El Libro Blanco del CISO

SEGUNDA EDICIÓN

Una iniciativa de

ISMS forum spain

CSC Cyber Security Center

Apoyo institucional

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

El Libro Blanco del CISO

SEGUNDA EDICIÓN

Dirección y coordinación:

ALBERTO HERNÁNDEZ, Director General de INCIBE
FRANCISCO LÁZARO, Miembro de la Junta Directiva de ISMS Forum.
GIANLUCA D'ANTONIO, Presidente de ISMS Forum.

Colaboradores:

ÁNGEL CAMPILLO
ÁNGEL PÉREZ
CARLES SOLÉ
CARLOS A. SAIZ
DANIEL LARGACHA
ELENA MATILLA
GEMMA DÉLER
GONZALO ASENSIO
GUSTAVO LOZANO
IVÁN SÁNCHEZ
JAVIER SEVILLANO
JÉSÚS MÉRIDA
JOSÉ RAMÓN MONLEÓN
JOSÉ ANTONIO PEREA
LUIS BALLESTEROS
MANUEL FERNÁNDEZ
MARCOS GÓMEZ
MARIANO J. BENITO
PEDRO DÍAZ
RAFAEL SANTOS
RAFAEL HERNÁNDEZ
RAMÓN ORTIZ
ROBERTO BARATTA

Revisores:

ALFONSO LÓPEZ-ESCOBAR
ELENA MATILLA
GUSTAVO LOZANO

Editor:

DANIEL GARCÍA SÁNCHEZ, Director General de ISMS Forum.

Diseño y maquetación:

CYNTHIA RICA GÓMEZ, Responsable de comunicación de ISMS Forum.

ÍNDICE

1 INTRODUCCIÓN Y CONTEXTO ACTUAL

El Foro Económico Mundial en su Informe Global de Riesgos del 2019 incluye dentro del Top 5 los riesgos más preocupantes que amenazan la estabilidad global (por la combinación de su probabilidad de ocurrencia e impacto) al robo o uso fraudulento de los datos, así como a los ciberataques. Son estas, por tanto, unas de las grandes preocupaciones a nivel global tanto en el entorno público como privado. La dependencia de las redes y de los sistemas de información para el bienestar, la estabilidad y el crecimiento de las Naciones es un hecho, como también lo es la interdependencia de tecnologías e infraestructuras.

Para las empresas, los nuevos paradigmas como son la Transformación Digital, el uso de soluciones basadas en la Nube o Cloud Computing, la incorporación de dispositivos IoT, el Big Data, suponen un cambio en la forma de entender cómo la tecnología facilita el negocio.

Por otro lado, la tendencia Fast, Cheap & Easy en la gestión de Sistemas de Información para reducir el tiempo y coste de la provisión de nuevas soluciones y que se apoya en metodologías ágiles (Lean, DevOps, Agile) supone tanto un reto en la elaboración de los Análisis de Riesgos, como en el control del desarrollo de sistemas de información y hace más importante la necesidad de tener en cuenta la Seguridad de la Información desde el diseño y durante todo el ciclo de vida de cualquier Producto o Servicio.

Todos los actores están preparándose a este nuevo escenario. La Administración está centrando sus esfuerzos en la definición de distintos marcos regulatorios: La Estrategia de Ciberseguridad, el Reglamento General de Protección de Datos Personales, el Real Decreto-Ley de Seguridad de las Redes y los Sistemas de información, el Esquema Nacional de Seguridad (ENS), la normativa sobre protección de infraestructuras críticas y la normativa de seguridad privada. Todas ellas con un factor común, establecer un conjunto de criterios o medidas de seguridad a aplicar.

Por todo ello, el papel del Responsable de Seguridad de la Información (CISO por sus siglas en inglés de Chief Information Security Officer) cobra un papel trascendental en las organizaciones del siglo XXI. La seguridad por defecto, desde el diseño y la debida gestión de los riesgos de seguridad son elementos clave para garantizar la supervivencia de las organizaciones del futuro, y en general de la sociedad. Debe ser capaz de poder cohesionar la estrategia en materia de Seguridad de la Información de las organizaciones.

No obstante, dependiendo de cada entidad estas funciones del CISO pueden ser asignadas a otros roles (o junto con otros roles) dentro de la estructura or- ganizativa. Algunos de estos roles son: el del CRO (Chief Risk Officer), el COO (Chief Operating Officer), CIO (Chief Information Officer) DPO (Data Protection Officer), CDO (Chief Data Officer), CTSO (Chief Technology Security Officer) o CSO (Chief Security Officer). En todo caso, será cada entidad quien deba de- finir el modelo organizativo y de relación en materia de seguridad dentro de su organización prevaleciendo el principio de segregación de funciones. En función de la madurez de las entidades y su sensibilidad ante la seguridad de la información el rol del CISO se encontrará jerárquicamente enmarcado: en la alta dirección (formando parte de los comités de dirección), en la Dirección de IT - Tecnologías de la Información, en la Dirección de Riesgos o en Seguridad Corporativa.

Esté donde esté, sin lugar a dudas el CISO es una figura clave dentro de las organizaciones debiendo definirse claramente sus atribuciones y su perfil, como ya se hizo anteriormente con otros roles como el del CIO, el CFO (Chief Financial Officer) o Auditoría Interna.

Este Libro Blanco dedica el capítulo IV a identificar el marco normativo al que debe dar respuesta el CISO. Su propósito es orientativo y no debe entenderse como una lista exhaustiva dada la intensidad y constante evolución de los trabajos que se realizan en esta materia, tanto a nivel nacional como europeo e incluso internacional/global. En el estudio del marco normativo, el CISO debe tener en cuenta junto con la legislación, aquella regulación que se desarrolla en otros foros, en ocasiones formados directamente por la industria, y que le es de aplicación. Un ejemplo sencillo es la normativa PCI-DSS, que en la práctica se puede considerar de obligado cumplimiento y que emana del consorcio formado por los esquemas de pago.

Este libro blanco recoge el rol y funciones del CISO del siglo XXI, como facilitador del negocio para alcanzar sus objetivos y aumentar su resiliencia.

II ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA

La seguridad de la información describe el conjunto de actividades orientadas a proteger la información allí donde se procese (sistemas), almacene (repositorios) y transmite (redes de comunicaciones), buscando mantener la confidencialidad, la disponibilidad e integridad de la información, así como su autenticidad y trazabilidad.

El presente capítulo identifica la misión y responsabilidades principales del Responsable de Seguridad de la Información de una organización, conocido también como CISO (Chief Information Security Officer).

II.1.- La misión del CISO.

El CISO tiene como misión definir la estrategia global de Seguridad de la Información de la organización a su cargo, coordinar su materialización en todos los ámbitos de la misma, identificar el nivel de riesgo existente y promover una cultura de resiliencia en esta materia.

Para lograr el cumplimiento de dicha misión el CISO debe contar con dos aspectos fundamentales:

- Tener los conocimientos, competencias y experiencia necesarias (se desarrolla en el capítulo VI)
- Apoyo de la Alta Dirección, con una definición clara de ámbitos y responsabilidades.

Este último punto es especialmente crítico pues, como se verá en el capítulo V de Modelos Organizativos y Relacionales, es imprescindible tener un marco de relación claro con todos los stakeholders relacionados con el desarrollo de su misión.

Como ocurre con el modelo organizativo, no existe una definición única de las funciones responsabilidad del CISO. Se pretende, no obstante, realizar una relación lo más exhaustiva posible, identificando de algún modo aquéllas que consideramos imprescindibles y aquellas que, en función del tipo de organiza- ción o madurez de esta, podrían recaer en otras áreas de la organización.

Las siguientes responsabilidades (agrupadas por dominios de seguridad) deben entenderse como la misión principal de un CISO, entendiendo las mismas como no delegables. Siendo el mínimo necesario exigible para considerar que existe realmente un responsable de la seguridad de la información en una entidad:

Dominio estratégico

- Alinear la estrategia de seguridad de la información con los objetivos de la organización.
- Comunicar y coordinar las áreas operativas, actuando de enlace con la Alta Dirección en materia de seguridad de la información (estado de riesgos, planes de acción, amenazas, incidencias y control económico)
- Establecer métricas e indicadores de seguridad que permita a la organización conocer su nivel de seguridad actual, así como la mejora a futuro.
- Formar, concienciar y sensibilizar a la organización en materia de seguridad de la información.

Dominio de cumplimiento normativo y legal

- Definir el marco normativo de seguridad (Políticas, Normas y procedimientos) y velar por su cumplimiento
- Supervisar el cumplimiento de la legislación en los aspectos referidos a su ámbito de actuación.
- Mantener interlocución con otras organizaciones, instituciones, reguladores y Fuerzas y Cuerpos de Seguridad del Estado en materia de seguridad de la información.

Dominio de gestión de riesgos

- Identificar el nivel de riesgo existente en los activos de información de la organización a su cargo.
- Asesorar a los propietarios de dichos activos para definir el "apetito de riesgo" asociado, impulsando su definición para cada riesgo identificado, y la estrategia más adecuada de gestión (asumir, reducir, transferir o eliminar).
- En base a la definición del apetito de riesgo anterior establecer el plan de acción correspondiente identificando requisitos específicos de seguridad.
- Identificar e impulsar la identificación y establecimiento de los controles de seguridad necesarios para acometer el riesgo (controles organizativos, procedimentales, así como los técnicos y humanos).

Dominio operativo

- Supervisar el Nivel de seguridad, el cumplimiento de los controles y el grado de eficacia de las medidas aplicadas.
- Gestionar la operación de seguridad de la información, sea directa, a través de servicios externalizados o a través de otras áreas de la organización.
- Liderar la gestión de incidentes de seguridad, sea directa, a través de servicios externalizados o a través de otras áreas de la organización.

Si bien las funciones descritas anteriormente son responsabilidad última del CISO, es habitual que, en función de las características de cada entidad, algunas de ellas sean delegadas a otras áreas organizativas.

II.2.- Actividades del CISO.

Para llevar a cabo estas funciones, son muchas las actividades que desarrolla el CISO, enumerándose a continuación las principales.

Se toma como marco de referencia el proporcionado por NIST (National Institute of Standards and Technology), que es el más utilizado actualmente (existen otros marcos de control que servirían igualmente). Si bien ampliándolo en unos casos y modificándolo en otros. Es posible también utilizar un marco principal de referencia complementándolo con otro en base a los requerimientos de negocio, por ejemplo, usar NIST y complementarlo con ISO/IEC 27001:2013 en un alcance concreto porque vamos a certificarnos, o complementarlo con la ISO20000 si nuestro negocio se dedica a la operación de sistemas o ISO22301 si la continuidad de negocio en clave para el desarrollo del mismo.

IDENTIFICAR

- Conocer el contexto de negocio para definir los planes estratégicos, tácticos y operativos necesarios.
- Definir las estrategias de la organización en seguridad de la información, asegurando que se alinean con el resto de las estrategias de la organización, y de que son aprobadas por la Dirección.
- Una vez aprobada la estrategia, desarrollar su ejecución bien directamente, o mediante la supervisión de otras áreas que están involucradas en dicha ejecución y mediante la coordinación con otras áreas de la organización.
- Conocer los activos de la empresa (personas, procesos, aplicaciones, redes y sistemas), su valor y criticidad.
- Conocer los aspectos/obligaciones normativos, legales y contractuales aplicables y su aplicabilidad al contexto de la empresa.
- Identificar los recursos necesarios (personal y presupuesto) para realizar la función de seguridad de la información adecuadamente, y en función de ello efectuar una priorización y planificación que establezca el equilibrio
- adecuado entre la estrategia aprobada y los recursos disponibles.
- Definir el mapa de riesgos de seguridad de la empresa: Realizar la evaluación de riesgos de Seguridad de la Información de la organización, incluyendo tanto las actividades de análisis de riesgo, como de evaluación de los mismos y preparación de los planes de tratamiento de riesgos deriva- dos. En ocasiones, esta actividad cubrirá el total de gestión de riesgos de la organización.
- Identificar el nivel de riesgo aceptable para la Organización; es decir que umbral de riesgo esta dispuesto asumir la alta dirección.
- Definir los indicadores y las métricas de seguridad necesarios para evaluar el estado de la seguridad.
- Definir el marco de control normativo de seguridad (políticas, normas, guías, procedimientos).
- Establecer los reportes hacia la Alta Dirección, los órganos de gobierno, las áreas de interés (Auditoría, Control Interno, Ries- gos, RRHH, etc.) y stakeholders relacionados con su función.

- Establecer los comités y grupos de trabajo necesarios para coordinar la seguridad de la información dentro de la compañía. Debería existir al me- nos un comité periódico con participación directiva.

- Establecer los contactos pertinentes con reguladores, peers (sectoriales y multisectoriales), fuerzas y cuerpos del estado, fabricantes y proveedores estratégicos. Este punto es relevante pues contribuye a consolidar una red de inteligencia global permitiendo anticipar la identificación de amenazas en las organizaciones participantes.

- Establecer los canales de reporte y colaboración con autoridades y reguladores, CERTs de interés y fuerzas y cuerpos de seguridad del Estado.

PROTEGER

- Diseñar e implantar de la arquitectura de seguridad.

- Prevenir el fraude, al menos el cometido a través de medios electrónicos.

- Establecer la clasificación de la información/dato y de las medidas de protección.

- Establecer e implantar las medidas de protección de la infraestructura IT (perimetral, redes, servidores) incluyendo la configuración segura por defecto.

- Establecer e implantar las medidas de protección de losen dispositivos de usuario.

- Establecer las medidas de seguridad exigibles a entornos Cloud.
  Incluir la seguridad por defecto y en el diseño en aplicaciones (desarrollo seguro), así como la gestión proactiva de vulnerabilidades.

- Asegurar el cumplimiento normativo.

- Definir y participar en las actividades de formación, concienciación y sensibilización en Seguridad de la Información del personal de la Organización.

- Establecer los planes de formación, concienciación y sensibilización a toda la organización. Diseñar las guías (“playbooks”) de respuesta ante incidentes

- Supervisar (al menos) la seguridad y privacidad de los datos (según las funciones que se hayan establecido de manera complementaria al Delegado de Protección de Datos).

DETECTAR

- Supervisar las actividades de actualización permanente y corrección de errores en los sistemas de información de la organización, lo que inclu- ye la realización de pruebas de penetración en los sistemas, seguimiento de actividades de parcheo y corrección de vulnerabilidades, inventario TI, etc.

- Monitorizar y gestionar alertas sobre la actividad de personas, sistemas y aplicaciones.

- Monitorizar activa sobre amenazas avanzadas (threat inteligence) así como detectar activos no controlados/nocorporativos.

- Detectare comportamiento normal, anomalías y desviaciones.

- Detectar ataques a la infraestructura/comunicaciones (DDoS) y elaborar análisis forenses.

- Participar en la realización de ciberejercicios (simulación ofensiva y respues- ta).

- Ejecutar acciones de threathunting (búsqueda proactiva de amenazas avan- zadas en redes internas que evaden las medidas de protección habituales).

- Establecer medidas de defensa activa.

RESPONDER Y RECUPERAR

- Definir, implantar y liderar la respuesta ante incidentes de seguridad de la información en la organización.

- Coordinar las medidas de contención y recuperación necesarias para resolver el incidente que se produzca y, si es preciso, invocar al equipo de Continuidad de Negocio implicado.

- Participar, ante incidentes de especial criticidad, que afecten de forma grave los compromisos y actividades de la organización, o que se prevea tengan importantes consecuencias derivadas, en el Comité de Crisis aportando su visión experta para lograr, de forma ágil, conocer la gravedad, implicaciones, su posible evolución, así como definir cuál debe ser el posicionamiento de la organización ante todos los stakeholders e impulsar una respuesta global desde una perspectiva estratégica,

- Denunciar ante las autoridades competentes un ciberataque.

- Realizar o coordinar análisis forenses, y en su caso, los informes periciales. Así como defenderlos en sede judicial (si procede).

- Diseñar la respuesta automatizada ante casos de uso conocidos.

- Establecer y llevar a cabo la notificación de incidentes conforme a las distintas leyes y normativas.

- Supervisar la continuidad de negocio de las operaciones, incluyendo y superando los planes de recuperación ante desastres, o los planes de contingencia TI desarrollados por las áreas de sistemas de la información.

INFORMAR Y COORDINARSE

- Informar/reportar a la alta Dirección y cuando proceda: a autoridades competentes o en sede judicial.
- Coordinarse con otras figuras relevantes relacionadas con su ámbito de actuación tales como Protección de Datos, Área Jurídica, Auditoría, Ries- gos Corporativos, Comunicación, Recursos Humanos.
- Coordinarse con otros centros de respuesta a incidentes.
- Colaborar en grupos de interés en esta materia.

Algunas organizaciones con mayor madurez, recursos y/o circunstancias específicas pueden haber establecido varias funciones y roles dentro de su organización para satisfacer todas las necesidades señaladas. Todo ello sin perjuicio de la capacidad del CISO de abordar todas ellas y de la necesidad del CISO de estar informado y/o supervisar estos aspectos de la organización para asegurar el cumplimiento de los objetivos de seguridad de la información.

Se ha de incidir en la conveniencia de mantener al CISO focalizado en actividades de su ámbito específico, segregando las responsabilidades y funciones propias de la operación de TI en los equipos de sistemas.

Finalmente, se destaca la necesidad de que se detalle de manera clara el nivel de segregación de funciones dentro del modelo organizativo y de relación. Por ejemplo, habrá organizaciones donde el CISO junto con su equipo marque la estrategia y políticas e implementen los controles de seguridad (operar la seguridad) y otras, en las que definan la estrategia, políticas y supervisen, y se segregue la operación a otras áreas más técnica relacionada con TI. En todo caso el CISO debe jugar un papel fundamental de segunda línea de defensa con Auditoría Interna (tercera línea de defensa).

II.3.- Actividades del CISO no directamente relacionadas con TI.

La mera revisión de las actividades de un CISO revela que sus responsabili- dades incluyen, pero no se limitan a los Sistemas de Información y a aspectos TI. Ciertamente, el CISO debe ser un experto en Seguridad de la Información en TI, al igual y al mismo nivel que lo debe ser en Seguridad de la Información con una fuerte base técnica pero también con visión y comprensión del negocio.

Esa misma inspección de las actividades señala repetidamente que la responsabilidad del CISO se centra fundamentalmente en la definición y supervisión de

los distintos elementos y campos que son necesarios para asegurar la correcta gestión de la seguridad de la información.

Por ello, un CISO debe ser transversal a toda la organización en la medida en la que debe proteger la información y los activos tecnológicos de toda la organización. Las medidas de protección de la información abarcan tanto medidas tecnológicas como no tecnológicas y es responsabilidad del CISO dirigir y velar por su aplicación.

II.4.- El CISO como Directivo.

Aunque muchas organizaciones consideran la figura del CISO como un recién llegado a la organización, esta afirmación simplemente revela que estas organizaciones no han sido conscientes de la necesidad de esta figura hasta hace poco. Las organizaciones con más madurez han nombrado y cuentan con un responsable de la seguridad de la Información y una estructura organizativa asociada a él desde hace más de 25 años. Y ciertamente, se trata de una figura cada vez más demandada por las organizaciones, a medida que se convierte en una cuestión prioritaria para su negocio la adecuada protección de la información y activos que utilizan en sus actividades, sea propia o de ter- ceros, sea directamente o con colaboradores.

En la actualidad el CISO es la máxima autoridad en materia de seguridad de la información en una organización.

Es el directivo de la entidad que se encarga de dirigir, orientar la estrategia de seguridad de la entidad y coordinar su implantación. Es su responsabilidad ali- near los objetivos de seguridad de la información de la entidad con sus objeti- vos de negocio. Con el mismo horizonte y visión que el resto de los directivos de la organización en sus ámbitos respectivos, sean la tecnología (CTO), los Sistemas de Información (CIO), o la ejecución del total de la organización (CEO).

