hacen uso de esta tecnología han optado por introducirla en sus respectivos entornos tecnológicos bajo una estrategia definida de ciberseguridad.

En un análisis por sectores, destacan Fabricación, así como Energía y Recursos, como los sectores con mayor preocupación por tener una estrategia clara en cuanto a la utilización de los servicios y aplicaciones Cloud bajo la perspectiva de ciberseguridad.

¿Disponen de una estrategia de ciberseguridad en cloud?



En un punto intermedio se hallan Transporte, Hostelería y Servicios, con un 60% de empresas del sector que disponen de una estrategia Cloud, seguido de Banca con un 62% y Consumo y Distribución, con un 60%.

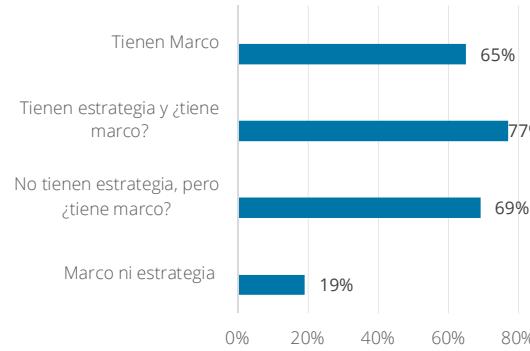
¿Se dispone de un marco de controles específicos para Cloud Computing?

Con el aumento del uso de servicios en Cloud se ha hecho más necesario contar con marcos de referencia de seguridad específicos que aseguren el cumplimiento normativo, la protección del dato, la detección de incidentes y buenas prácticas en materia de seguridad de la información. En cómputo general, **de las empresas que hacen uso de aplicaciones o servicios Cloud, solo el 65% de estas disponen de un marco de control específico para Cloud**.

Si además tenemos en cuenta la existencia de una estrategia Cloud, **solo el 77% de las empresas con una estrategia Cloud dispone también de un marco de controles específico. Sin embargo, desde el lado opuesto, del total de empresas que no cuentan con una estrategia Cloud, el 69% de estas sí cuenta con un marco de controles específicos para Cloud**, lo que demuestra que ya sea a través de una estrategia o un marco de controles, las empresas con aplicaciones o servicios Cloud tienen un claro interés por la seguridad en este tipo de tecnologías. Se puede concluir que **el 81% de las empresas que emplean Cloud disponen de una estrategia o de un marco**.

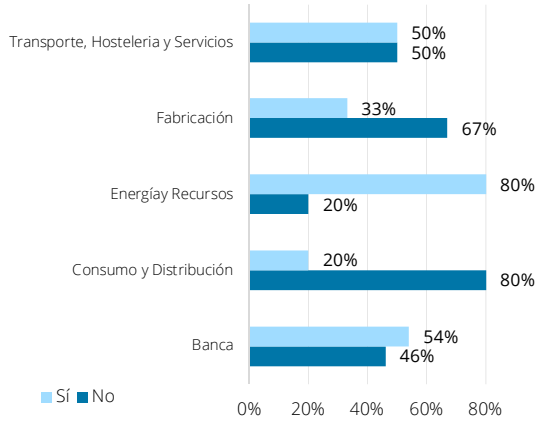
Con el aumento del uso de servicios en Cloud se ha hecho más necesario contar con marcos de referencia de seguridad específicos.

¿Disponen de un marco de controles específicos para Cloud computing?



A partir de un análisis sectorial, se observa que Energía y Recursos, así como Transporte, Hostelería y Servicios, son los sectores donde la mayoría de las empresas que pertenecen a los mismos cuentan con un marco de controles específico para Cloud, con un 80% y 50% respectivamente. No obstante, si se trata de contar con una estrategia y un marco Cloud, es el sector de Energía y Recursos el que destaca, ya que el 80% de las empresas dentro de este grupo tienen tanto una estrategia como un marco. Le sigue, a cierta distancia, el sector de la Banca, con un 54% de empresas que cuentan con ambos elementos.

¿Cuéntan con una estrategia y un marco para cloud al mismo tiempo?