Como tal directivo, el CISO debe liderar diferentes órganos de gestión como el comité de seguridad de la información o el comité de ciberseguridad, en otros ser parte relevante como puede ser el caso del comité de protección de datos, y en otros ser un miembro permanente y activo como en el comité de riesgos, transformación digital o incluso comité de dirección dónde materialice su misión principal de gestión e implantación de la estrategia de seguridad de la información corporativa.

Obviamente no todas las organizaciones tienen estos comités, pero se quiere significar que en aquellos que estén constituidos, el CISO debe procurar ejercer un papel relevante y activo en ellos.

III LA FUNCIÓN DE SEGURIDAD DE LA INFORMACIÓN

III.1.- Seguridad de la Información: evolución de la función de Control TI a Gestión de riesgos y cumplimiento.

Para que sirva de contexto la seguridad que hoy en día conocemos como Ciberseguridad (al menos para la mayor parte de la población) no siempre fue así y del mismo modo fue cambiando el rol del CISO conforme han ido evolu- cionando los departamentos de seguridad y su nombre.

Allá por los años 90 este departamento tecnológico se llamaba seguridad de control de acceso; principalmente porque los datos se "encontraban" en su mayoría en el CPD. En este contexto el CISO era una persona operativa, dependiendo del departamento de informática o del área de sistemas, que aplicaba las medidas de seguridad sobre el control de acceso a la información.

Después y puesto que existía una figura de seguridad física, evolucionó hacia seguridad lógica para hacer una distinción, ya que no sólo se trata de control de acceso, usuarios, etc. sino que abarca más temas tecnológicos; el CISO en estos casos extendió su influencia, pero siempre referido al control de acceso y manteniendo la dependencia orgánica.

Posteriormente el equipo del CISO viró hacia la seguridad perimetral , pasando a controlar toda la seguridad perimetral y, por tanto, a ver como un todo los diversos dispositivos que la componían y que requerían de reglas y procedimientos de actuación; realmente no se había salido de tener a administradores de sistemas de seguridad y, por supuesto, integrado en el departamento de informática.

Con el paso del tiempo, la figura ha ganado madurez y se ha entendido necesaria en términos de negocio, incorporando este rol en los procesos de negocio de las organizaciones. Siendo por tanto un rol estratégico además de técnico.

Toda esta transformación ha dado lugar a que el CISO esté integrado en las Organizaciones en diferentes posiciones que los siguientes modelos presentados en el capítulo IV.

También la denominación del alcance objetivo de lo que protegía ha ido evolucionando con el tiempo. Inicialmente era Seguridad Informática puesto que el foco estaba en los equipos informáticos, más tarde se denominó seguridad lógica tanto para denotar que protegía activos más amplios que los ordenadores, como una forma de identificarla diferenciándola de la seguridad física. El posterior nombre de Seguridad de la Información puso el foco en la infor- mación (principal activo) y ya no sólo en los sistemas que la tratan.

Una evolución de este término es el termino de Ciberseguridad es el que está calando en las Organizaciones y en la Sociedad ya que contempla todos los aspectos: Humanos, datos, información, técnicos, organizativos, políticas, planes y procedimientos, cumplimiento normativo, y de coordinación, supervisión y definición. Incluso, se empieza a hablar del concepto de "seguridad digital" como sustitución del de ciberseguridad, que pretende ser más acorde al nuevo paradigma tecnológico en el que se está inmersos.

Si bien es cierto que inicialmente la Ciberseguridad puede ser considerada como una parte de la Seguridad de la Información (la relativa a sistemas conectados al "Ciberespacio" -Internet-), lo cierto es que tanto por ser prácticamente imposible encontrar un activo de información que no se conecte, directa o indirectamente a Internet, como por la asociación del término a ataques que ya no sólo tratan de información, sino también de vidas humanas, el término se va fortaleciendo frente a otras denominaciones.

Una vez conocido el contexto de la evolución del departamento de seguridad de la información también es importante conocer los nombres de la figura que ha encabezado esta área. Ya que no siempre se llamó CISO, al menos no en España.

A lo largo de los tiempos hemos podido ver nombres tales como jefe de seguridad informática, responsable de seguridad lógica, responsable de seguridad informática o director de seguridad informática (cuando ya empezaba a verse la seguridad en un nivel ejecutivo), etc. El nombre por el que más se le conoce hoy en día es el de CISO, término procedente del entorno cultural anglosajón.

Una vez ubicado el origen y evolución del nombre del departamento de Seguridad de la Información y el nombre del puesto que lo gestiona podemos entrar a analizar diferentes modelos organizativos y relacionales dentro de una determinada empresa, independientemente del sector.

Al principio como hemos visto en los nombres de los departamentos, el CISO (no llamado así antes) se ubicaba en áreas muy dispares; esto puede seguir ocurriendo según la empresa, tamaño, naturaleza, sector, etc. Es muy importante recalcar que no existe un modelo único o perfecto, sino que todos son imperfectos y por tanto contarán con ventajas y desventajas; no se trata de decidir cuál de estos debe existir, sino de plantear un análisis de la mayoría de los modelos que existen y que son igualmente válidos para cada organización. No debemos olvidar que al final, las empresas las componen trabajadores, es decir personas que se relacionan entre ellos con un mismo objetivo.

Se configura, consecuentemente, como una función cada vez más transversal ("cross") en la medida en la que todos los procesos de negocio se van digitalizando. En esta evolución hacia una visión holística de la tecnología, la gestión de los riesgos con ella relacionados, se convierte en un elemento estratégico de la toma de decisiones. El CISO se configura como un Gestor y al mismo tiempo Asesor de la Dirección General capaz de organizar los recursos necesarios para asegurar la resiliencia de la organización frente a las ciberamenazas.

Por lo tanto, está claro que la SEGURIDAD y la figura del CISO debe de ser cada vez más una función multidisciplinar. Con múltiples áreas de acción y con diversidad de competencia, según las diferentes organizaciones.

El entorno regulatorio y los desafíos que el cumplimiento normativo representan para el gobierno de las tecnologías de la información ven en la figura del CISO un referente dentro de la organización. Los nuevos paradigmas tecno- lógicos como son el Cloud Computing, la Inteligencia Artificial, el Internet de las Cosas, etc. centrarán el desarrollo normativo de los próximos años. En la medida en que la gestión de los riesgos tecnológicos se traduzca en derechos y obligaciones una función del CISO será la de colaborar para asegurar el cumplimiento de este nuevo entorno regulatorio.

En una realidad convergente, donde la conectividad se convierte en un requisito básico del entorno, la Seguridad de la información debe asegurar la protección de los activos tanto físicos como lógicos a través de una organización eficiente de las capacidades, recursos y procesos tecnológicos. El objetivo es la seguridad, confianza y resiliencia de los entornos y de las personas.

III.2.- Gobierno de la Seguridad de la Información.

Podemos definir Gobierno Corporativo como "La estructura a través de la cual se establecen los objetivos de la empresa, y se determinan los medios para alcanzar dichos objetivos y monitorear el desempeño" (OCDE). Esta estructura aplicada a seguridad de la información incluye:

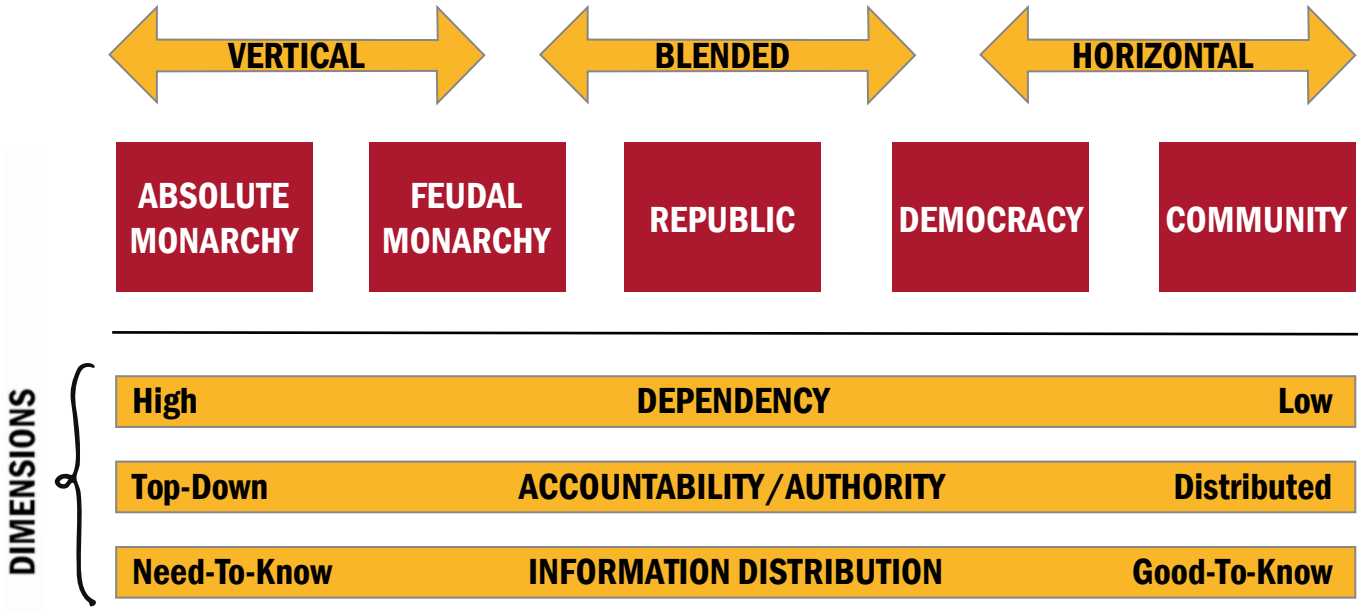
- La estrategia corporativa global de seguridad de la información.
- Políticas corporativas y sus respectivas normas y procedimientos.
- Planes estratégicos de recuperación y respuesta
- Planes de concienciación, formación y sensibilización.
- Análisis y gestión de riesgos.
- Planificación de auditorías y otras actividades de aseguramiento.

Las organizaciones han tenido que realizar una transformación radical con el avance de las tecnologías de la información, que ha convertido cualquier elemento físico en un bloque de información almacenada digitalmente al que hay que aportar seguridad, ya que cualquier daño en la confidencialidad o integridad de la información puede causar daños irreparables para las organizaciones.

El Gobierno de la seguridad debe alinear los objetivos y estrategias de Seguridad de la información con los objetivos y estrategias del negocio. Debe estar soportada por un sistema de control interno basado en el análisis de los riesgos de acuerdo a la legislación vigente y las regulaciones que impulsan y refuerzan estos cometidos.

En la actualidad nos encontramos con una realidad creciente en número e importancia, las ciberamenazas que obligan a las organizaciones a reinventarse en materia de seguridad, ya que las herramientas, protocolos y procesos tra- dicionales han dejado de ser efectivos. Proteger la información y controlar el acceso a los recursos internos se han convertido en puntos estratégicos a tener en cuenta en cualquier organización.

Para responder a estas ciberamenazas es muy importante la adecuada integración del CISO en la organización. Bien sea esta plana o jerarquizada, la función de seguridad de la información debe de ser capaz de interactuar y sustentarse en el más alto nivel de la organización.



De acuerdo a este esquema podemos hablar de dos tipos de estructuras organizativas:

- Horizontales, aquellas en las que sobresalen las figuras y los cargos directivos por encima del resto de integrantes.

- Verticales, en las que dichos cargos delegan las responsabilidades en niveles intermedios o bajos.

En la actualidad nos encontramos con una realidad creciente en número e importancia, las ciberamenazas que obligan a las organizaciones a reinventarse en materia de seguridad, ya que las herramientas, protocolos y procesos tradicionales han dejado de ser efectivos. Proteger la información y controlar el acceso a los recursos internos se han convertido en puntos estratégicos a tener en cuenta en cualquier organización.

Así las cosas, cualquiera que sea el arquetipo que prevalezca en una organización o la forma como se encuentre organizada la función de seguridad de la información, ésta debe sustentarse en el más alto nivel directivo de la organización.

De esta forma, para la Seguridad de la Información, nos podemos encontrar las siguientes capas de entidades y responsabilidades:

•Gobierno: Elabora Programa Seguridad acorde a los Requisitos Estratégicos (Política y estrategia)
•Gestión: Ejecuta el Programa de Seguridad (y Planes de Acción)
•Operación: Ejecuta los Procesos o actividades operativas de seguridad. (Instrucciones, Reglas, Normas, Etc.).

Según la encuesta realizada en 2019 por ISMS Forum a CISOs de diferentes empresas en España, reconocen que su función prioritaria es la dirección Estratégica y Planificación. Este hecho sitúa la capa de gobierno como la más importante.

La encuesta menciona como la siguiente función prioritaria a la Construcción de relaciones y asociaciones con las partes interesadas de negocios y de TI. Se puede considerar que esta función se encuentra a caballo entre las capas de Gobierno y de Gestión. Otra función mencionada como prioritaria es la Comunicación y Concienciación de Seguridad.

La Dirección de las organizaciones tiene que ser consciente de los ciberriesgos que conlleva su actividad, debe conocer las estrategias, planes y medios de que disponen para defenderse de un ciberataque, debe comprender el impacto potencial que puede tener un ciberataque en la organización y debe contar con planes de recuperación ante desastres para responder a tiempo y con solvencia a un ciberataque, ya que el tiempo de reacción es un factor clave.

Por ello, es imprescindible que la Dirección reciba un adecuado informe del estado de seguridad, con carácter periódico que incluya, entre otros:

- Nivel de protección.
- Medidas de vigilancia existentes.
- Mecanismos de respuesta, recuperación y vuelta a la normalidad en caso de un ciberataque.

El cuadro de mando que le tiene que llegar a la Dirección debe proporcionar una gran visibilidad sobre el estado general de la seguridad de la información en relación con los objetivos de negocio de la organización. Este informe debe ser entendible, conciso y comparable.

El conocimiento y la capacidad de acción de un CISO viene de una forma determinante impuesta por su ubicación en el Organigrama de la empresa y en su capacidad de influencia y concienciación.

En el siguiente apartado veremos algunos de los diferentes modelos Organizativos y relacionales.

IV CUMPLIMIENTO IT. MARCO NORMATIVO E INTERNACIONAL.

La presente sección tiene como objetivo orientar al CISO en las leyes y normativas que deberá tener en consideración para ejercer su actividad. Es preciso reseñar que la normativa aplicable a su función dependerá del modelo organizativo de la empresa, naturaleza y sector de actividad.

Los siguientes apartados identifican las áreas de actividad sujetas a regulación o normativa. En cada una se incluye una introducción sobre cuál es su objeto y su ámbito de aplicación. No obstante, teniendo en cuenta que el marco legislativo y regulatorio se encuentran en constante evolución, se recomienda como buena práctica mantenerse actualizado en cada momento de la regulación de aplicación.

A este efecto, el Código de Derecho de la Ciberseguridad que publica el BOE: https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1 junto con el de Protección de Datos de Carácter Personal, son dos buenas fuentes para identificar y acceder a las versiones actualizadas de la legislación identificada.

Esquema Nacional de Seguridad

La LEY 11/2007, DE 22 DE JUNIO, DE ACCESO ELECTRÓNICO DE LOS CIUDADANOS A LOS SERVICIOS PÚBLICOS ESTABLECIÓ EL ESQUEMA NACIONAL DE SEGURIDAD[1] (en adelante ENS) que, aprobado mediante Real Decreto 3/2010[2], de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del REAL DECRETO 951/2015, DE 23 DE OCTUBRE[3]

1 Disponible en https://www.ccn.cni.es/images/stories/normas/pdf/ley_11_2007_ac- ceso_electronico_ciudadanos.pdf
2 Disponible en https://www.ccn-cert.cni.es/publico/ens/BOE-A-2010-1330.pdf
Así como la ley Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Recoge el ENS en su artículo 156 apartado 2. http://boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10566.pdf
3 Disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-11881f

El ENS tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en el ámbito de la Administración Electrónica en España. Establece los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

En el ENS se encuentra la primera referencia legislativa de la figura del responsable de seguridad de la información: "El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios." (RD_3/2010, 8 de enero 2010)

Para consideración del CISO, el ENS es de aplicación en la Administración General del Estado, Administraciones de las Comunidades Autónomas y Administraciones Locales y en las entidades de derecho público vinculadas a ellas. Las relaciones con las Administraciones también están sujetas al ENS.

En cualquier caso, aunque no sea de aplicación a las empresas privadas, constituye un marco de referencia útil para el establecimiento de una adecuada política de seguridad y es de especial interés para aquellas que trabajen próximas a la Administración y/o consideren la posibilidad de acreditarse para el manejo de información clasificada.

Protección de datos.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016[4] relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos o RGPD en lo sucesivo) y por el que se deroga la Directiva 95/46/CE.

LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN[5] DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (anteriormente denominado Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal).

La normativa de Protección de Datos afecta a todos los países de la Unión Europea y es de obligado cumplimiento para todas las empresas cuando recopilan, guardan, tratan, o gestionan datos personales de los ciudadanos de la Unión Europea. Tiene como objetivo devolver al ciudadano el control sobre cómo se utilizan sus datos personales. El Reglamento General de Protección de

4 Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf
5 Disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Datos (RGPD) es de ámbito europeo y, por tanto, aplicable en España don- de en la actualidad se está incorporando al marco legal nacional a través del nuevo proyecto de ley de Protección de Datos.

El incumplimiento del Reglamento General de Protección de Datos (RGPD) puede acarrear sanciones significativas.

La disciplina de Protección de Datos requiere del nombramiento de un delegado de protección de datos (DPD por sus siglas en castellano) o "Data Protection Officer" (DPO, por sus siglas en inglés) y sus funciones son compatibles con el rol del CISO o encontrarse en otra área de la empresa en función del modelo organizativo (por ejemplo, en Asesoría Jurídica). En cualquier caso, tiene implicaciones directas sobre la protección de los sistemas de información y, por tanto, el CISO siempre deberá tenerla en consideración.

Código Penal y Ley de Enjuiciamiento Criminal.

El CODIGO PENAL. LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, del Código Penal está en constante evolución, siendo su última actualización (en fecha de publicación de esta edición del Libro Blanco del CISO) de marzo de 2019.

El Código Penal es de atención por dos motivos diferentes:

— A partir de 2015, la persona puede ser responsable penalmente de los delitos que expresamente señala el Código Penal que pueden dar lugar a su responsabilidad. Por ello es habitual que las organizaciones desarrollen sistemas de Compliance para prevenir la infracción de normas de carácter penal y evitar eventuales sanciones que generen responsabilidad a la empresa. La participación del CISO es fundamental en estos sistemas de Compliance.

— Propiamente por la codificación de los "delitos informáticos", es decir, tanto aquellos en los que la infraestructura IT o la información son el objeto o bien jurídico protegido, como los delitos en los que la tecnología es el medio para su comisión (el llamado "Ciberdelito").

Así mismo, la Ley de Enjuiciamiento Criminal es de atención por contener en el Título VIII, Capítulo 4 y siguientes, información relevante para la obtención de evidencias y el despliegue de controles.

Directiva NIS (Network and Information Systems).

DIRECTIVA 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado[6] nivel común de seguridad de las redes y sistemas de información en la Unión y REAL DECRETO-LEY 12/2018[7], DE 7 DE SEPTIEMBRE, DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN que traspone la Directiva al ordenamiento jurídico español.

La directiva NIS tiene como objetivo lograr un elevado nivel común de se- guridad de las redes y sistemas de información dentro de la Unión Europea. Establece condiciones de seguridad para empresas y organismos que pro- porcionan servicios esenciales enmarcadas en los sectores estratégicos de la administración, espacio, industria nuclear, industria química, investigación, agua, energía, salud, tecnologías de la información, transporte, alimentación y sistema financiero y tributario. Regula la seguridad de redes y sistemas de información utilizados para la provisión de los citados servicios esenciales y servicios digitales (comercio electrónico, motores de búsqueda y grandes ser- vicios de computación en la nube).

La directiva NIS es de ámbito europeo y, por tanto, directamente aplicable en España donde se ha incorporado al marco legal nacional. Al igual que el resto de directivas comunitarias, se ha de transponer en leyes nacionales en todos los países no pudiendo éstas en ningún caso contravenir sus disposiciones.

El legislador nacional, en la transposición de la Directiva, ha adaptado a la realidad nacional la Directiva con la identificación de las diferentes autoridades control y CERTs gubernamentales para sus ámbitos naturales de actuación.

El Real-Decreto Ley será ratificado a Ley para que pueda desarrollarse su reglamente en el que se incidirá en las medidas necesarias para la debida protección de los sistemas de información y comunicación de los servicios esenciales y digitales.

Es importante destacar que el Real Decreto-Ley 12/2018 dice en su artículo 16.3: "Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella. Sus funciones específicas serán las previstas reglamentariamente."

6 Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CE- LEX:32016L1148&from=ES
7 Disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

Ley de Seguridad Privada.

La Ley 5/2014, DE 4 DE ABRIL,[8] de Seguridad Privada tiene por objeto regular la realización y la prestación de actividades y servicios de seguridad privada que, desarrollados por éstos, son contratados, por personas físicas o jurídicas, públicas o privadas, para la protección de personas y bienes. Igualmente regula las investigaciones privadas que se efectúen sobre aquéllas o éstos.

Recoge en su artículo 36 las funciones de la figura del Director de seguridad para la organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles entre otras.

Deberá existir un modelo de relación y colaboración constante entre el CISO y el CSO tanto desde un punto de vista de gestión de incidentes como para elevar la función de seguridad a los órganos de dirección de las organizaciones. El objetivo de protección es común y se deberán buscar al máximo las sinergias dentro de la organización.

Hay varios aspectos que el CISO deberá tener en cuenta en dicha relación:

1) En caso de incidentes en los que pudieran detectarse infracciones pe- nales, administrativas, laborales, tributarias, etc. existe la obligación de in- formar a las Autoridades de Control. El CISO deberá informar al Director de Seguridad de tales eventos siendo éste el responsable de efectuar la comunicación.

2) En caso de incidentes que pudieran implicar compromiso de información sensible de la empresa, gubernamental, control de exportación o de datos personales deberán tomarse acciones de comunicación a diferentes como se indica en los apartados pertinentes (a continuación, dentro de esta misma sección).

3) En caso de investigaciones, ya sea por incidentes relacionados con ma- las prácticas, acciones deliberadas, ciberataques, etc. el CISO deberá ase- gurarse que existen políticas refrendadas por Asesoría Jurídica que avalen la legitimidad de la intervención de los activos informáticos de la empre- sa incluyéndose la intercepción de comunicaciones, inspección de orde- nadores de empleados, inspección de correo electrónico para garantizar que dichas investigaciones sean legítimas.

8 Disponible en https://www.boe.es/buscar/pdf/2014/BOE-A-2014-3649-consolidado. pdf

En la actualidad, se encuentra en desarrollo el nuevo reglamento de seguridad privada dónde se prevé la inclusión expresa de referencias a las actividades de Seguridad Informática y Ciberseguridad. [9]

Ley de Protección e Infraestructuras Críticas.

En España la LEY 8/2011, DE 28 DE ABRIL, estableció por primera vez las medidas para la protección de las infraestructuras críticas (más conocida ya como Ley PIC o simplemente LPIC) junto con el reglamento que la desarrolla (Real Decreto 704/2011, de 20 de mayo).

La LPIC tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas.

Para cumplir con ese objetivo se impulsa la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, frente a ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.

En la Ley y en su posterior RD no se menciona la figura del responsable de Seguridad de la Información, si bien posteriormente por instrucción de la Secretaría de Estado de Seguridad se solicita que los Operadores de Infraes- tructuras Críticas deben designar y comunicar tanto un CISO, como un CISO suplente.

El Plan Nacional de Protección de Infraestructuras críticas establece la necesidad de crear la mesa de Ciberseguridad de Infraestructuras críticas, en la que tienen representación los CISOS de todos los sectores mediante un representante elegido por cada sector.

Esta mesa se reune para tratar los temas de interés relacionados con la ciberseguridad.

Secretos empresariales.

La recientemente publicada Ley 1/2019, de 20 de febrero, de Secretos Empresariales tiene por objeto la protección de los mismos.

9 Disponible en https://www.policia.es/actualidad/pdf/texto_borrador_seg_pri.pdf

La ley considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero que sea secreto, en el sentido que:

— no es generalmente conocido ni fácilmente accesible,
— tiene un valor empresarial real o potencial, precisamente por ser secreto, y
— es objeto de la aplicación medidas razonables para mantenerlo secreto.

Sector Financiero y banca

Es el sector financiero y bancario uno de los sectores más regulados, y no solo en los ámbitos más específicos de su propia actividad, sino también en otros ámbitos de estas entidades, como son el tecnológico o el de seguridad. Motivo por el cual los CISOs de estas entidades dedican un buen número de recursos y esfuerzos al cumplimiento regulatorio.

El REAL DECRETO-LEY 19/2018, DE 23 DE NOVIEMBRE, de servicios de pago y otras medidas urgentes en materia financiera, que tiene por objeto, tras la consolidación de la zona única de pagos de la Unión Europea, adaptar la regulación a los nuevos cambios tecnológicos.

Este RD recoge las disposiciones de la DIRECTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO Y DEL CONSEJO[10], DE 25 DE NOVIEMBRE DE 2015, sobre servicios de pago en el mercado interior, (PSD2), y del REGLAMENTO DELEGADO (UE) 2018/389 DE LA COMISIÓN DE 27 DE NOVIEMBRE DE 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros.

Los organismos reguladores, el Banco Central Europeo y los bancos centrales nacionales, establecen también una amplio marco regulatorio, a través de la European Banking Authority (EBA), sobre la actividad en el ámbito tecnológico de las entidades, y desarrollan guías para la gestión de riesgos tecnológicos, la externalización, los proveedores cloud,

Directrices sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES), EBA/GL/2017/05.

10 Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CE- LEX:32015L2366&from=EN

Recomendaciones sobre la externalización de servicios a proveedores de servicios en la nube, EBA/REC/2017/03.

Guidelines on outsourcing, publicadas por el Comitttee of European Banking Supervisors (CEBS), en el 2006.

EBA Guidelines on outsourcing arrangements EBA/GL/2019/02, que será de obligado cumplimiento a partir del 30 de septiembre de 2019, reemplazando a las dos anteriores.

Existen además normas de consorcios privados que obligan al cumplimiento de un marco normativo de seguridad para aquellas entidades financieras que participan en ellos o son miembros de los mismos. Los más relevantes son el de PCI-DSS y el de SWIFT.

El estándar de Seguridad de Datos para la Industria de Tarjeta de Pago, PCI-DSS, que en la actualidad está en su versión 3.2.1.[11] El SWIFT Customer Security Controls Framework, cuya versión actual es la v2019.

Sector Juego.

Las empresas del Sector Juego (juego online) están sujetas a las siguientes leyes y normativas:

- Ley 13/2011, de 27 de mayo, de regulación del Juego[12] y RD de desarrollo de la Ley del Juego y su desarrollo conforme al Real Decreto 1613/2011, de 14 de noviembre.[13]

- Órdenes ministeriales de afectación (Orden EHA/2528/2011, de 20 de septiembre, por la que se establecen los requisitos y el procedimiento de designación de entidades independientes que realicen las certificaciones de evaluación del software de juegos y de seguridad de operadores de juegos).[14]

- Resoluciones Técnicas (Resolución de 6 de octubre de 2014, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición por la que se desarrollan las especificaciones técnicas de juego, trazabilidad y seguridad que deben cumplir los sistemas técnicos de juego de carácter no reservado objeto de licencias otorgadas al amparo de la Ley 13/2011, de 27 de mayo, de regulación del juego.[15])

12 Disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2011-9280
13 Disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2011-17835
14 Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2011-15092
15 Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2014-10302

Sector Defensa

Las empresas del Sector Defensa que manejan información nacional clasificada están sujetas a las siguientes leyes y normativas:

- Ley 9/1968, de 5 de abril Secretos Oficiales.[16]

- Política de Seguridad de la Información del Ministerio de Defensa. Para las empresas es aplicable el área de seguridad de la información de la "Seguridad de la Información en poder de las Empresas (SEGINFOEMP[17])". Las normas e instrucciones SEGINFOEMP[18] especifi-an las medidas de protección dirigidas a las empresas y aplicables por ellas, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información del Ministerio manejada por éstas, como consecuencia de su participación en pro- gramas, proyectos o contratos del Ministerio.

- Normas de la Autoridad Nacional para la Protección de la Información Clasificada (Oficina Nacional de Seguridad del CNI).[19]

- Normativa y guías CCN-STIC del Centro Criptológico Nacional. Con- tienen, además de recomendaciones para la seguridad, el procedimiento y requerimientos de seguridad para acreditación de sistemas para el manejo de información clasificada.[20]

- Normativa de Seguridad OTAN (North Atlantic Treaty Organization – NATO). De obligado cumplimiento para la ejecución de programas OTAN clasificados (por ejemplo, Eurofighter y NH90).[21]

- Normativa OCCAR (Organisation Conjointe de Coopération en ma- tière d'ARmement). De obligado cumplimiento para la ejecución de programas OCCAR clasificados (por ejemplo, A400M, MMF, MA- LE-RPAS y Tiger).

16 Disponible en https://www.boe.es/buscar/pdf/1968/BOE-A-1968-444-consolidado. pdf
17 Orden Ministerial 76/2006, de 19 de mayo, "Seguridad de la Información en poder de las Empresas (SEGINFOEMP)" http://www.belt.es/legislacion/vigente/Seg_inf/Seg_inf/esta- tal/290506_OM_Seg_Informacion.pdf http://www.defensa.gob.es/portalservicios/servicios/industriade-fen- sa/seginfoemp/
18 Instrucción 52/2013, de 17 de junio, del Secretario de Estado de Defensa, por la que se aprueban las Normas para la Seguridad de la Información del Ministerio de Defensa en poder de las empresas. http://www.defensa.gob.es/Galerias/portalservicios/seginfoemp/Ins- truccion_52_2013.pdf y Resolución 320/14546/13, de 23 de septiembre, del Director General de Armamento y Material, por la que se aprueban los procedimientos para la implementación de la Instrucción 52/2013, de 17 de junio, del Secre- tario de Estado de Defensa, por la que se aprueban las normas para la seguridad de la información del Ministerio de Defensa en poder de las empresas. http://www.defensa.gob.es/Galerias/portalservicios/seginfoemp/Re- solucion_DIGAM_Procedimientos_de_SEGINFOEMP.pdf
19 Disponible en https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_ Normas_de_la_Autoridad.pdf
20 Información pública disponible en https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html
21 De especial relevancia Documento C-M(2002)49 disponible en https://www.cni.es/comun/recursos/descargas/DOCUMENTO_21_-_ Security_within_NATO_-_C-M49-COR1-12.pdf y sus directivas AC/35 asociadas, disponibles en http://www.dksi.bg/

- Normativa ESA (European Space Agency) De obligado cumplimiento para la ejecución de programas clasificados de la ESA.

- Normativa LoI/FA EDIR (Letter of Intent / Framework Agreement for European Defence Industrial Restructuration). El tratado FA EDIR se firmó el 27 de julio de 2000 en Farnborough (Reino Unido) entre Francia, Alemania, Italia, España, Suecia y Reino Unido. Su objetivo es facilitar la reestructuración de la industria europea de defensa, con el fin de promover una base tecnológica e industrial más potente y competitiva.

No todas estas normas son de dominio público por lo que es recomendable, en el caso de trabajar con información clasificada, el contacto directo con los distintos organismos públicos.

Export Control.

La disciplina de Export Control puede o no ser competencia del CISO en función del modelo organizativo de la empresa. Dicha función puede ser responsabilidad de otras áreas (por ejemplo, Asesoría Jurídica). Debe existir la figura o rol de oficial de control de exportación o "Export Control Officer", responsable del cumplimiento normativo. En cualquier caso, tiene implicaciones directas sobre la protección de los sistemas de información. y, por tanto, el CISO debe siempre tenerla en consideración.

Las normativas de control de exportación tienen carácter nacional (Estados Unidos, Reino Unido, España, etc.) y tienen como objetivo proteger que la tecnología exportada a otros países y empresas u organismos no pueda ser reexportada a terceros sin permiso del creador. Algunas de ellas como la estadounidense ITAR son muy restrictivas, implican controles de nacionalidades del personal y pueden conllevar significativas sanciones en caso de incumplimiento. Algunas normativas de control de Exportación son:

- Normativa US ITAR (Part 130) – International Traffic-In Arms Regula- tions. Regula la exportación de material militar.[25]

- Normativa US EAR (Export Administration Regulation – regula la ex- portación de material de doble uso (militar/civil)[26]

22 Disponible en http://www.occar.int/occar-rules
23 Disponible en https://download.esa.int/docs/eso/esa-reg-004e.pdf
24 Disponible en https://www.gov.uk/guidance/letter-of-intent-restructuring-the-euro- pean-defence-industry https://www.gov.uk/government/publications/letter-of-intent-sub-commi- ttee-3
25 Disponible en https://www.pmddtc.state.gov/regulations_laws/documents/official_ itar/2016/ITAR_Part_130.pdf
26 Disponible en https://www.bis.doc.gov/index.php/regulations/export-administra- tion-regulations-ear

- Real Decreto 679/2014, de 1 de agosto, de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.[27]

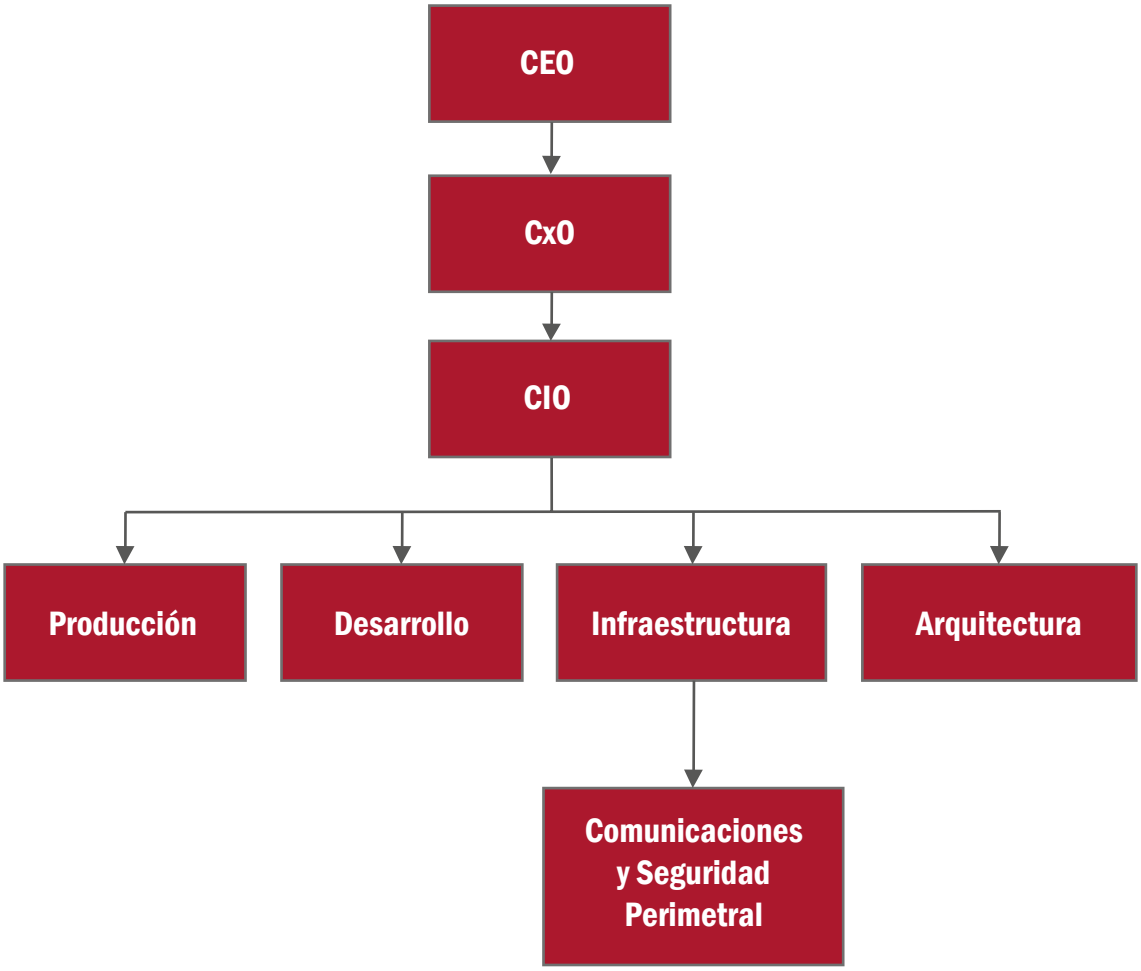
- Normas de Export Control en la Unión Europea u otros países que dispongan de legislación o normativa en esta materia.

27 Disponible en https://www.boe.es/boe/dias/2014/08/26/pdfs/BOE-A-2014-8926. pdf

V MODELOS ORGANIZATIVOS Y RELACIONALES

V.1.- Modelo 1: El CISO dentro de una subárea de tecnología.

En este modelo organizativo el CISO se encuentra en el departamento de tecnología, en el área de infraestructura que según la empresa puede llamarse producción, explotación, etc. Este modelo se presenta en compañías con una madurez tal que considera la seguridad de la información intrínseca a las funciones de tecnología. La figura del CISO, en este modelo, se aproxima quizá al de un administrador de los sistemas de seguridad.



Ventajas

- Muy cercano de la operativa.
- Cercanía con el personal de tecnología.

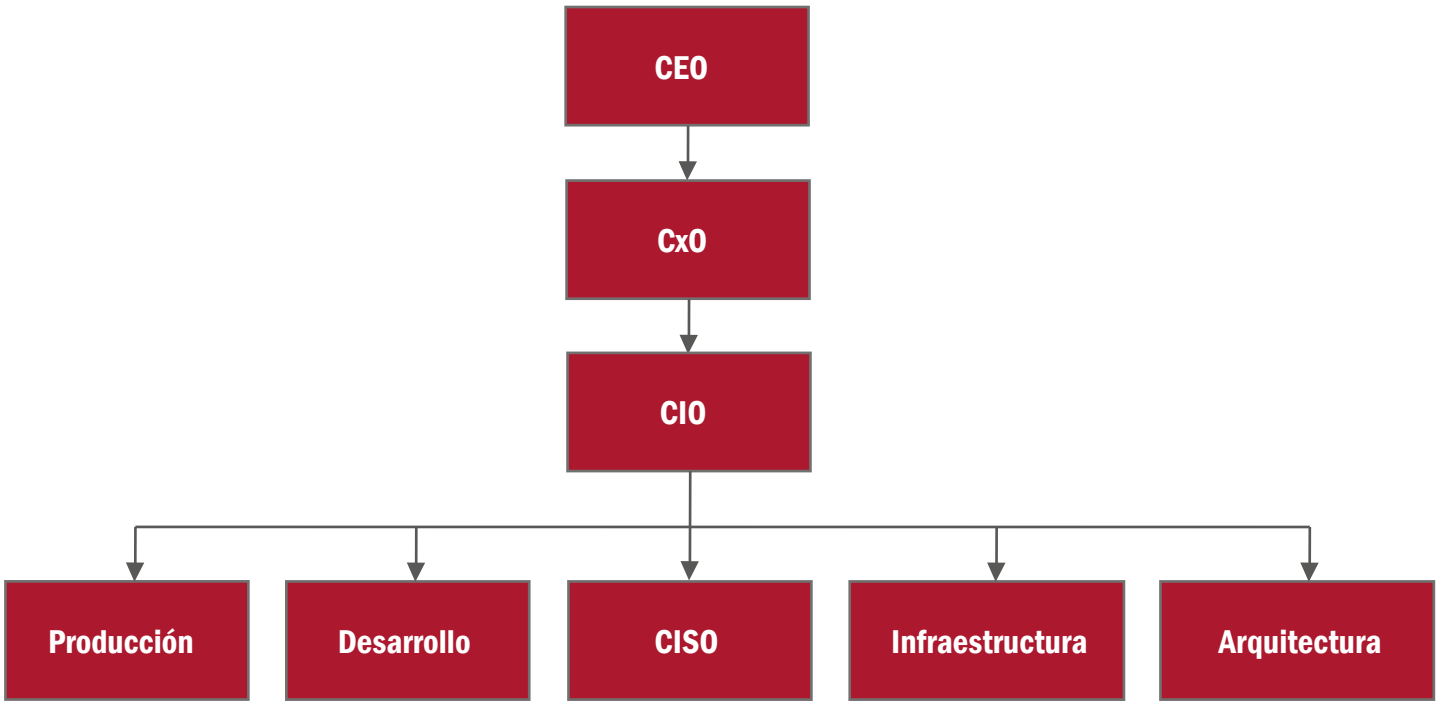
Inconvenientes

- Menor capacidad de decisión.
- Menor visibilidad.
- Posible conflicto de intereses.
- Ámbito de competencia reducido a la infraestructura.
- Presupuesto dependiente del reparto interno al departamento de tecnología.