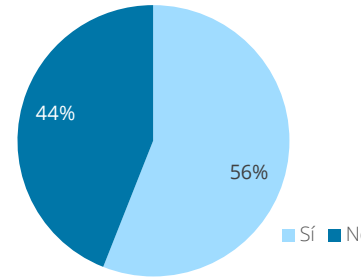


¿Su estrategia de ciberseguridad contempla medidas específicas de IoT, además de sus particularidades, amenazas y vulnerabilidades?

Los dispositivos IoT cobran cada vez más protagonismo en las empresas y, aunque su adopción varía según el sector, a través de los resultados obtenidos se observa cómo **sorprendentemente esta tecnología va ganando terreno, ya que un 87% del total de las empresas participantes cuenta con dispositivos IoT de algún tipo**.

Adicionalmente, las empresas que deciden adoptar esta tecnología también parecen ser cada vez más conscientes de la importancia de la seguridad en este tipo de escenarios y es que **el 56% de las empresas que hacen uso de dispositivos IoT ha decidido incluirlos dentro de su estrategia de Ciberseguridad.** No obstante, a pesar de presentar una tendencia al alza, este dato puede seguir siendo insuficiente si se atiende al hecho de la gran presencia de vulnerabilidades en estos entornos.

% de empresas que en su estrategia de ciberseguridad contempla los dispositivos IoT y sus particularidades, amenazas y vulnerabilidades

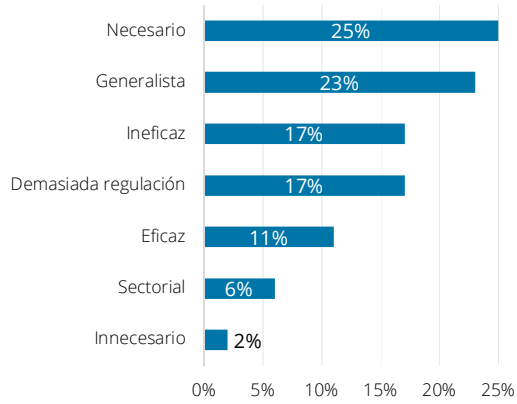


Los dispositivos IoT cobran cada vez más protagonismo en las empresas y, aunque su adopción varía según el sector.

Entorno regulatorio

¿Cómo ve el conjunto de regulación en el sector en el que trabaja?

Con un entorno regulatorio creciente y en evolución para dar cobertura a nuevas tecnologías emergentes, **un 25% de las empresas consultadas opina que la regulación actual es necesaria mientras que otro 23% estima que es generalista.** Esta última opinión es compartida sobre todo por los sectores de la Educación, Consumo y Distribución, Transporte, Hostelería y Servicios.



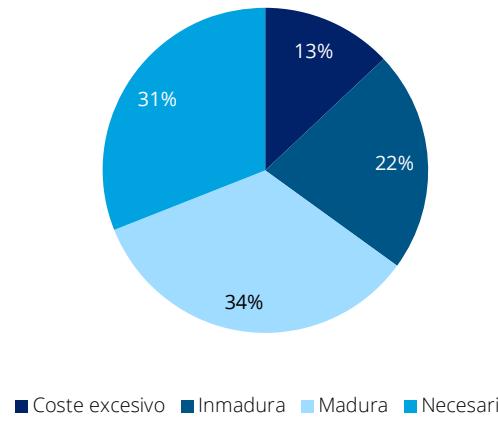
Llama la atención que en cuanto a la percepción de la eficacia del entorno regulatorio actual, **solo el 11% de las empresas considera que este es eficaz**, mientras que un porcentaje superior de empresas (17%) considera que es ineficaz o, en el peor de los casos, que es innecesaria, aunque es cierto que esta opinión es compartida solo por un 2% de empresas.

A nivel sectorial, la percepción del entorno regulatorio no es homogénea, ya que va desde innecesaria hasta excesiva, como ocurre con el sector Banca donde, además, junto con Fabricación, es de los sectores donde menos consenso interno existe.

Por último, **la Industria Agroalimentaria, al igual que Banca, son los únicos que consideran que son sometidos a regulaciones realmente sectoriales**.

¿Qué oferta de servicios Cyber cree que hay en el mercado?