V.2.- Modelo 2: El CISO en un área específica de seguridad.

El CISO cuenta con su propio departamento, es decir existe dentro del organigrama el departamento de seguridad de la información, pero se adscribe a la misma estructura jerárquica dentro del departamento de tecnología.

Dentro de este modelo pueden existir variantes teniendo en cuenta las funciones, por ejemplo, seguridad de la información puede ser un área de definición y control y las otras funciones de ejecución, mantenimiento y explotación estarían repartidas por el resto de los departamentos.



Ventajas

- Muy cercano de la operativa.
- Cercanía con el personal de tecnología.
- Toma de decisión a nivel tecnológico.

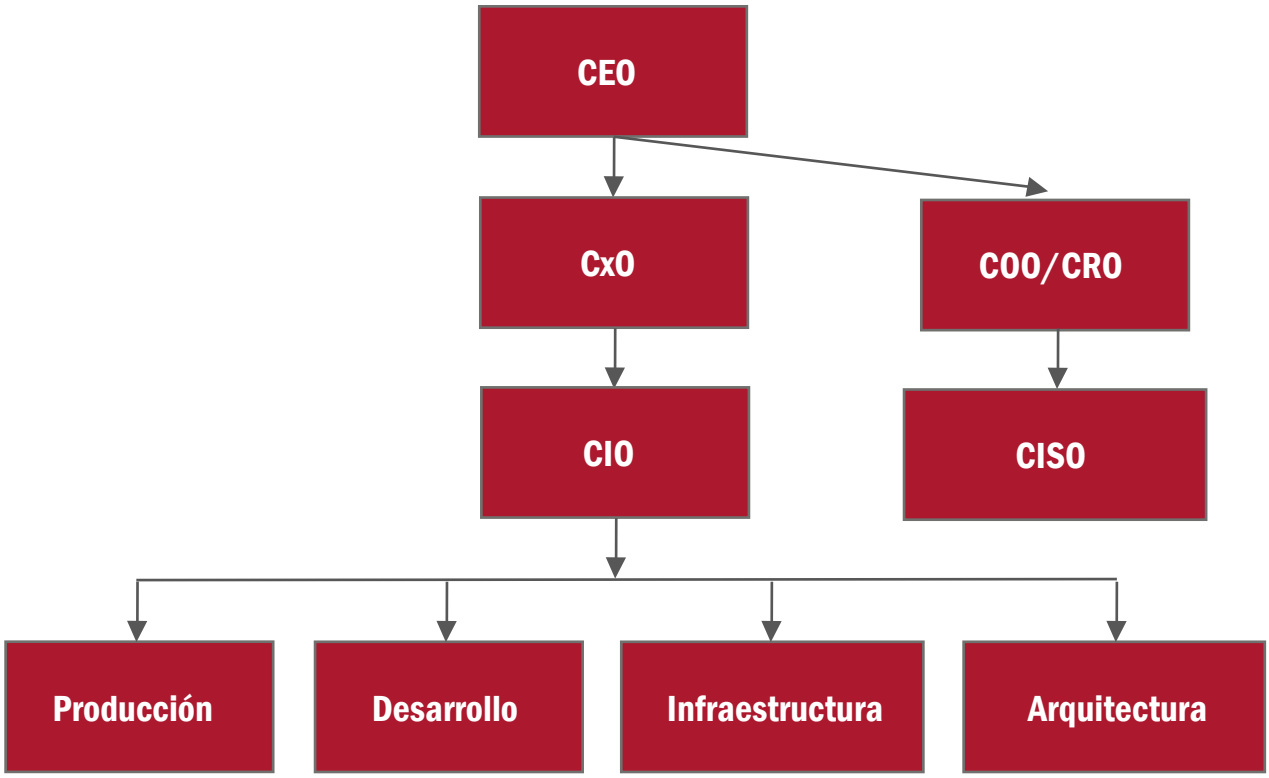
Inconvenientes

- Menor visibilidad.
- Posible conflicto de intereses.
- Ámbito de competencia reducido a la función de tecnología.
- Presupuesto dependiente del reparto interno al departamento de tecnología.

V.3.- Modelo 3: Seguridad de la información fuera de Tecnología.

En este modelo el CISO no depende de Tecnología y reporta normalmente al COO (Chief Operating Officer) o al CRO (Chief Risk Officer), pero como bien indica la ilustración puede ser cualquier rol ejecutivo de una organización (CxO). Funciona como un "staff" sobre todos los aspectos concernientes a la seguridad de la información desde el punto de vista de riesgos o amenazas a dicha información.

Este modelo está desplegado en organizaciones que apuestan por el CISO como un nivel directivo pero sin llegar al comité de dirección ya que dicha representación está definida en el CRO.



Ventajas

- Mayor capacidad de decisión.
- Mayor visibilidad.
- No hay conflicto de intereses.
- Asignación presupuestaria independiente.
- Capacidad de interacción con todas las demás áreas de staff.

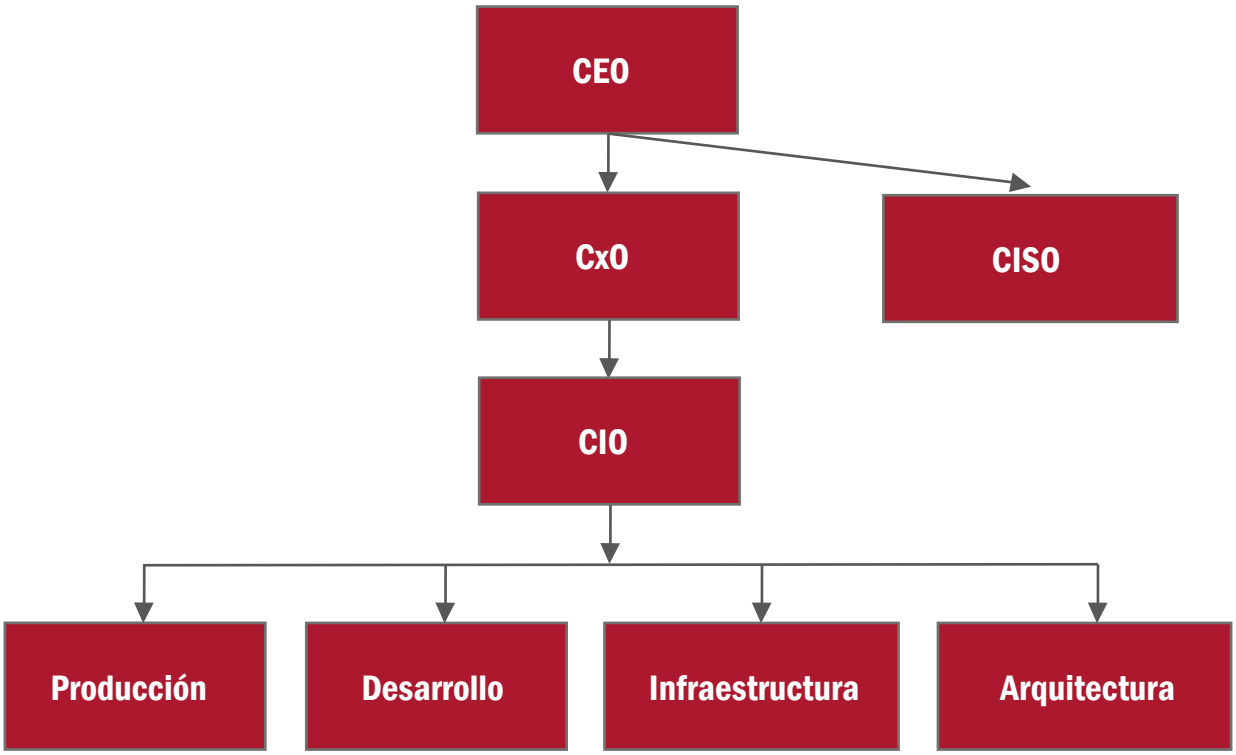
Inconvenientes

- Lejos de la operativa.
- Lejanía con el personal de tecnología.
- Posible solapamiento con áreas de control del riesgo.

IV.4.- Modelo 4: El CISO dentro de la alta dirección.

Para este modelo el CISO no sólo está fuera de Tecnología, sino que es con- si- derado un ejecutivo de alto nivel y, por tanto, pertenece al comité de di- rección. Suele reportar al Director General, presidente o consejero delegado (depende la de organización). Es un modelo más evolucionado y tiene cabida en empresas y organizaciones que consideran la seguridad de la información necesaria e imprescindible para el desarrollo del negocio.

Las políticas y procedimientos de seguridad definidos por este departamento directivo se ejecutan y operan desde cada área de la empresa en conformidad con el CIO.



Ventajas

- Mayor capacidad de decisión.
- Mayor visibilidad.
- No hay conflicto de intereses.
- Asignación presupuestaria independiente.
- Capacidad de interacción con todas las demás áreas de staff

Inconvenientes

- Lejos de la operativa.
- Lejanía con el personal de tecnología.
- Se requiere de más áreas que operen la Seguridad Informática.

V.5.- Modelo 5: Modelo Organizativo.

Además de estos modelos el CISO puede formar parte de un modelo de organización que dependa de la estrategia e incluso de condiciones legales o de un órgano gestor recomendado por la regulación. Hay sin duda una gran tendencia a modelizar la gestión de la seguridad en lo que se llama "Las 3 líneas de defensa" dentro de una organización. En la primera línea de defensa estará la seguridad operativa, en la que se encontrará el CISO si en su organización no hay segregación de funciones entre la seguridad operativa y el CISO.

En la segunda línea de defensa se encontrará el CISO (haya o no segregación de funciones en seguridad de la información), así como como el área de cumplimiento y en la tercera línea, generalmente, y por requisitos de segregación de funciones, corresponde al Departamento de Auditoria Interna y Auditoría externa.

En este modelo el CISO se configura como un gestor de las 2 primeras líneas de defensa y que se apoyan en las buenas prácticas para gestionar los riesgos de forma global en la organización.

A través de estas 3 líneas de defensa se lleva a cabo un gobierno de la seguridad basado en la segregación del control y de las funciones sin conflicto de intereses. En la primera línea se ejecutan las acciones más operativas y más cercanas al negocio, al día a día. Desde la segunda línea se realizan los con- troles, la monitorización y el seguimiento de las acciones de la primera línea con respecto al riesgo de la organización y, por último, la tercera línea verifica lo que se ha realizado tanto en la primera como la segunda línea para que sean independientes, con funciones distintas y buscando el mayor beneficio referido a la gestión de los riesgos globales.

Dentro de este modelo organizativo el CISO gestiona de forma unificada la seguridad de la información. En la mayoría de las empresas e instituciones esta solución partió desde la primera línea de defensa y, por tanto, allí donde se ubica al CISO. En otras organizaciones, sin embargo, se encuentra en la segunda línea y en la primera línea existe un responsable de seguridad tecno- lógica (Chief Technology Security Officer), un LISO (Local Information Security Officer) e incluso un BISO (Bussiness Information Security Officer).

En el caso de España este modelo es de aplicación reciente y en algunas organizaciones el CISO aunque esté ubicado en Tecnología y, por tanto, como primera línea de defensa, en realidad realiza bajo su "paraguas" funciones que son tanto de la primera como de la segunda, a lo que en el sector se le llama la línea 1 punto 5 (1,5).

Entre estas dos líneas se encontrarían aquellas tareas asignadas al CISO relacionadas con la gestión y aseguramiento de la Privacidad.

Tras un análisis de estos modelos, lo más importante es determinar las tareas y características de la figura del CISO sin estar influido por la posición del CISO dentro de la organización o a quién reporte en la misma.

V.6.- Características de un CISO.

El CISO es una posición a nivel ejecutivo cuya misión es proporcionar al órga- no de gobierno de una compañía (normalmente comité de dirección) apoyo y asesoramiento experto en materia de seguridad de la información y protec- ción de activos. A diferencia de un director de seguridad de la información, el CISO tiene responsabilidad global sobre la gestión de la seguridad de la infor- mación y además es la figura que representa la seguridad de la información en el comité ejecutivo de la compañía.

Para cumplir con los objetivos de mantener y desarrollar el sistema de ges- tión de seguridad de la información y tener capacidad táctica para desarrollar dicho programa con éxito, el CISO necesita ser parte del equipo de gestión senior de la compañía, no simplemente un gestor técnico.

En esa línea hay tres claves que facilitan al CISO el éxito:

- Independencia: Debe de ser independiente de influencias o presiones de aquellos involucrados en el día a día. Por ello no debe ser juez y parte en temas tecnológicos tanto desde el punto de vista operativo como de inversión.

- Empoderamiento: Debe tener el poder dentro de la organización, con el apoyo y supervisión del órgano ejecutivo (ej. Comité de Seguridad) para recomendar, implantar procesos, salvaguardas y medidas de formación y concienciación relacionadas con la seguridad de la información.

- Posición organizativa: La posición en una organización debe ser aquella que facilite su función como capacitador de buenas prácticas en seguridad, no limitado al entorno TI sino también a problemáticas de seguridad de la información y del negocio.

V.7.- ¿A quién debe reportar el CISO?

Como hemos dicho antes no hay modelo mejor que otro, o modelo perfecto, ya que si así fuese todo el mundo utilizaría el mismo.

A continuación, se exponen distintos estudios que avalan estos principios:

En 2015 El GTISC (Georgia Tech Information Security Center) indicaba que la segregación de responsabilidades continuaba siendo un problema en las lí- neas de reporte CISO/CIO, tal como se refleja en el siguiente informe:

https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/ en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf

Líneas de reporte

•40% al CIO.
•22% al CEO.
•8% al CFO.
•6% Consejo Administración.

En 2018 en el informe de la consultoría PWC "Global State of Information Security Survey" https://www.pwc.com/us/en/services/consulting/cyberse- curity/library/information-security-survey.html se evidencia una tendencia a separar el rol del CISO:

- 40% CISOs/CSOs reportan a CEO
- 27% a directores del consejo
- 24% al CIO
- 17% al CSO
- 15% al CPO (Chief Privacy Officer)

Sin embargo, el informe de Ponemon del año 2017 "The Evolving Role of CISOs and their importance to the business" (https://interact.f5.com/rs/653- SMC-783/images/RPRT-SEC-1167223548-global-ciso-benchmarkUPDATED. pdf) indica que:

- 60% de los CISOs tienen canal directo con CEO en caso de incidentes serios.
- 50% siguen reportando al CIO.
- 9% reportan al CTO.
- 9% reportan al CFO.
- 8% al Consejo.
- 6% al COO.
- 6% al Risk Manager Leader.

La encuesta "El Rol de CISO" elaborada en ISMS Forum Spain entre los CISOS de empresas españolas el primer trimestre de 2019 indica que, según sectores el Reporting del CISO se distribuye del siguiente modo:

- 57,5% reportan al CIO.
- 20% al CTO
- 7,5% a un Comité Interdepartamental
- 7,5 % a Otros órganos corporativos
- 2,5% al CSO/COO
- 2,5 % al CFO

En la misma encuesta los propios CISOS mayoritariamente -47,5%- opinan que deberían reportar al CEO, a un Comité de Dirección interdepartamental (20%) o al CIO un 12,5%. El 20% restante se repartiría entre alguna de estas aréas: Negocio, Jurídico, Riesgo, CSo y un significativos 2,5 % de NS/NC.

En cuanto a qué nivel están los responsables a los que Reportan los CISOS, según la encuesta de ISMS Forum:

- 70% está un nivel por encima
- 25% está dos niveles por encima
- 5% están más de dos niveles por encima

De estos estudios cabe destacar que el CISO aumenta de forma progresiva su interacción con el CEO, muy especialmente en caso de incidentes y se tiende a incrementar la segregación de funciones entre CISO/CIO/CTO.

Al mismo tiempo se deben resaltar los siguientes epígrafes:

Expectativas

— Debe ser una posición suficientemente independiente para mantener una visión objetiva del nivel de exposición a los riesgos.

— Debe tener cercanía al primer nivel de la compañía, su función es identificar y proteger riesgos asociados al uso de la información, pero para ello precisa que la estrategia de la compañía le priorice la criticidad de los activos de información y cuáles son los impactos en la organización.

Realidades

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.

V.8.- Tipos de empresas.

Cuando nos referimos a complejidad de la empresa cabe distinguir entre Organizaciones complejas y simples:

Organizaciones complejas, aquellas que tienen uno o varios de estos factores:

- Dispersión geográfica
- Dispersión funcional
- Dispersión
- Estructuras societarias
- Alto volumen de transacciones de negocio

En este segmento de Organizaciones complejas normalmente hablamos de corporaciones y, en estos casos, deben considerarse, como mínimo, las siguientes casuísticas de acuerdo con el nivel de centralización del grupo empresarial:

- En empresas en las que la gestión se encuentra más centralizada y las sociedades filiales se centran en cuestiones operativas, el rol del CISO corporativo tendrá atribuciones muy superiores a un grupo tipo holding y, por tanto, se focalizará en mantener la visión estratégica, emitir políti- cas de grupo y supervisar el despliegue de la función en los negocios.

- En grupos con líneas de negocio diversificadas es factible que surja la figura del BISO (Business Information Security Officer).

- En corporaciones internacionales se generará la obligatoriedad de cumplir las respectivas legislaciones locales. En estos casos es factible que surja la figura del LISO (Local Information Security Officer).

A efectos de este informe el resto de las empresas se consideran organizaciones simples. En estos casos, salvo empresas que pertenezcan a sectores de actividad muy regulados, es práctica habitual que los roles se adapten a las competencias y habilidades del equipo directivo existente, pues suelen concentrar responsabilidades con cierto grado de heterogeneidad.

V.9.- Recomendaciones.

Los riesgos cibernéticos evolucionan continuamente y aumentan su impacto en los negocios, es por ello que la correcta designación organizativa del CISO, sus responsabilidades e interrelaciones son una asignatura clave para la alta dirección de las empresas.

Una mala ubicación organizativa del CISO afectará negativamente a su capacidad de identificar e influir para la mejora de capacidades de protección de la ciberseguridad y la privacidad de la información.

Independientemente de las figuras de CISO y CSO (Chief Security Officer) y si deben estar juntos o no, es importante destacar la importancia de tener una estrategia de Seguridad Integral que logre una adecuada y coordinada cober- tura de riesgos de los siguientes ámbitos:

- Riesgos Tecnológicos: Son los que debe cubrir el rol del CISO aquí planteado (ciberataques, virus, ransomware, etc...).

- Riesgos Físicos: Comprende a sabotajes, robos, vandalismo, movilizaciones y, en general, a cualquier evento que pueda afectar a la seguridad de las personas y de las infraestructuras; normalmente estos aspectos dependen del Director de Seguridad pero, como estas amenazas pue- den realizarse por medios tecnológicos, podrían recaer en el futuro por una misma persona o tratarse en un mismo departamento de "Seguri- dad Global".

- Riesgos Operacionales: Una estrategia de respuesta a eventos disruptivos que puedan comprometer los objetivos de la compañía (p.ej. fallo en un CPD o línea de producción de una fábrica); aunque actualmente son independientes del CISO, en un futuro no muy lejano y por los mismos motivos del caso anterior, podrían englobarse en el departamento de la "Seguridad Global".

VI PERFIL DEL CISO

V.I. FORMACIÓN Y CAPACITACIÓN.

En el capítulo II, apartado 1 describiendo las funciones del director de Segu- ridad de la Información se hace referencia los roles de CISO (figura el plano de la autoridad formal) y CTSO (responsable tecnológico de la seguridad de la información). Si bien en el aspecto directivo ambas funciones, que pueden ser o no desempeñadas por la misma persona, requieren un perfil con similares cualidades, esto no es extrapolable al plano operativo puesto que las especialidades son muy diferentes.

En el aspecto de autoridad formal como ya se ha comentado en el punto precedente el CISO debe conocer el negocio (seniority), la legislación aplicable y los riesgos de seguridad informática y ciberseguridad (estar al día de amenazas y tendencias) porque no podría tomar decisiones con criterio de otro modo.

El CISO debe conocer el marco regulatorio y legal aplicable a la actividad de la empresa (véase capítulo I, apartado 2) y debe conocer metodologías de análisis de riesgos (MAGERIT, NIST, CRAMM…), los estándares para la seguridad de la información (ISO 27XXX, entre otras), así como la Estrategia Nacional de Ciberseguridad, que deberá orientar y trasponer a la estrategia y políticas de seguridad de la información de la empresa, que son competencia suya. Igualmente lo será la certificación si es requisito para la empresa y cualquier acreditación para manejo de información conforme a las normativas mencionadas (Véase I.2).

Como recomendación, el CISO debería disponer de la habilitación que exige la Ley 5/2014, de 4 de abril, de Seguridad Privada al Director de Seguridad ya que le dotará de una visión integral de la seguridad, e incluso es posible su intervención en incidentes actividades relacionadas con los campos que legislativamente requieren de dicha habilitación. Obsérvese que la función de Director de Seguridad también puede recaer en el CISO, en cuyo caso la habilitación es obligatoria).

Es esencial que el CISO disponga de una adecuada formación académica, conocimiento de idiomas, capacidad de interrelación con homólogos de otras empresas, asistencia a foros y eventos de ciberseguridad, etc. Cualquier otra

formación o capacitación profesional complementaria es interesante para estar actualizado incluso a nivel técnico, aunque si existe la figura del CTSO, en caso debería ser asesorado por éste y su equipo técnico especializado.

Como parte de su capacitación, debe participar en ciberejercicios y simulaciones de crisis, pues obviamente sólo se está preparado en aquello que se entrena.

Si CISO y CTSO convergen en la misma persona el espectro de conocimiento del CISO es más amplio si bien la ausencia de segregación de funciones en materia de seguridad puede dificultarle la independencia a la hora de establecer el marco y supervisar su ejecución.

Al igual que si CISO y DPD convergen en la misma persona, las ventajas son múltiples para la Organización (unicidad de objetivos, refuerzo de la protección y la supervisión), pero en dicho caso deberá esforzarse en establecer las debidas precauciones para no incurrir, a ojos de terceros, en conflicto de intereses.

En cuanto al citado rol de CTSO (sea o no parte de los cometidos que le aplican al CISO), siendo el perfil mucho más técnico, es fundamental tener las siguientes capacitaciones:

- Formación académica: preferentemente ingenieros de telecomunicación o informáticos con Máster de especialización en Gobierno de la Seguridad de la Información o MBA.

- Formación en idiomas: el inglés es un elemento de trabajo casi impres- cindible porque tanto publicaciones como foros, eventos, etc. se desa- rrollan con frecuencia en inglés.

- Certificaciones profesionales (algunos ejemplos):

    - CCSP - Certified Cyber Security Professional. Certificación otorgada por ISMS Forum.

    - CDPD – Certificación de Delegado de Protección de Datos. Certifi- cación homologada otorgada por ISMS Forum bajo el Esquema de Certificación de la Agencia Española de Protección de Datos.

    - CDPP - Certified Data Privacy Professional. Certificación otorgada por ISMS Forum.

- CISA - Certified Information Systems Auditor (CISA). Certificación para auditores de ISACA (Information Systems Audit and Control As- sociation - Asociación de Control y Auditoría de Sistemas de Infor- mación).

- CISM - Certified Information Security Manager. Certificación para gestores de seguridad de la información de ISACA (Information Systems Audit and Control Association - Asociación de Control y Auditoría de Sistemas de Información).

- CISSP - Certified Information Systems Security Professional. Certificación otorgada por (ISC)^2 (International Information Systems Security Certification Consortium, Inc).

- CRISC - Certified in Risk and Information Systems Control. Certificación para gestores de control de riesgos en sistemas de información de ISACA (Information Systems Audit and Control Association - Asociación de Control y Auditoría de Sistemas de Información).

- SSCP - Systems Security Certified Practitioner. Certificación en seguridad informática otorgada por (ISC)^2 (International Information Systems Security Certification Consortium, Inc).

- Existen otras muchas certificaciones complementarias que pueden ser de interés:

  - CIA (Certified Internal Auditor) de IIA (Institute of Internal Auditors)
  - CISMP (Information Security Management Principles)
  - CGEIT (Certified in the Governance of Enterprise IT) CompTIA+ (Advanced Security Practitioner) Certified CISO (CCISO)
  - Certificaciones de CISCO:
  - CCNA Security
  - CISCO Certified Network Professional Security Certificaciones de
  - SANS Institute Certificaciones de Offensive Security Certificaciones GIAC
  - Certificaciones CERT
  - Certified Computer Security Incident Handler Certification

V.II. SOFT SKILLS

El rol de CISO implica disponer de habilidades adicionales o paralelas, conocidas como "soft skills" que le permitan desempeñar una función compleja, muchas veces no bien definidas y que requiere de un gran equilibrio entre la autoritad, el reconocimiento del rol y su valor por parte de los demás; y la potestad, la asignación y asunción de tareas y responsabilidades.

Conjugar ambos, a veces aparentemente contrapuestos, requiere a este perfil un compendio de conocimientos adicionales, a veces incluso profundos, de otras disciplinas técnicas o humanistas, y al mismo tiempo de capacidades personales y emocionales. Este enjuague de habilidades adicionales confor- mará la valía del profesional, y se debe prestar atención.

V.II.1.- Capacitación y habilidades directivas.

Es evidente que cualquier perfil directivo necesita, ante todo "seniority" (experiencia profesional) y autoridad. El CISO es una figura directiva con un elevado –y creciente- grado de responsabilidad y las consecuencias de sus decisiones tendrán importante repercusión en materia de estrategia, presupuestos, políticas, instalaciones, operatividad de recursos, plazos, cumplimiento contractual, legislativo y normativo y dependerán en gran manera de él los riesgos, en materia ciber, que la empresa pueda atenuar o deba asumir. Es fundamental, por tanto, contar con un profesional con sólidos conocimientos del negocio y capacidad para valorar los daños que la pérdida de confidencialidad, integridad o disponibilidad de la información puedan causar a la empresa. Deberá ser capaz de identificar y/o entender los riesgos y valorar posibles soluciones para contrarrestarlos y no cabe la menor duda que en su carácter no puede faltar coraje y templanza no sólo para la toma de decisiones sino para ser capaz de afrontar y liderar actuaciones en casos de crisis.

Sin embargo, no por el hecho de tener autoridad y coraje puede estar exento de flexibilidad y de tener y saber aplicar el sentido común. El negocio reta permanentemente las medidas de seguridad porque suelen obstaculizar las iniciativas tecnológicas o lastrarlas con demoras y sobrecostes. La seguridad no puede conducir a la inmovilidad o suponer un freno especialmente en tiempos en los que la transformación digital se perfila como una necesidad, o incluso como un elemento que condiciona la competitividad de la organización o hasta su supervivencia a medio o largo plazo.

Hay otras muchas habilidades deseables para el CISO como son la capacidad de organización y priorización, la constancia y el compromiso con la empre- sa, la mentalidad de seguridad que cualquier miembro de este sector debe llevar en el ADN y las dotes de liderazgo. Respecto a este último aspecto, el CISO es responsable de un equipo humano y no pueden faltar las dotes para dirigirlo con diligencia y crear compromiso e implicación en toda la organiza- ción. Las habilidades interpersonales (inteligencia emocional), la formalidad y el respeto son claves para un buen desempeño de su función y la delegación es un fac- tor imprescindible. El CISO no puede saberlo todo; ser especialista de todo. El director de orquesta no tiene por qué saber tocar cada uno de los instrumentos pero ha de coordinar su ritmo para lograr una perfecta ejecución de la partitura.

El CISO debe dotarse de las capacidades y recursos de comunicación que su función requiere; debe transmitir, persuadir, sensibilizar y convencer. Tanto en su propia organización, como hacia el resto de las áreas.

EL CISO debe cultivar y dedicar parte de su tiempo a establecer relación con otros profesionales con análogas responsabilidades, a colaborar con asociacio- nes, con grupos especializados y a participar en actividades de colaboración pública-privada. Todas actividades, que forjan vínculos, le harán que esté al día y que disponga de una potente herramienta de ayuda, basada en la confianza, para solventar problemas a los que se enfrente por primera vez o en aquellos que necesite de una experiencia contrastada en una materia en la que todavía no se haya adentrado o se le haya presentada de forma sobrevenida.

Por último, hay una característica que nunca debe faltar en cualquier perso- na pero que es esencial en los miembros de seguridad independientemente de su ámbito de actuación: la integridad y la ética personal. En seguridad no puede existir la "segunda oportunidad" para las personas que defraudan la confianza. Se puede admitir una equivocación pero nunca una falta de honestidad o rec- titud. La confianza –digamos- se tiene por defecto pero, si se pierde, nunca se recupera.

VII CONCLUSIONES

El rol del CISO como máximo responsable de la seguridad de la información es ya prácticamente imprescindible en todas las entidades. La Transformación Digital, el panorama actual y futuro de amenazas y la necesidad de garantizar el cumplimiento de nueva legislación nacional e internacional.

El rol del CISO es un rol Directivo, especializado en seguridad de la información, pero con las mismas atribuciones que el resto de los directivos. Es el máximo responsable de asesorar a la alta Dirección para establecer la estrategia de seguridad de la información, asegurando que se alcancen los objetivos de negocio. El rol del CISO debe reportar a la Alta Dirección utilizando un esquema de Gobierno de seguridad de la información garantizando la segregación de funciones con otras áreas.

El rol del CISO es, sin embargo, tan imprescindible como aun insuficientemente conocido o reconocido por algunas organizaciones. Por ello, en el pasado se han tomado diversas decisiones sobre la ubicación de la función del CISO en el organigrama que no explotan suficientemente los conocimientos, visión ni la capacidad de aportar valor a la organización.

El CISO debe ser multidisciplinar, conociendo materias tan variadas como seguridad física y protección de activos, derecho de las Tecnologías, seguridad de las personas, detección y respuesta ante incidentes, privacidad y cumplimiento normativo, continuidad de negocio, gestión de riesgos, y teniendo como eje central un conocimiento profundo de la seguridad de la información.

El rol de CISO no había sido aún definido con precisión puesto que ha sido moldeado a lo largo del tiempo por las necesidades de las organizaciones y la evolución de las amenazas, frente a otros roles definidos por documentos, estándares o regulaciones que establecen claramente sus funciones y atribuciones.

Incluso la escasa legislación existente en la que la figura del CISO está directamente o indirectamente, debería armonizarse y darle al CISO un enfoque homogéneo e integral no ya en su denominación, sino lo que es mucho más importante en aspectos tales como en la definición de sus funciones, responsabilidades, aportación y relevancia.

Por ello, este Libro Blanco recopila la experiencia y visión de CISOs que ya lo son en organizaciones punteras, innovadoras y con necesidades identificadas claras en seguridad de la información.

Sirva este Libro Blanco como referencia para ayudar a la Administración a armonizar la función del CISO en actuales y futuras regulaciones y a las entidades para definir la función correctamente dentro de su organigrama.

ABREVIATURAS Y ACRÓNIMOS

BISO	**Business Information Security Officer**
CCN	**Centro Criptológico Nacional**
CCO	**Chief Communications Officer**
CDO	**Chief Digital Officer/Chief Data Officer**
CEO	**Chief Executive Officer**
CERT	**Computer Emergency Response Team**
CFO	**Chief Financial Officer**
CIO	**Chief Information Officer**
CIS	**Communications and Information Systems**
CISO	**Chief Information Security Officer**
CNI	**Centro Nacional de Inteligencia**
CNPIC	**Centro Nacional de Protección de Infraestructuras y Ciberseguridad**
COO	**Chief Operating/Operations Officer**
CPD	**Centro de Proceso de Datos**
CPO	**Chief Privacy Officer**
CRO	**Chief Risk Officer**
CSO	**Chief Security Officer**
CTO	**Chief Technology Officer**
CTSO	**Chief Technological Security Officer**
DPO	**Data Protection Officer**
ENS	**Esquema Nacional de Seguridad**
IT	**Information Technology TI**
LISO	**Local Information Security Officer**
NIS	**Network and Information Systems**
OT	**Operational Technology**
PCI-DSS	**Payment Card Industry - Data Security Standard**
PSD-2	**Payment Services Directive**
RD	**Real Decreto**
RGPD	**Reglamento General de Protección de Datos (GDPR)**

El Rol del CISO

Una iniciativa de

ISMS forum spain

En colaboración con

Cyber Strategy

Deloitte.

El Rol del CISO

ÍNDICE

I. Introducción

I.1.- La Seguridad de la Información

Actualmente, la necesidad de gestionar los riesgos relacionados con la Seguridad de la Información esta tomando más importancia que nunca. En esta línea, las organizaciones han decido tomar medidas y proteger su tesoro más preciado: La Información. El primer paso para hacerlo es nombrar un responsable, ampliamente conocido como Chief Information Security Officer (CISO), quién deberá asumir todas las funciones necesarias para mantener la información de su empresa a buen recaudo.

Actualmente, la necesidad de gestionar los riesgos relacionados con la Seguridad de la Información esta tomando más importancia que nunca. En esta línea, las organizaciones han decido tomar medidas y proteger su tesoro más preciado: La Información. El primer paso para hacerlo es nombrar un responsable, ampliamente conocido como Chief Information Security Officer (CISO), quién deberá asumir todas las funciones necesarias para mantener la información de su empresa a buen recaudo.

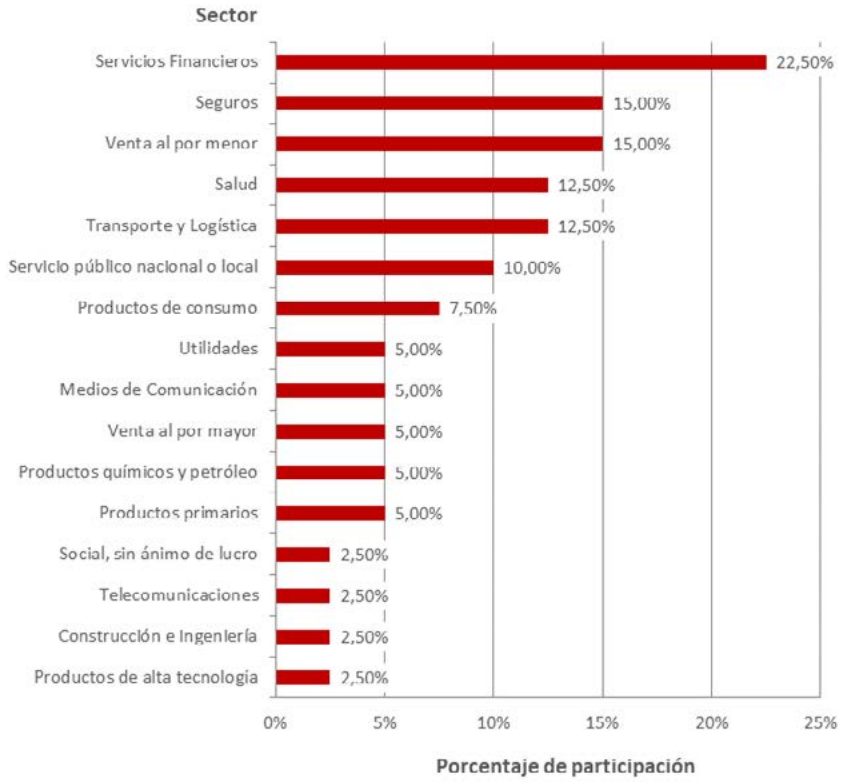
I.2.- Visión general: Sectores

1.2.1.- ¿En qué sector opera su empresa?

De cara a mostrar una visión general de los sectores involucrados en el estudio, a continuación se muestra el desglose por sector de las empresas participantes.

Tradicionalmente, los sectores de Banca y Seguros son los que más necesidad de invertir en ciberseguridad han observado. Esta tendencia se ve claramente reflejada en los participantes del presente estudio, y es debida tanto a las exigentes regulaciones impuestas sobre el sector bancario como a que dichas organizaciones representan un objetivo más llamativo para todo atacante, lo que las obliga a mantenerse en la vanguardia de las medidas de seguridad. Por lo tanto, participar en este este tipo de estudios les resulta especialmente útil.

Asimismo, la tendencia de otros sectores como Salud, Público, Transporte o Retail, para contar con perfiles especializados en el ámbito de la ciberseguridad cada vez es mayor, y es algo que se mantiene en los porcentajes de participación de este estudio. Sin embargo, algunos ámbitos como el de Telecomunicaciones se encuentran entre los últimos lugares. Esto, lejos de deberse a que encuentren poca necesidad de invertir en ciberseguridad, viene dado porque no se ha conseguido suficiente acercamiento a empresas de dicho ámbito.