Con una clara tendencia a la externalización de servicios de ciberseguridad y la existencia de elevados presupuestos para tal fin, es destacable que **solo el 34% de las empresas encuestadas considera como madura la oferta de servicios de ciberseguridad actual**, mientras que un significativo 22% considera que esta es aún inmadura.



Adicionalmente, y desde un punto de vista económico, la percepción del 13% de las empresas consultadas es que los servicios de ciberseguridad ofrecidos son excesivamente caros. No es sorprendente que las empresas que consideran los servicios de ciberseguridad caros son las empresas que menos facturan de las encuestadas (menos de 500 millones al año).

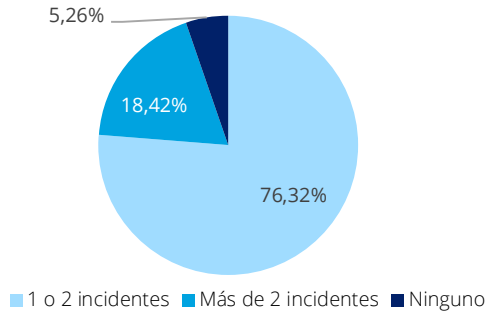
Las empresas que consideran los servicios de ciberseguridad caros son las empresas que menos facturan de las encuestadas (menos de 500 millones al año).

Incidentes de seguridad

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

En un escenario de amenazas complejo y en constante evolución, no sorprende que el 71% de las empresas consultadas afirme ser víctima de un incidente de ciberseguridad de cierta gravedad al menos una vez al año, siendo la media general de 2 incidentes graves al año en base a los datos obtenidos.

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

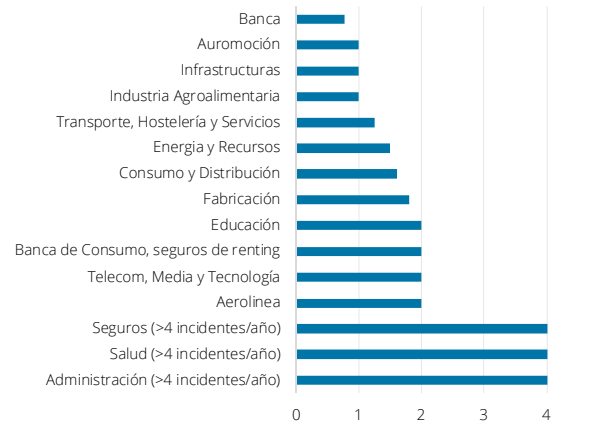


Analizando los datos por sector, se puede observar que Administración, Salud y Seguros son los sectores que reportan un mayor número de ciber incidentes en el último año, siendo este un dato muy interesante, ya que el 75% de empresas de estos sectores cuentan con un Comité de Respuesta a Incidentes y el 100% disponen de los servicios de SOC.

No sorprende que el 71% de las empresas consultadas afirme ser víctima de un incidente de ciberseguridad de cierta gravedad al menos una vez al año.

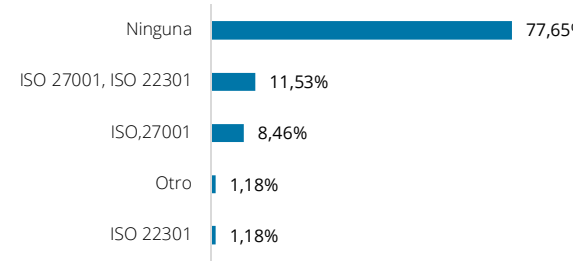
Administración, Salud y Seguros son los sectores que reportan un mayor número de ciber incidentes en el último año.

Promedio de incidentes al año



Incidentes de seguridad sufridos el último año VS las certificaciones de seguridad de las que dispone

Empresas que disponen de certificaciones:



% de empresas que sufrieron un incidente significativo de cibserguridad

Como se puede observar, 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 ciber incidentes o minimiza sus impactos. **Las empresas que no tienen ninguna certificación sufren incidente de ciberseguridad en un 77,65% de los casos**

Este dato desciende significativamente hasta el 11,53% de las empresas que sufre un incidente el último año cuando tienen de forma conjunta la certificación ISO 27001 e ISO 22301.