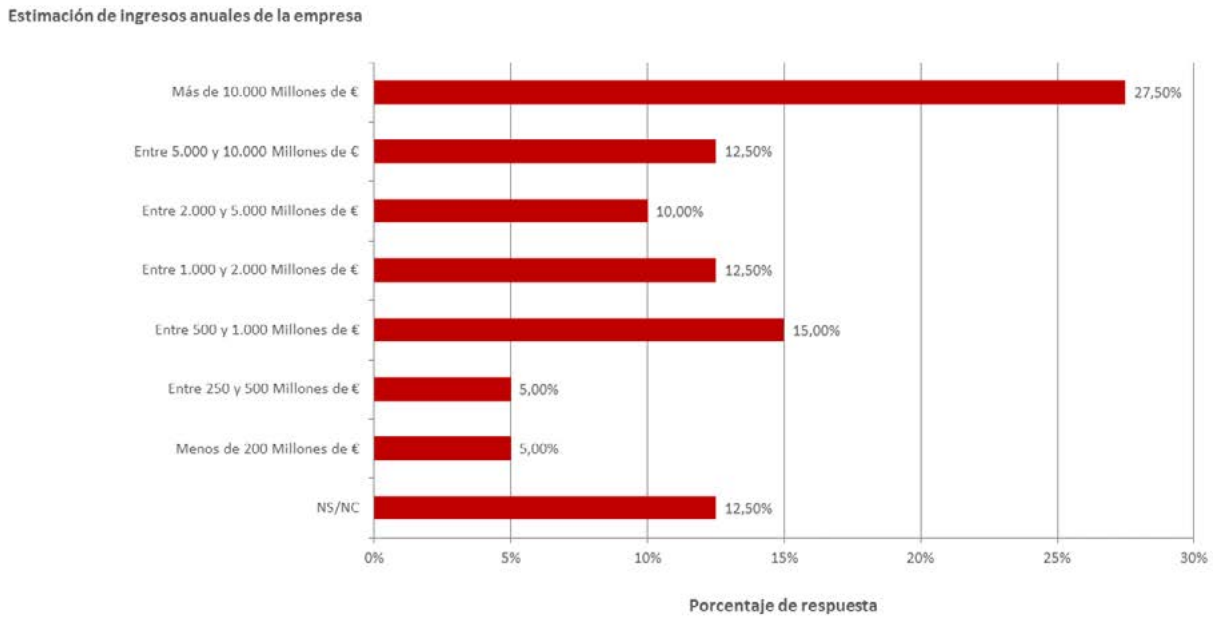
I.3.- Visión general: Ingresos

I.3.1.- ¿Cuáles son los ingresos anuales totales de su empre-

Podemos observar, que de forma mayoritaria, los empleados con categoría de CISO conocen el volumen de negocio o ingresos totales que reciben sus respectivas empresas procedentes de la venta de sus productos o servicios. Aun que cabe destacar que un 12'50% de los participantes no conocen el dato o han preferido no compartirlo.

Con respecto al acceso a esta información, indicar que normalmente las empresas que disponen de un perfil de CISO entre sus plantillas de empleados, suelen hacer públicas sus cuentas de beneficios en juntas de accionistas o reuniones internas. En esta línea, puesto que el perfil de CISO normalmente se reserva para promoción interna desde la posición de gerente, manager o superior, dicho perfil ya dispone de la información financiera sobre su organización.

Cerca del 40% de las empresas a las que pertenecen los perfiles encuestados se encontrarían en el TOP 20 del Ranking Nacional de Empresas* por facturación. Mayoritariamente, las empresas que disponen de perfiles como el de un CISO en su plantilla, son sociedades corporativas con un gran volumen de negocio.



I.4.- Visión general: Empleados

I.4.1.- ¿Cuál es el número de empleados de las empresas participantes?

De las respuestas obtenidas, se puede apreciar que el personal del 95% de las empresas participantes se compone de más de 1000 trabajadores, mientras que el 5% restante de estas empresas gestionan entre 100 y 500 empleados.

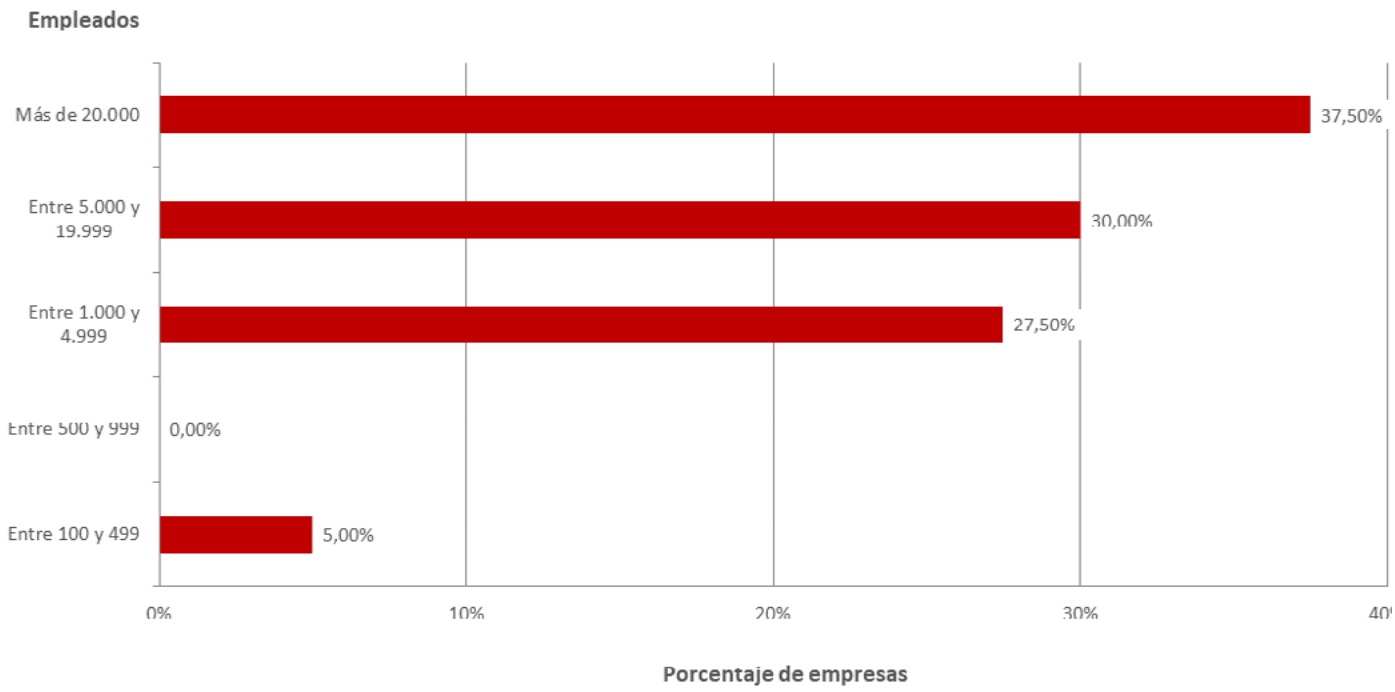
Entrando en detalle, se observa que el 95% anteriormente indicado se puede dividir en 3 rangos:

- El 27'5% de las empresas poseen entre 1.000 y 5.000 empleados.
- Por otro lado, un 30% administra entre 5.000 y 20.000 trabajadores.
- Y por último, la plantilla del 37'50% restante comprende más de 20.000 personas.

De estos datos, podemos obtener una imagen general del tamaño de las empresas participantes, la cual nos muestra que casi un 40% de las empresas encuestadas entrarían en el TOP 10 del Ranking Nacional de Empresas* por número de empleados.

Por otro lado, se puede extraer que actualmente, incluso ciertas compañías con menos de 500 trabajadores necesitan establecer la figura del CISO en su organigrama y están muy interesadas en comparar la madurez de su departamento de ciberseguridad con el estado general que muestra el presente estudio.

*Ranking de Empresas Españolas por facturación
https://ranking-empresas.eleconomista.es/
*Ranking de las 5.000 primeras empresas de España en el ejercicio 2016 http://epoca1.valenciaplaza.com/nacionalrankings/lista/buscar?orden_usuario-Nacionalranking/empleados2016%20DESC



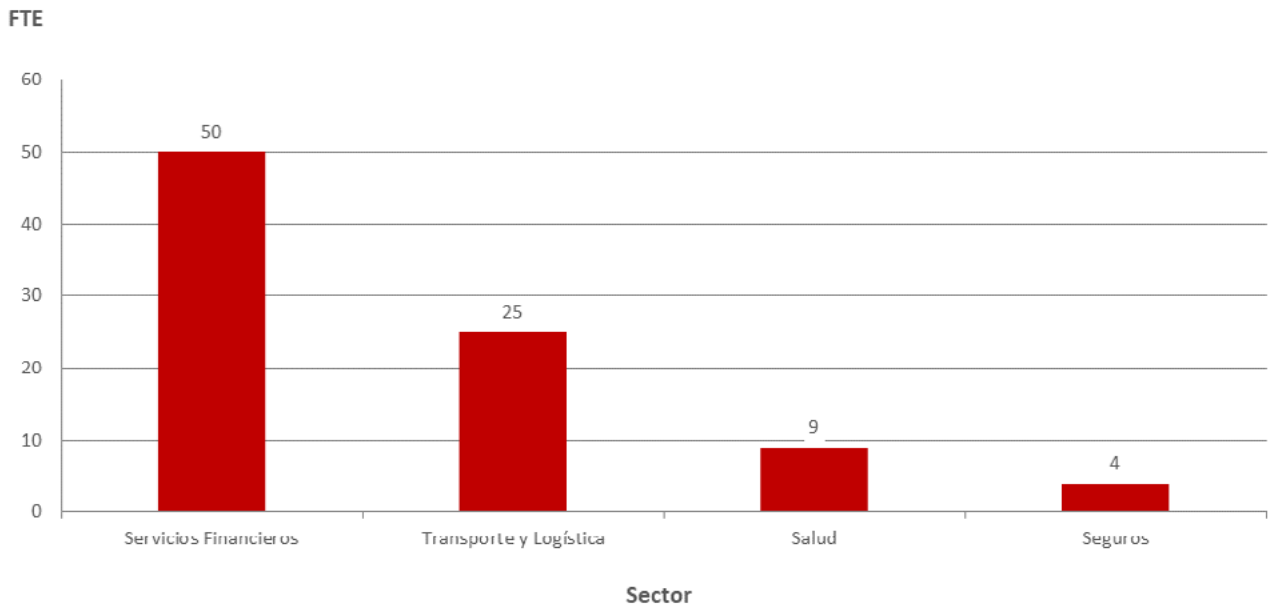
I.5.- Equivalente a Tiempo Completo

I.5.1.- ¿Cuál es el Equivalente a Tiempo Completo (FTE) del departamento de ciberseguridad?

De las respuestas obtenidas, podemos calcular que la media del Equivalente a Tiempo Completo del departamento de ciberseguridad de una empresa es de 20 unidades. Lo que significa que, por norma general, el equipo de ciberseguridad de una organización de tamaño considerable estaría compuesto por 20 trabajadores a tiempo completo. En cualquier caso, el número de personas necesitados para mantener la seguridad de la información no depende tanto del tamaño de la empresa ni de la cantidad de ingresos, sino que está más relacionado con el sector al que pertenece.

Se puede observar en la tabla, la cual recoge únicamente los sectores de los cuales se han obtenido más respuestas, que los Servicios Financieros son las empresas que más personal de seguridad necesitan para mantener la información que manejan protegida. Lo cual se debe a lo ya explicado en anteriores diapositivas relacionado con las exigentes regulaciones y el atractivo objetivo que representan para los atacantes. Esto sumado al hecho de que la fuga de su información o la posible violación del acceso a sus sistemas pueda conllevar la quiebra de miles de personas, obliga a este sector a tomar las medidas más altas posibles.

Por otro lado se encuentran los sectores de Transporte y Logística, Salud y Seguros, para los cuales consideramos que no se han obtenido suficientes muestras como para sacar conclusiones sólidas.

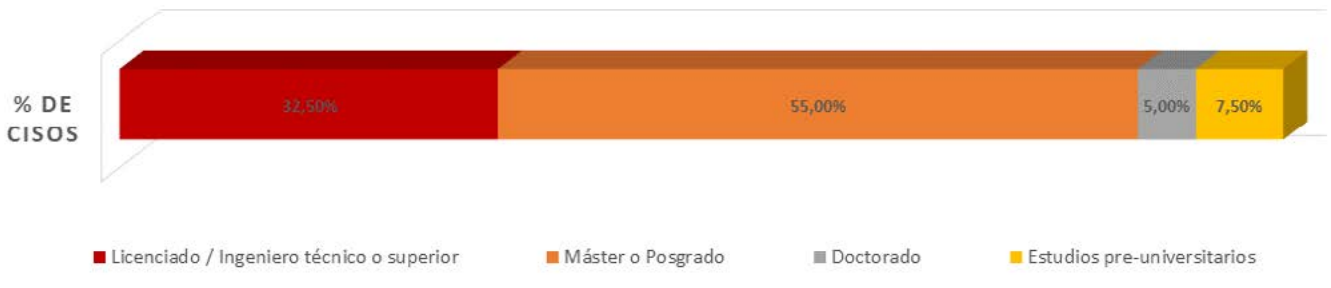


II. Estudios y formación

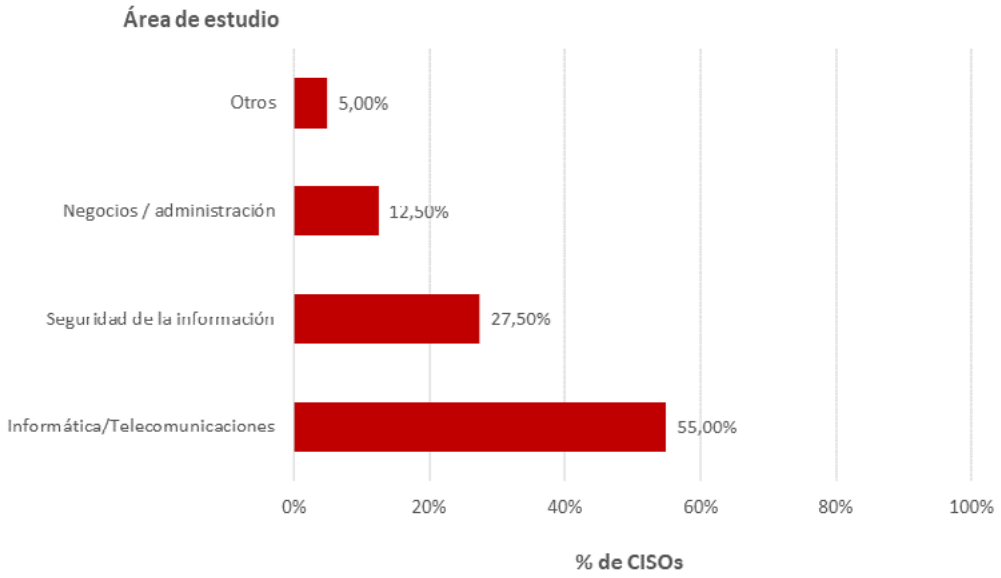
II.1.- Nivel de estudios

II.1.1.- ¿Cuál es el nivel más alto de estudios completado por los CISOs y en qué área?

De acuerdo a la encuesta lanzada a 40 CISOs de España, en las siguientes gráficas se observa qué nivel de estudios poseen y a qué área han enfocado su desarrollo académico:



Si bien más del 80% ha enfocado sus estudios al área de Seguridad de la Información, Informática o Telecomunicaciones, el rol del CISO actualmente se aleja de la parte técnica para centrarse en las necesidades de negocio. Como se indica en un estudio de Gartner*, la mayoría de los CISOs fracasa porque no entienden o no cumplen con los requisitos y expectativas del negocio.
Resulta interesante entender que, aparte de los conocimientos en materia de Seguridad de la Información, es imprescindible comprender y saber transmitir las necesidades de negocio.



II.2.- Área de trabajo del CISO

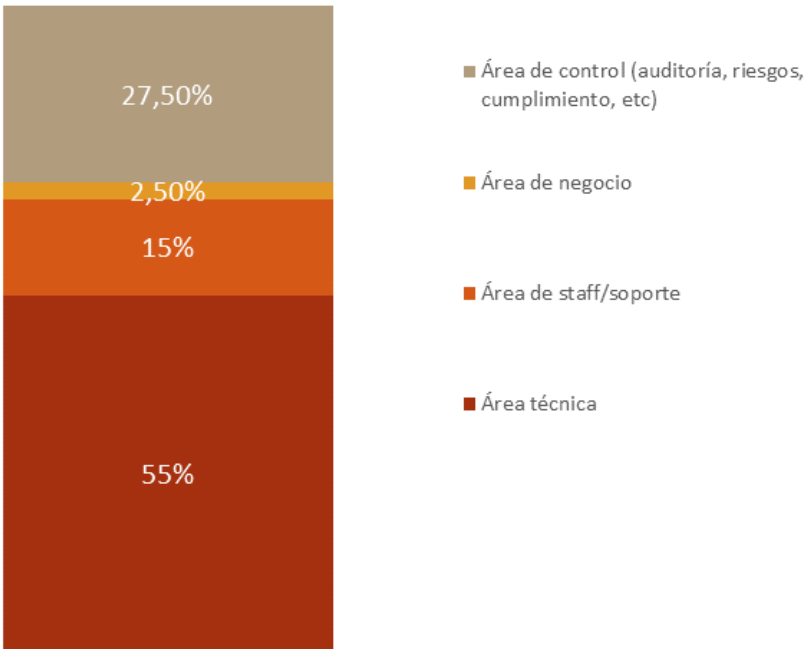
II.2.1.- ¿De qué área de expertise proviene y con qué área se identifica el CISO?

Anteriormente se ha demostrado que solamente el 12'5% tiene estudios en el área de negocios, no obstante, el 95% de los CISOs ha desarrollado su carrera profesional en el área de la Tecnología de la Información.

Aún siendo un porcentaje reducido los CISOs con estudios en el área de negocios/administración, parte de ellos han trabajado en área de TI antes de desempeñar su actual trabajo.

Dado que actualmente el CISO tiene mayor incidencia en las decisiones de negocio, es llamativo que solamente el 2'50% identifique su trabajo con el área de negocio y el 55% lo asocie con el área técnica. Esto puede deberse a que la figura del CISO requiere de conocimientos tanto técnicos como empresariales y, al tratarse de un rol bastante reciente, la gran mayoría de los CISOs provienen de áreas técnicas o de seguridad de la información.

* The Chief Information Security Officer's First 100 Days - 2018, Gartner



II.3.- Certificaciones Profesionales

II.3.1.- ¿Cuáles son las certificaciones más comunes entre los CISOs?

Poseer una certificación en el ámbito de la Seguridad permite validar conocimientos en la materia y competencias profesionales además, genera confianza en el profesional certificado.

Entre las certificaciones más conocidas en el sector de la Seguridad de la Información se encuentra la CISSP, CISA o la GIAC y en la gráfica podemos ver cuántos CISOs del panorama actual las tienen. Por otro lado, certificaciones como la SSCP tienen un enfoque más técnico. Entre las más comunes destaca CISM con un 60% de encuestados.

Solamente el 23'42% de las certificaciones de los CISOs encuestados tienen un enfoque técnico, lo cual corrobora que el rol del CISO está enfocado a funciones de negocio.

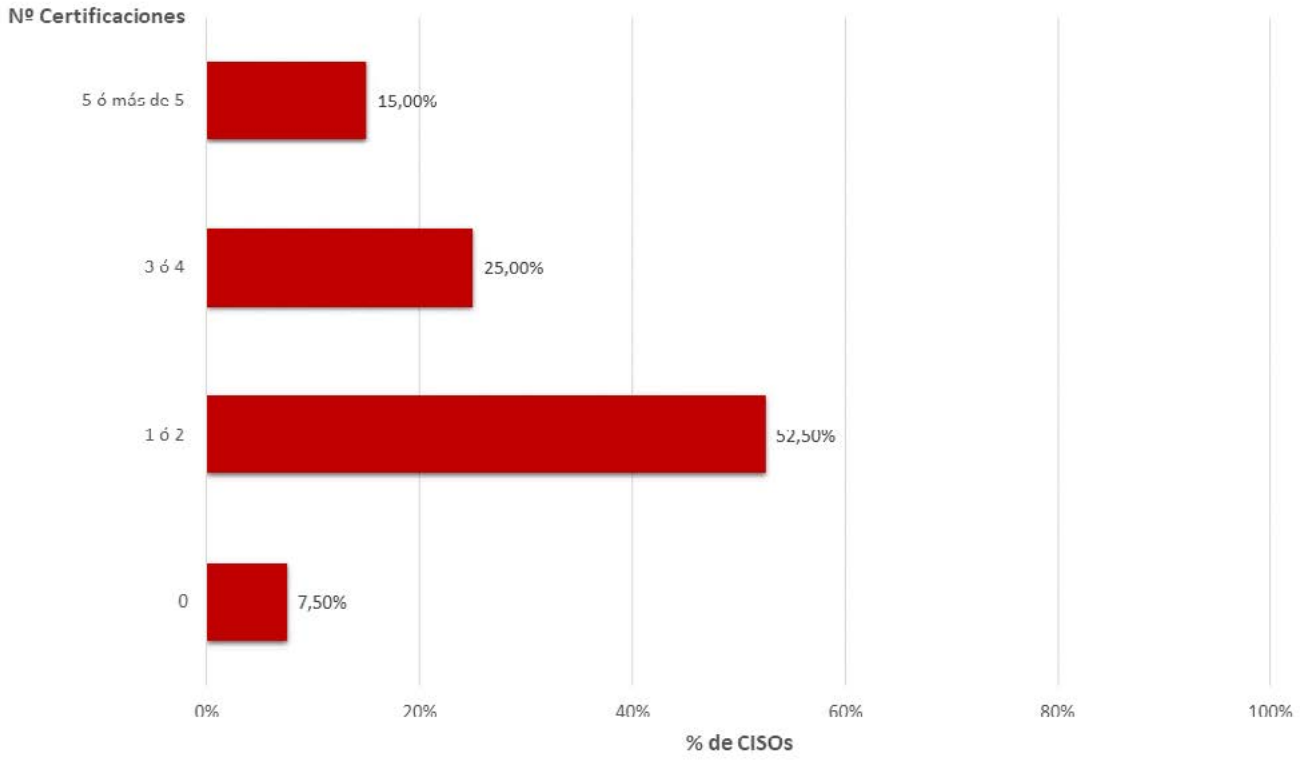
II.3.2.- ¿Cuántas certificaciones profesionales relacionadas con la seguridad tienen los CISOs?