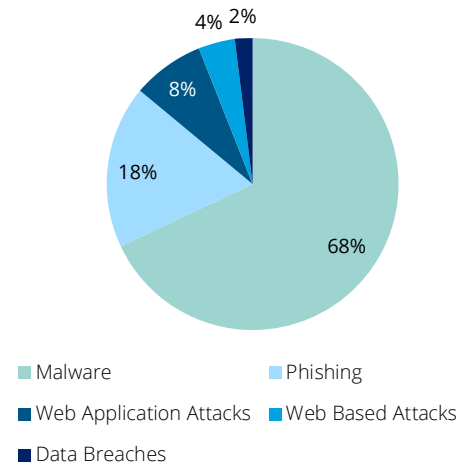
Y, ya por debajo, quedan las empresas que tienen solo 1 certificación.

Cabe destacar que las empresas que disponen de forma conjunta de la certificación ISO 27001 e ISO 22301, son a su vez las más grandes en términos de EBITDA, motivo por el cual son objeto de mayores ataques.

¿Cuáles cree que son las amenazas que afectan a su sector?

En consonancia con los informes publicados por organismos reconocidos internacionalmente, el malware, phishing y web application attacks parecen ser las amenazas con mayor incidencia en el contexto tecnológico de las empresas consultadas, independientemente del sector al que pertenecen. **Dentro de este grupo, se observa una clara preocupación por el malware, dado que el 68% de las empresas creen que esta es la principal amenaza para su negocio. Esto es un dato lógico si atendemos a los ataques sufridos por *ransomware* en los últimos años.**

Principales amenazas



El malware, phishing y web application attacks parecen ser las amenazas con mayor incidencia en el contexto tecnológico de las empresas consultadas.

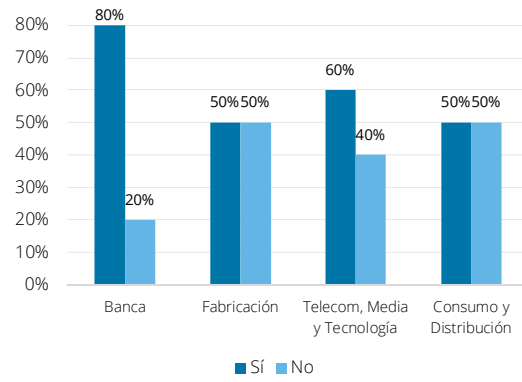
Percepción del CISO

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

En cuanto a la percepción del CISO sobre el nivel de seguridad de su empresa, **solo el 52% de ellos considera que esta se encuentra preparada para hacer frente a incidentes de seguridad**, mientras que un 38% considera que está poco preparada. Estos resultados concuerdan con los datos obtenidos con respecto a los recursos de los que disponen las empresas en materia de detección y respuesta a incidentes de seguridad.

Si se realiza un análisis por cuatro de los sectores claves, **destaca el sector Banca con un 80% de las empresas de este sector que consideran que están preparadas o bastante preparadas para hacer frente a un incidente de ciberseguridad que afecte a su negocio**.

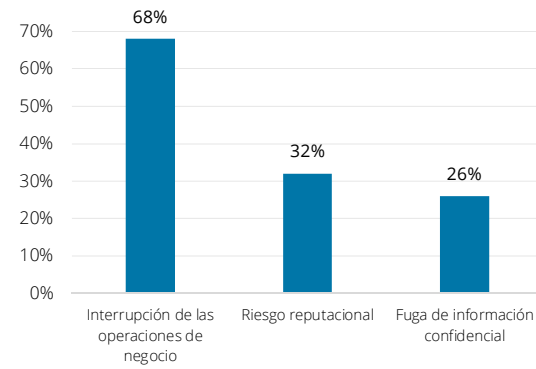
¿Se siente preparada para hacer frente a incidentes de seguridad?



No llama la atención que las empresas que consideran estar menos preparadas son las que tienen menos de 25 empleados en ciberseguridad (85% de ellas reportan menos de 10 empleados). También, cabe destacar que no hay ninguna empresa con más de 25 empleados dedicados que no se sienta preparada.

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

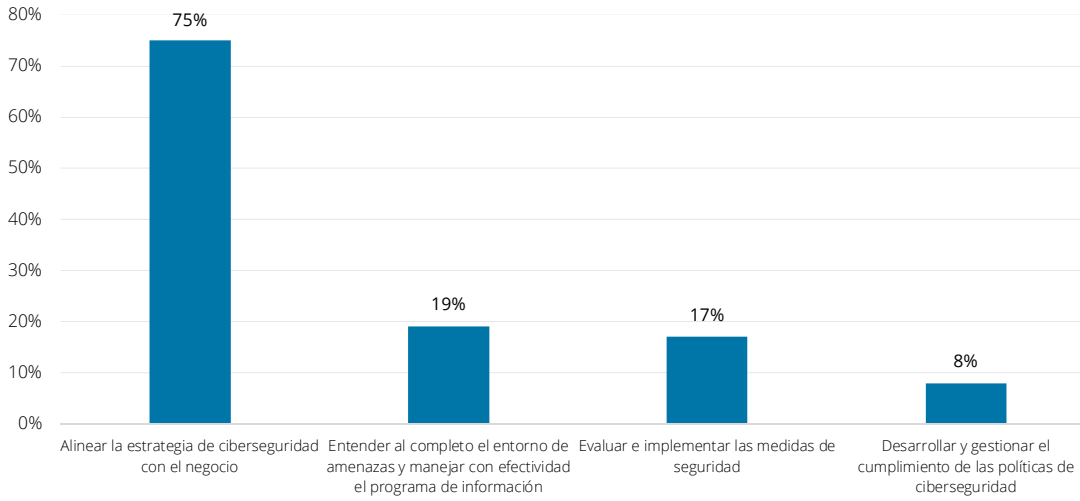
A continuación, vemos el porcentaje de CISOs que considera como principal preocupación:



Desde el punto de vista sectorial, las empresas de Fabricación son las más preocupadas por los riesgos que supongan una interrupción de sus operaciones, dado que el 86% de ellas considera la interrupción de las operaciones de negocio como su principal preocupación.

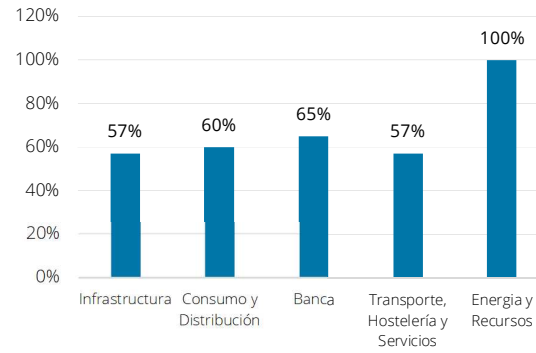
¿Cómo ordenaría las siguientes labores fundamentales del CISO de mayor a menor importancia?