Tras ver cuáles son las certificaciones más comunes entre los CISOs, se ha analizado cuántas posee cada uno de ellos.

Si bien de los 40 CISOs encuestados, había 3 que no poseían ninguna Certificación en materia de seguridad, el resto de encuestados tiene una media de 2.89 certificaciones/CISO.

Solamente un 15% obtuvo 5 o más certificaciones, Los CISOs que poseen esa cantidad de certificaciones son en su mayoría aquellos cuya formación académica estaba enfocada al área de los negocios. Por ello, se puede afirmar que las certificaciones permiten tener un visión de la Seguridad de la Información que complementa lo aprendido durante la carrera o estudios cursados.

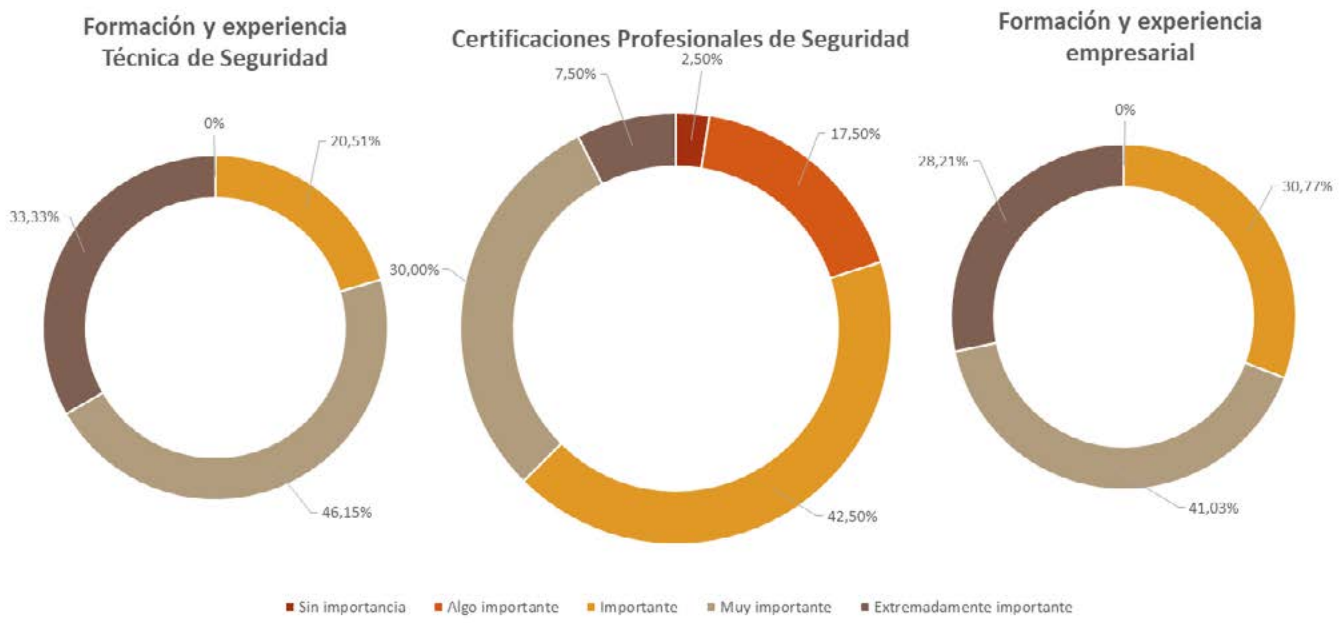
El rol de CISO lo toman progresivamente personas más enfocadas a negocio, que llevan a cabo sus labores gracias a las certificaciones de Seguridad.



II.4.- Valoración formación y certificaciones

II.4.1.- ¿Cuál es la valoración de la Formación y experiencia Técnica o empresarial y las Certificaciones de Seguridad?

En la encuesta realizada se pretendía conocer la valoración personal que tienen los CISOs sobre la formación y las Certificaciones Profesionales de Seguridad.



III. Puesto y funciones

III.1.- Posición en la organización

III.1.1.- ¿Cuánto tiempo lleva un CISO en su puesto actual?

En la década de los años 2000 no existían razones de peso ni culturales para dedicar esfuerzos y recursos humanos a una figura como es la que hoy en CISO. Los recursos se destinaban principalmente al área de auditoria o legal. Esto es uno de los motivos por los que solo un 8% de los CISOS encuestados llevaban más de 15 años en su cargo.

Ha sido en la última década cuando ha habido una necesidad real por parte de las empresas de todos los sectores y negocios de que exista una figura que se encargue de la seguridad de la información y que empiece a formar parte de sus estructuras organizativas. Este es uno de los motivos por el cual el 70% de los CISOS encuestados lleva menos de 10 años a su cargo, eso quiere decir que hasta principios del 2008 no tuvieron un papel relevante.

- La media de un CISO en su cargo es de 6 años y medio, teniendo en cuenta que la figura tiene un cargo de directivo llevar poco más de 6 años es demasiado poco para un cargo como este. Uno de los motivos principales es la alta demanda de la empresas por este tipo de perfil y cada vez más las empresas empiezan a ofrecen más dinero para que vayan a trabajar con ellos.

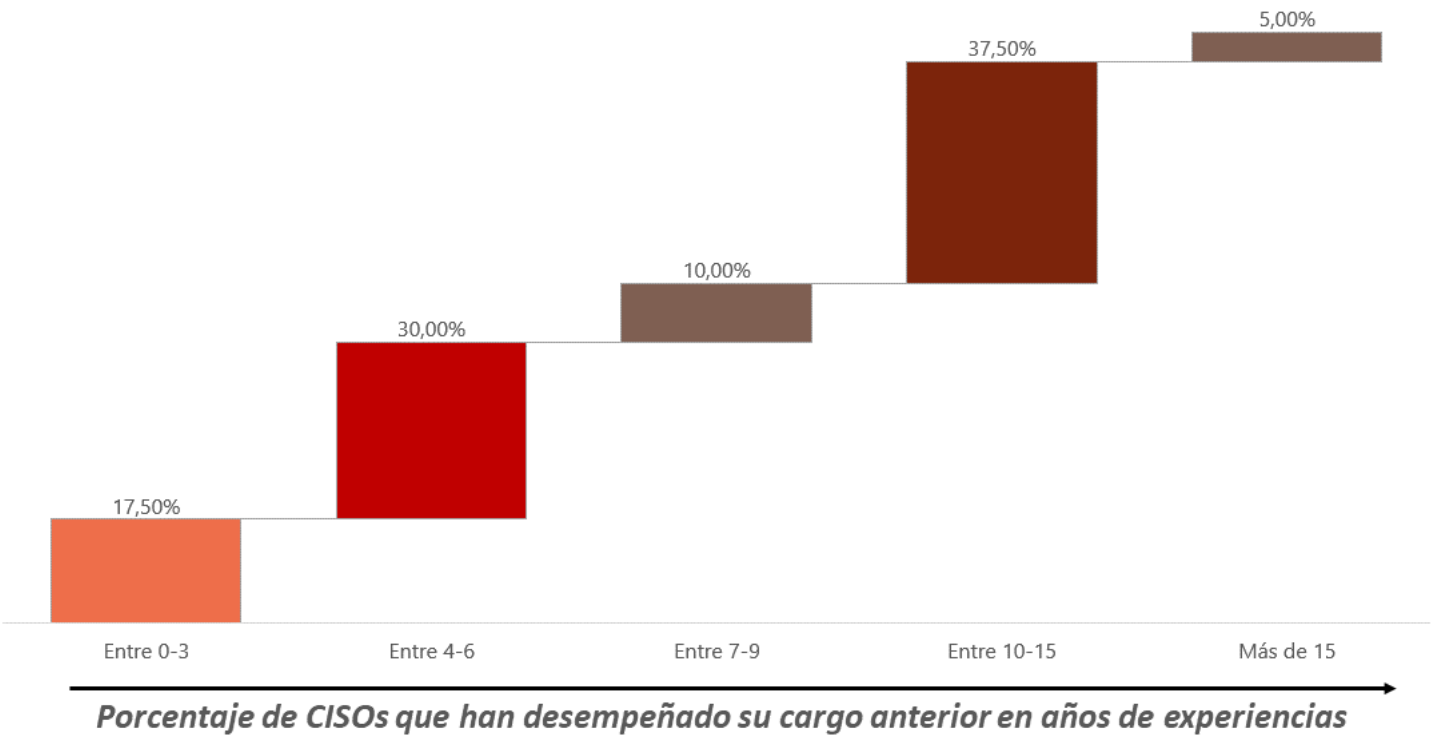
- Dentro del 70% de los CISOS que llevan menos de 10 años en su cargo el 68% llevan 5 años o menos, es un dato también bastante significativo, ya que los principales incidentes de seguridad han ocurrido en el último lustro llevando a las empresas a tomar medidas y destinar más recursos tanto económicos como humanos a esta área.

III.2.- Puesto anterior

III.2.1.- ¿Durante cuánto tiempo desempeñó el cargo anterior?

Si se analiza la experiencia previa de los CISOS se obtiene que la media de durante cuanto tiempo desempeñó su cargo es de un poco más de 8 años, esto es muy poco años de experiencia teniendo en cuenta que algunos casos pertenece a la capa ejecutiva de la organización. Esto quiere decir que en general son gente joven y empiezan a ser CISOS con 30-40 años. Si vemos la experiencia completa de un CISO observamos que están alrededor de los 14 años y medio de experiencia.

> Debido a la gran demanda de profesional se está contratando a más gente con menos años de experiencia. Un 30% han estado entre 4-6 años desempeñando su anterior cargo.



Observamos que en los últimos años ha habido dos grandes momentos de contratación de CISOS. Un 37,5% fue contratado con entre 10-15 años de experiencia.

Este repunte en los últimos 3 años es debido a lo ocurrido en los últimos incidentes de seguridad como el WannaCry que este año hace 2 años.

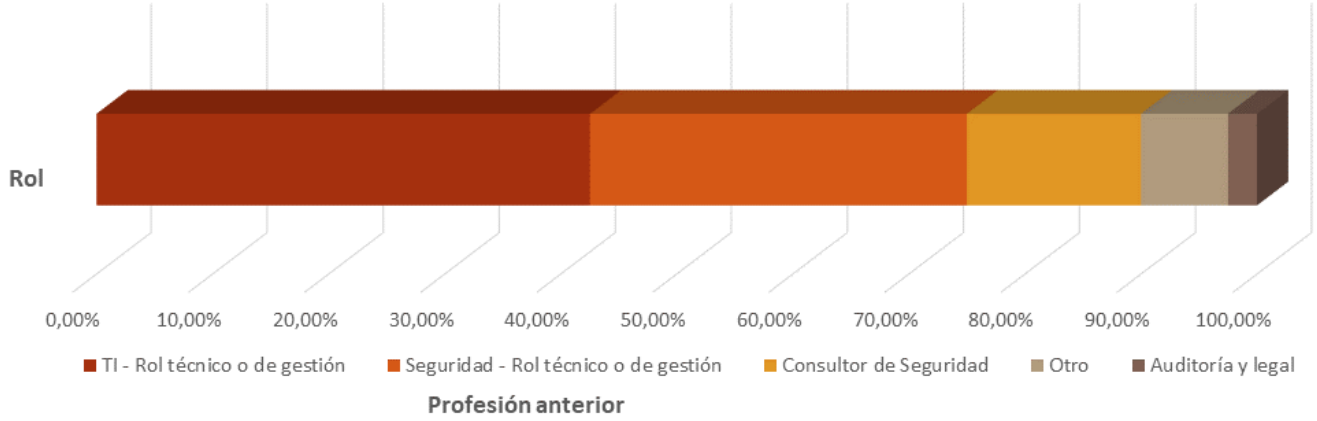
III.2.2.- ¿Cuál fue su rol profesional anterior?

El perfil de un CISO es principalmente es personas con experiencia en Seguridad o IT cuya formación académica normalmente es ingenieros de telecomunicaciones o informáticos, alto nivel de inglés, certificaciones profesionales de seguridad como pueden ser CISA, CISM, CISSP, Certificaciones de Amazon etcétera.

También es necesario complementarlos con conocimientos sobre el negocio, riesgos tecnológicos y ciberseguridad, además de tener que estar al día de todas las amenazas y tendencias del sector.

Se puede comprobar como el rol que tenia anteriormente el CISO en su anterior trabajo era relacionado con el área de TI, Seguridad o en el área seguridad de consultoría. Siendo estas áreas necesarias para desempeñar su función.

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf



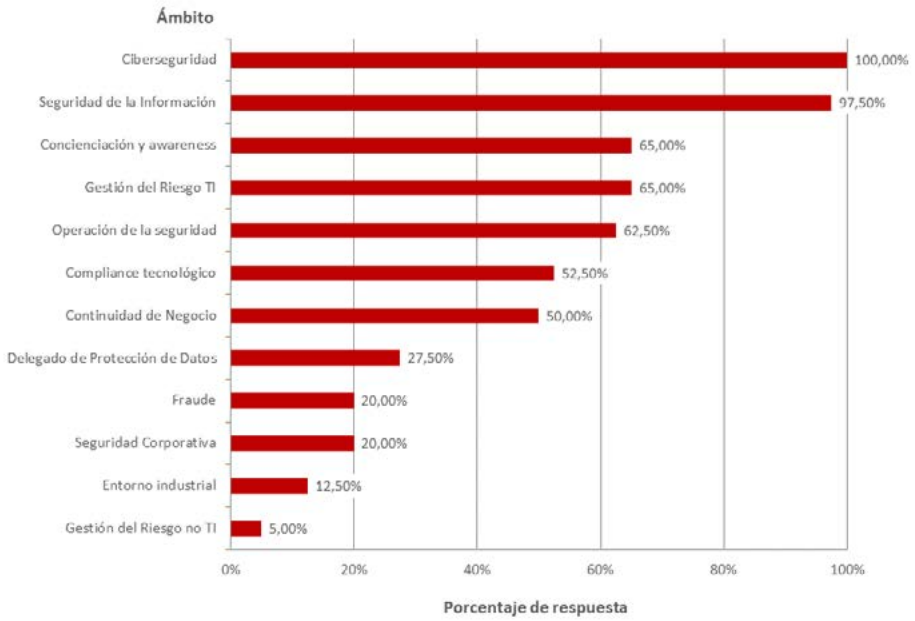
Un 90% de los encuestados provienen de ramas técnicas o de seguridad. En cambio un 2,5% provienen del auditoria y legal siendo que esta área normalmente está fuera de las funciones del CISO.

III.3. Ámbitos

III.3.1.- ¿De qué ámbitos relacionados con la ciberseguridad se encarga el CISO?

De las respuestas obtenidas en el presente estudio, se puede observar que en la mayoría de los casos la figura del CISO tiene responsabilidades relacionadas con la Concienciación y awareness, la Gestión del Riesgo TI, la Operación de la seguridad, y por supuesto, con la Gestión de la Seguridad de la Información y la Ciberseguridad. Como es lógico las funciones principales de un CISO son las que más porcentaje de respuesta han obtenido.

Por otro lado, ámbitos como la Gestión del Riesgo no TI, el Entorno industrial, la Gestión de la Seguridad Corporativa o el Fraude, se encuentran con menor frecuencia entre las funciones de un CISO y únicamente un porcentaje reducido de los encuestados consideran que sus tareas tienen relación con estos ámbitos.



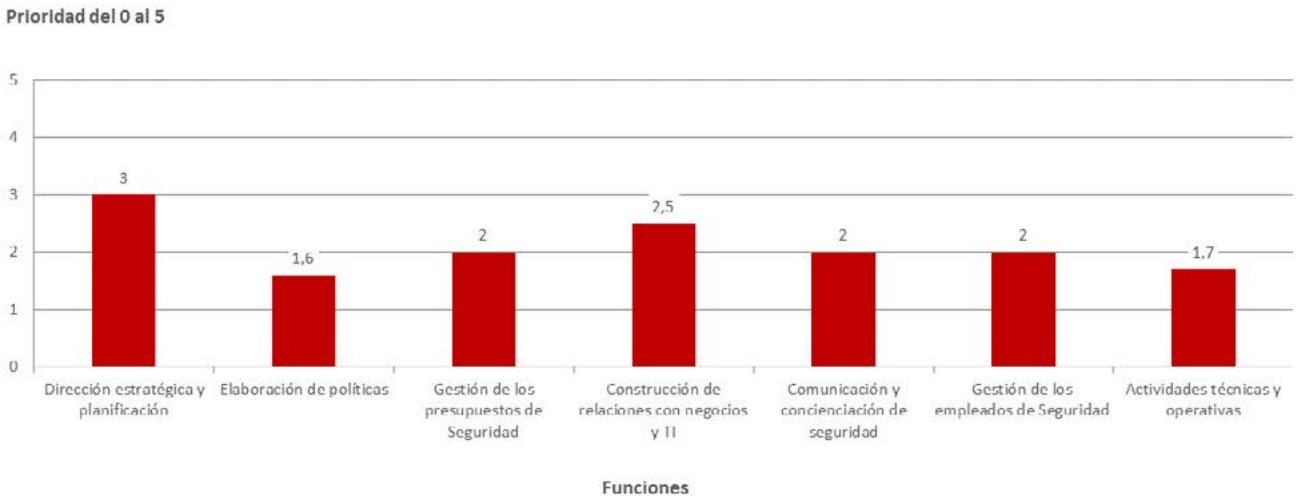
III.4.- Prioridades

III.4.1.- ¿Qué prioridad se le da a las diferentes funciones del

A partir de la prioridad que cada CISO ha indicado para las siguientes funciones, tal y como muestra el gráfico, la Dirección estratégica y planificación se trata de la tarea a la que más atención presta la figura del CISO por norma general, seguida de La construcción de relaciones y asociaciones con las partes interesadas de negocios y de TI.

Por otro lado, la Elaboración de políticas se encuentra en una posición menos prioritaria entre las tareas. Aunque la elaboración de políticas sea una parte esencial de la administración de la organización, a largo plazo, la prioridad de esta tarea acaba viéndose reducida para dar paso a otras como la Gestión de presupuestos y empleados y la Concienciación de ciberseguridad, las cuales se encuentran al mismo nivel entre las respuestas.

Por último, la tendencia general marca que las funciones del responsable de la ciberseguridad se orientan más hacia la gestión y se alejen de tareas a bajo nivel. Esto explica que las Actividades técnicas y operativas ocupen el último lugar entre las prioridades del CISO.