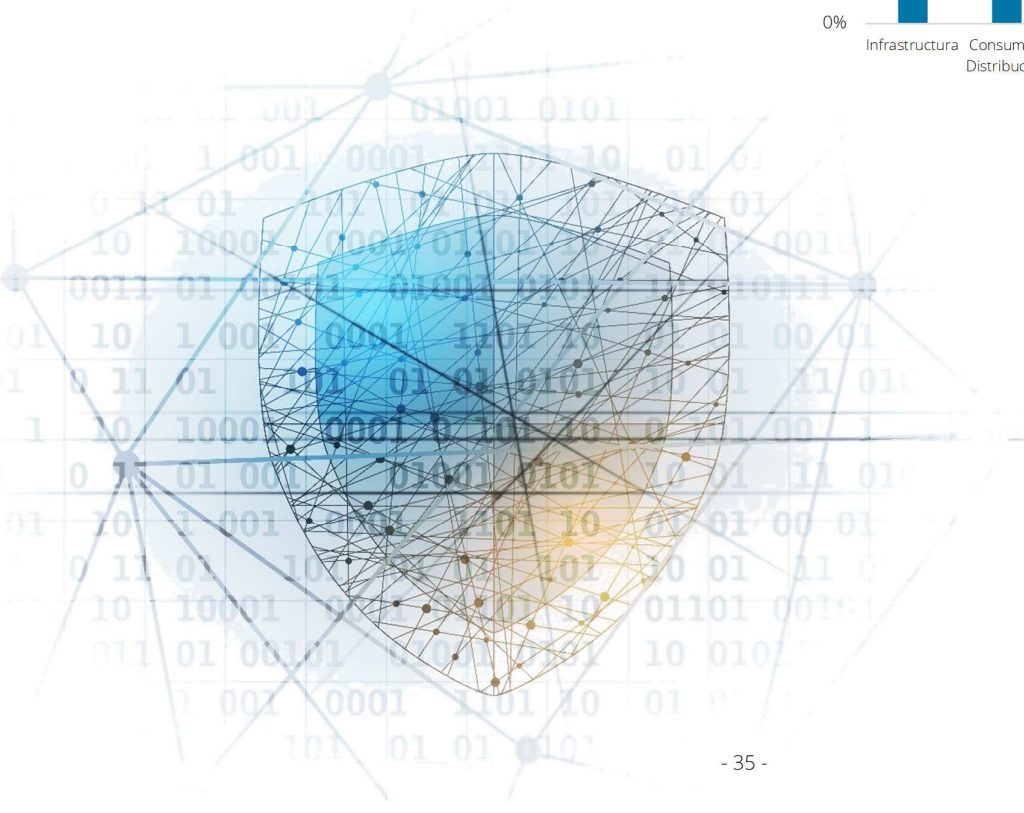
A continuación, vemos el porcentaje de CISOs que considera como principal preocupación:



En un análisis por sector, destaca que para el 100% de las empresas del sector Energía y Recursos la labor fundamental del CISO es el alineamiento de la estrategia ciberseguridad con el negocio, mientras que para casi la mitad de las empresas de los sectores de Infraestructuras y Transporte, Hostelería y Servicios, esta labor no es la más importante.

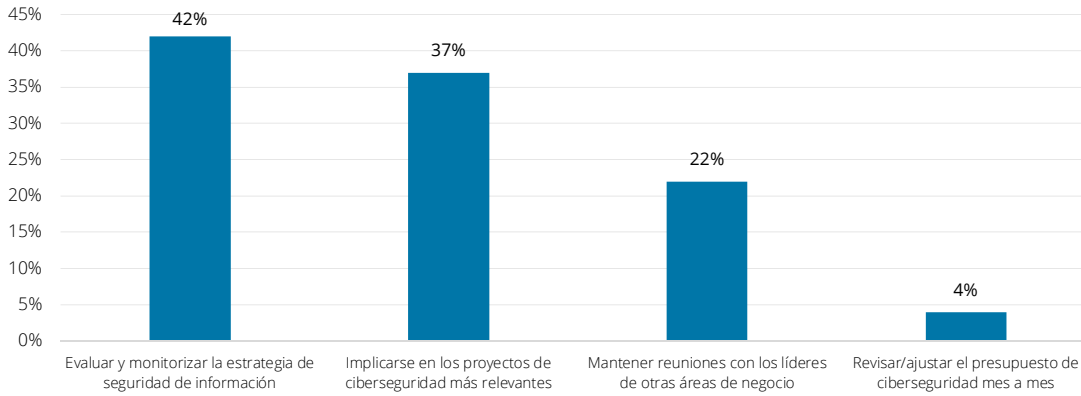
Alinear estrategia de negocio como principal preocupación





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

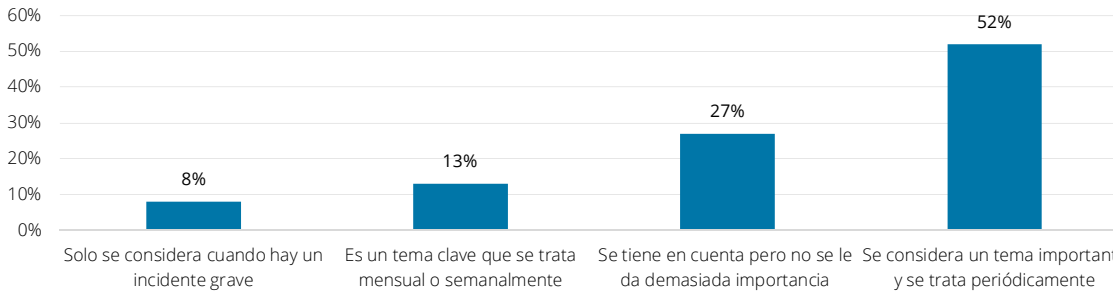
A continuación, vemos el porcentaje de CISOs que considera como principal actividad:



Se puede apreciar el contraste entre lo que se considera la labor más importante del CISO y las actividades que finalmente realizan, ya que **a pesar de que un 75% de ellos considera la alineación de la estrategia de ciberseguridad con el negocio como su labor más importante, las reuniones con otros líderes de negocio es prioridad dentro de la agenda para solo el 22% de ellos.**

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

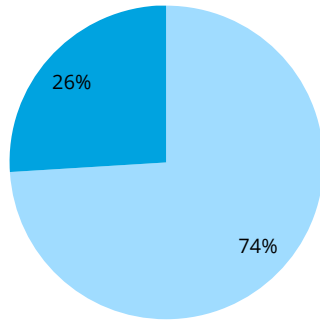
El papel de la Alta Dirección es clave en el éxito de la estrategia de seguridad de las empresas y, según los datos obtenidos, **para el 75% de las empresas consultadas la ciberseguridad es un aspecto muy importante que se trata periódicamente llegando, en algunos casos, a tratarse de forma semanal.**



El papel de la Alta Dirección es clave en el éxito de la estrategia de seguridad de las empresas y, según los datos obtenidos.

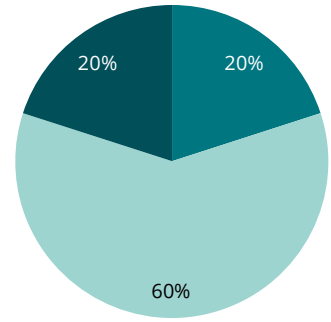
Si se realiza un análisis por sector, se obtienen los siguientes resultados:

Banca



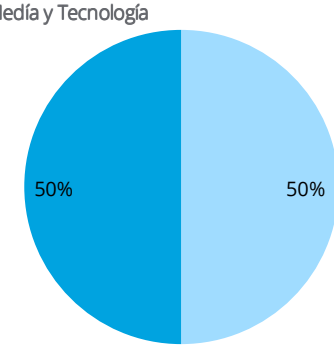
- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta pero no se la de demasiada importancia
- Es un tema clave que se trata semanal o mensualmente
- Solo se considera cuando hay un incidente grave

Consumo y distribución



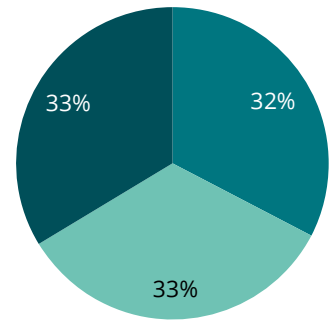
- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta pero no se la de demasiada importancia
- Es un tema clave que se trata semanal o mensualmente
- Solo se considera cuando hay un incidente grave

Telecom, Media y Tecnología



- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta pero no se la de demasiada importancia
- Es un tema clave que se trata semanal o mensualmente
- Solo se considera cuando hay un incidente grave

Fabricación



- Se considera un tema importante y se trata periódicamente
- Se tiene en cuenta pero no se la de demasiada importancia
- Es un tema clave que se trata semanal o mensualmente
- Solo se considera cuando hay un incidente grave

Dentro de este grupo, **destaca el sector financiero con un porcentaje de empresas significativo que cuenta con una Alta Dirección muy consciente de la ciberseguridad**.

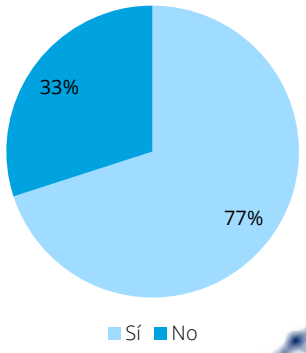
En el otro extremo se encuentra Fabricación, donde la Alta Dirección de un tercio de las empresas consultadas de este sector considera la ciberseguridad bajo un enfoque reactivo, es decir, solo cuando ocurre un incidente grave. No obstante, en base a las consideraciones del resto de empresas de este sector, se observa una tendencia creciente en cuanto al tratamiento de la ciberseguridad a niveles más ejecutivos.

Percepción del CISO en tiempos de pandemia

¿En los planes de contingencia incluidos en el Plan de Continuidad de su negocio de su compañía, anteriores a la pandemia, se contemplaban acciones de teletrabajo?

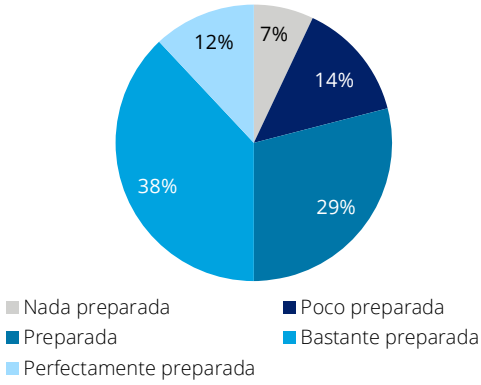
Con el avance tecnológico actual y el contexto sanitario en el que estamos sumergidos, la implantación de la modalidad de teletrabajo ha sufrido una gran aceleración. En un análisis sobre si existía ya cierta preparación por parte de las empresas para continuar con sus operaciones en un escenario de pandemia, se ha podido comprobar que un 77% de las empresas sí contemplaban el teletrabajo como alternativa en sus planes de contingencia.

¿Se contemplaba el teletrabajo en los planes de continuidad de negocio?



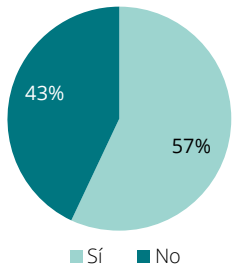
¿Cómo de preparada están las empresas para afrontar los riesgos de ciberseguridad que conlleva el teletrabajo en situaciones como la actual?

Solo un 21% de las empresas afirmar estar nada o poco preparada ante eventuales riesgos derivados del teletrabajo.



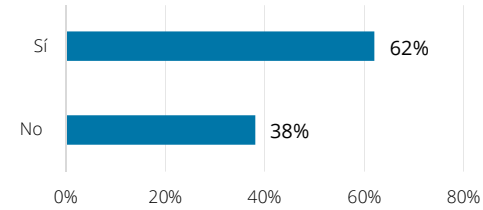
¿Considera que su organigrama de responsabilidades de ciberseguridad facilita la continuidad de las operaciones en un entorno no presencial?

Más de la mitad de los CISOs encuestados, solo el 43% de los mismos, considera que su organigrama de ciberseguridad actual facilita la continuidad de las operaciones en un entorno no presencial.



¿Considera que los intentos de ataque a su infraestructura tecnológica han aumentado en el momento de la adopción de las medidas de teletrabajo?

El 62% de las empresas consultadas consideran que los intentos de ataques a sus infraestructuras tecnológicas han aumentado tras la adopción del teletrabajo como su principal modalidad de trabajo.

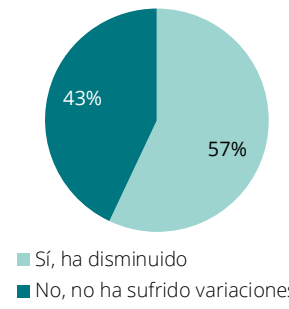


El 62% de las empresas consultadas consideran que los intentos de ataques a sus infraestructuras tecnológicas han aumentado tras la adopción del teletrabajo.

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

Más de la mitad de los CISOs consultados han sido testigos de cómo, en contraste con lo esperado desde un punto de vista de dotación de recursos, los presupuestos anuales dedicados a la ciberseguridad han sufrido una reducción en comparación con años anteriores. Es imaginable que estas reducciones obedezcan a limitaciones impuestas por el propio negocio en previsión de caídas en su volumen de facturación y beneficios, mas no a una disminución en la conciencia de las empresas sobre la importancia de la ciberseguridad ante el abanico de riesgos derivados de este nuevo contexto tecnológico y social.

¿Considera que el presupuesto anual de ciberseguridad se ha visto variado?



Deloitte.