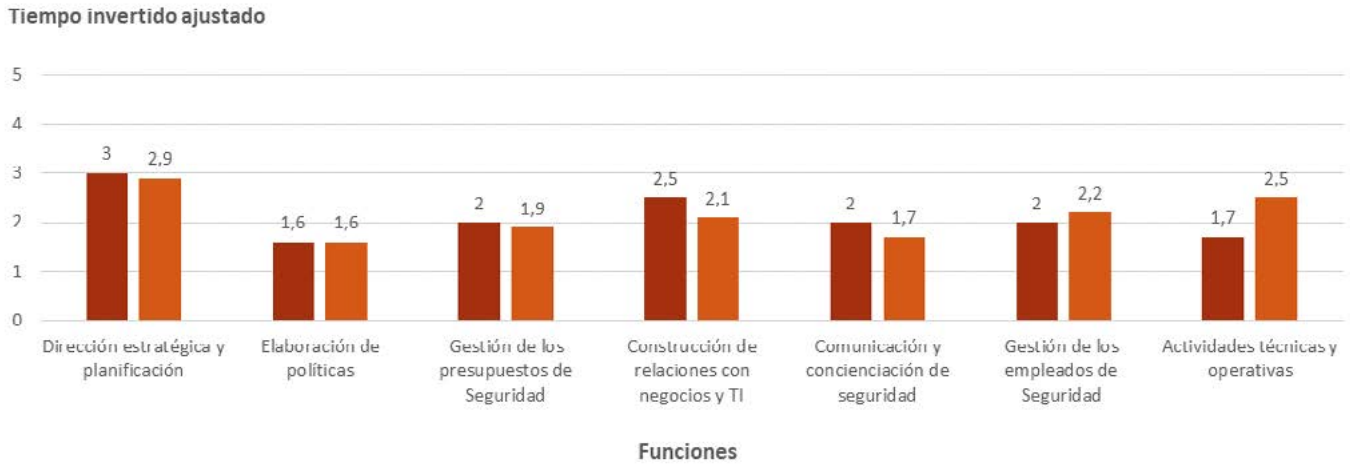
III.5.- Tiempo Invertido

III.5.1.- ¿Cuánto tiempo invierte el CISO en las funciones anteriores?

Se puede observar que mayoritariamente, las tareas a las que se les atribuye mayor importancia también son en las que se invierte más tiempo. El tiempo dedicado a las funciones de Dirección estratégica y planificación, Elaboración de políticas, y Gestión de los presupuestos concuerda con la prioridad que se le da a las mismas.

Sin embargo, a pesar de que la Gestión de los empleados y las Actividades técnicas son dos funciones con menor prioridad, según lo indicado por los propios CISOs encuestados, también son dos de las tareas que conllevan mayor implicación de tiempo por su parte. Bien es sabido que el trabajo técnico y operativo conlleva una alta inversión de tiempo y en algunas ocasiones, el alto conocimiento que la figura del CISO posee, le obliga a tomar parte en este papel.

Por otro lado, se encuentran las funciones de Construcción de relaciones y Concienciación. Para estas tareas, las respuestas indican que implican menos tiempo del que en un principio parecería debido a su importancia.



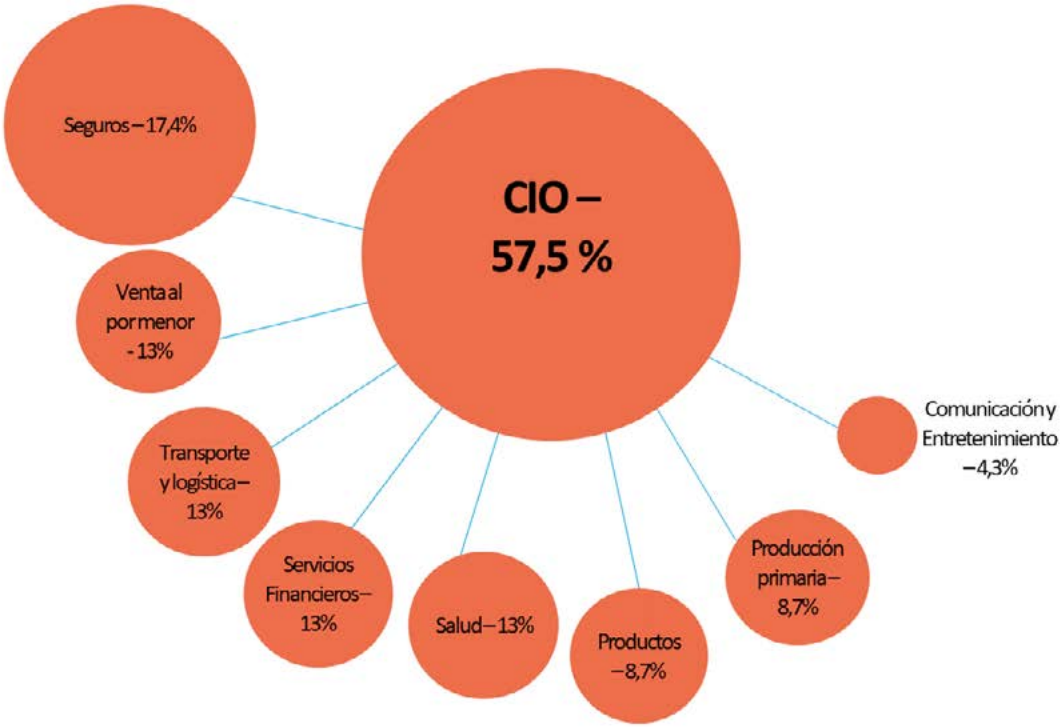
IV. Reporting y futuro

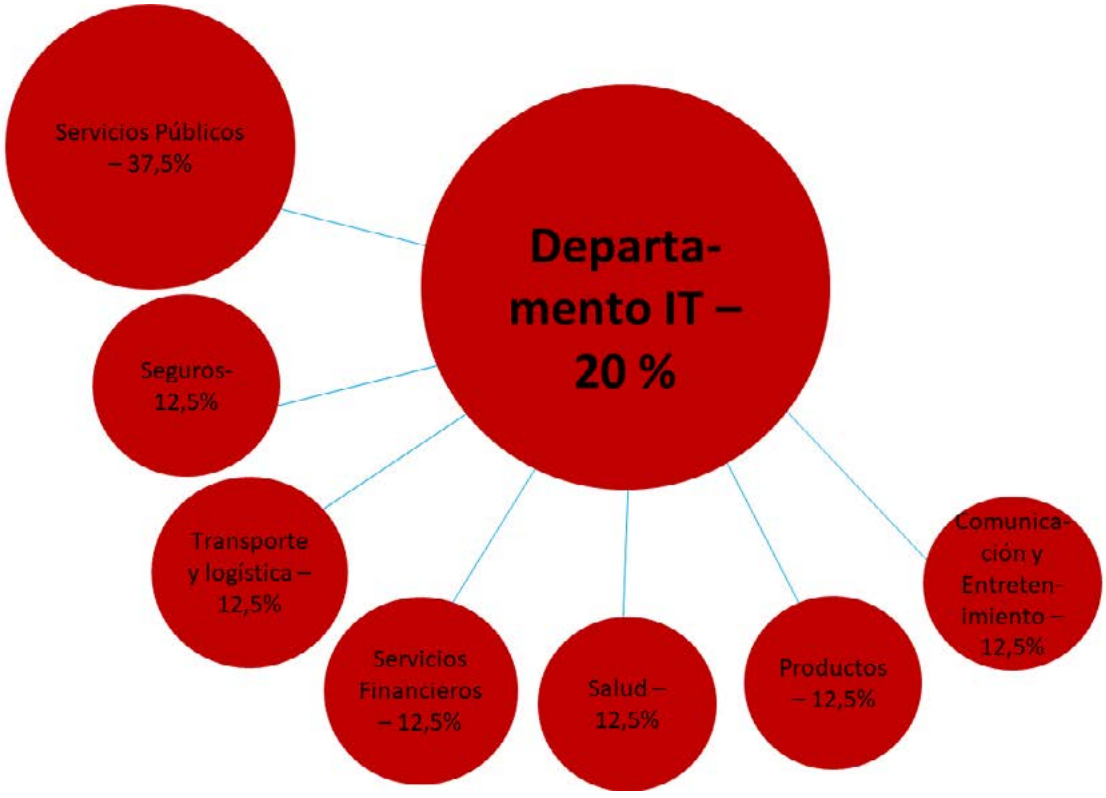
IV.1.- Modelo organizativo

IV.1.1.- ¿A quién reporta un CISO?

No existe un modelo de gobierno definitivo, ya que cada empresa tiene un modelo y sector de negocio totalmente diferentes. Aun así, aunque la encuesta esté realizada a todo tipo de sectores se evidencia que la figura del CISO principalmente tiene un área específica de seguridad dentro de la empresa reportando directamente al CIO o al departamento de IT en su caso.

Si se analiza a quién reporta un CISO según el sector llegamos a la conclusión dentro del 20% que reportan al departamento de IT casi el 40% se identifican con el área de servicios públicos.


CIO – 57,5 %
Seguros – 17,4%
Venta al por menor - 13%
Transporte y logística – 13%
Servicios Financieros – 13%
Salud – 13%
Productos – 8,7%
Producción primaria – 8,7%
Comunicación y Entretenimiento – 4,3%


Departa-mento IT – 20 %
Servicios Públicos – 37,5%
Seguros- 12,5%
Transporte y logística – 12,5%
Servicios Financieros – 12,5%
Salud – 12,5%
Productos – 12,5%
Comunica-ción y Entreten-imiento – 12,5%


Comité Interdepar tamental – 7,5%
Otro – 7,5%
Departam ento Financiero - 2,5%
CSO / COO - 2,5%

IV.1.2.- ¿A quién considera un CISO que debería reportar?

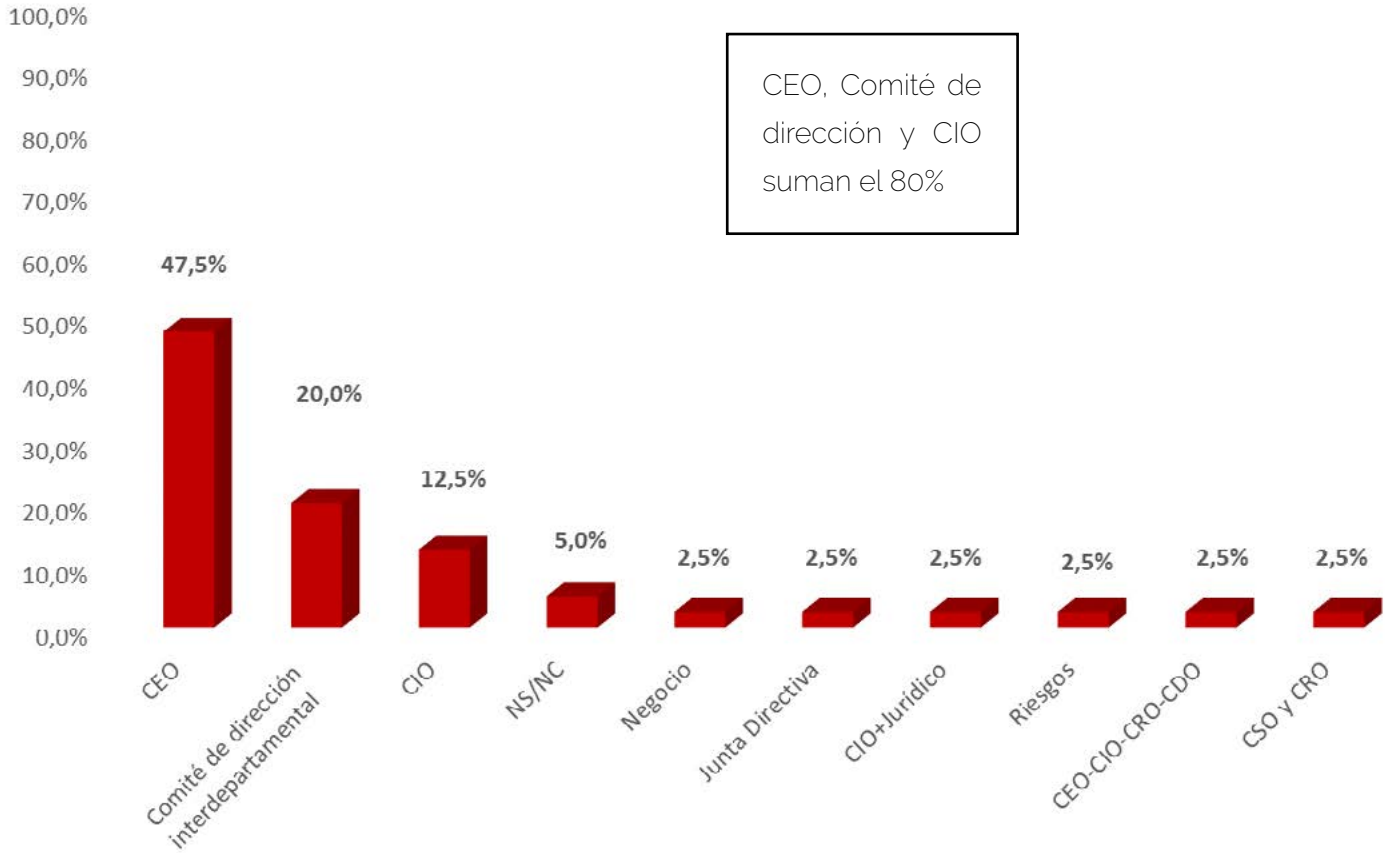
Según los encuestados casi el 80% de los CISOS considera que debería reportar siguiendo los 3 modelos de gobierno para su posición y reporte. También un dato significativo es que un 5% de NS/NC a quien debería reportar.

Los 3 modelos de gobierno más comunes son:

Reportando directamente a la alta dirección. Fuera del área de tecnología y reportando directamente al consejero delegado, presidente o CEO. Los puntos fuertes serian que tiene más capacidad de decisión a alto nivel pero sacrificando la cercanía de la operativa del día a día en el área de tecnología.

Reportando al COO/CRO/Comité de Dirección. Este punto suele ser más común en empresas relacionadas con la industria. Como en el anterior caso también fuera de tecnología pero como una figura de directivo sin llegar a la alta dirección.

Un área dentro del CIO. En la misma arquitectura departamental que Tecnología, esto le ayuda a estar cerca de la operativa y toma de decisiones a nivel tecnológico.

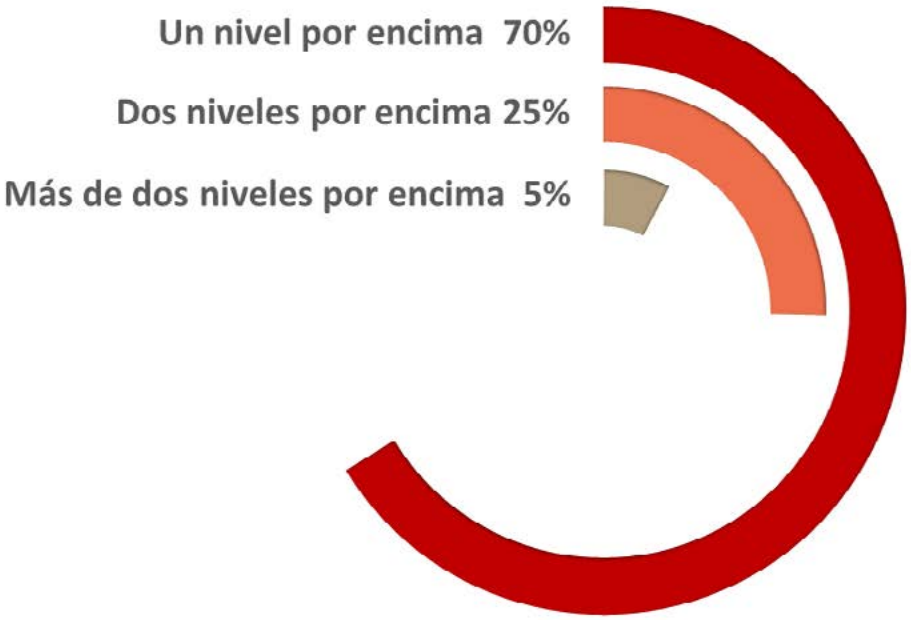


IV.1.3.- ¿A qué nivel está la persona a la que reporta directamen-

Como hemos visto con anterioridad la figura del CISO reporta principalmente a los órganos de gobierno ya sea el CIO, CEO o comité de dirección. Todas estas figuras corresponde jerárquicamente a uno o dos niveles por encima dentro de la organización, desde donde se encuentra el CISO:

Si comprobamos los resultados obtenidos de a quién reporta en la empresa con cuantos niveles está por encima obtenemos datos interesantes. En el caso del CIO hay casi un 4,5% de encuestados que dice que está a más de dos niveles por encima, no es habitual que la figura del CISO y CIO estén tan separadas jerárquicamente.

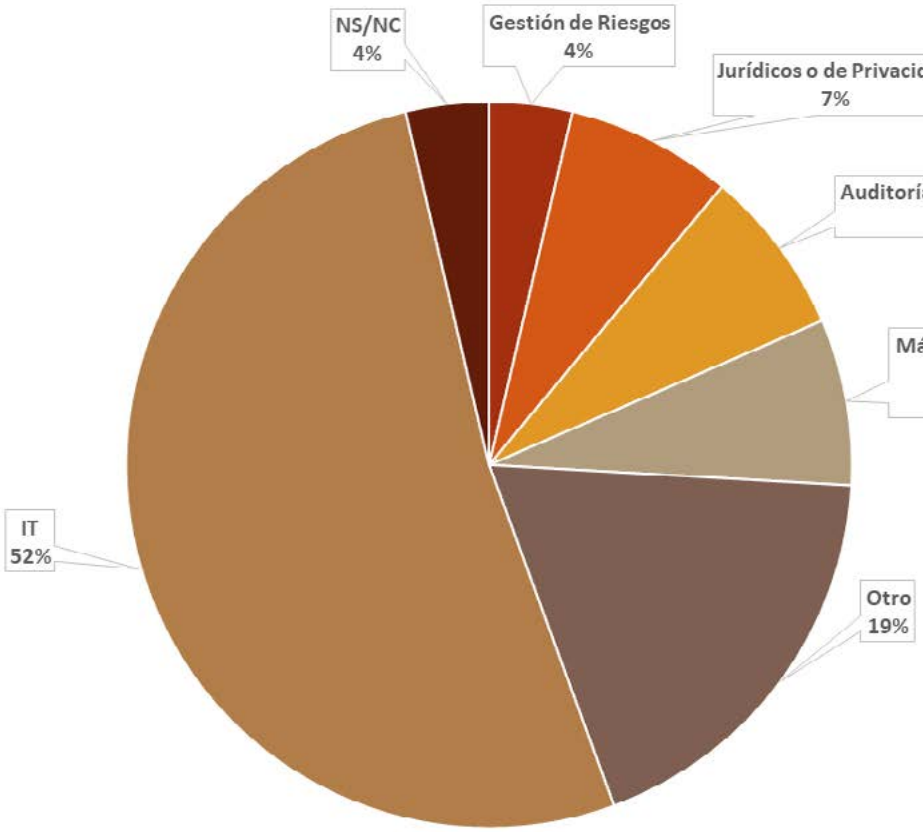
	5%	25%	70%
¿A quién reporta dentro de la empresa?	**Más de dos niveles por encima**	**Dos niveles por encima**	**Un nivel por encima**
CIO	4,35%	17,39%	78,26%
Comité de dirección interdepartamental		66,67%	33,33%
Departamento de TI	12,50%	37,50%	50,00%
Departamento financiero			100%
CxO			100%
Otro		33,33%	66,67%



IV.1.4.- ¿Cuál espera que sea el siguiente paso?

El rol de CISO es un rol de directivo en la organización aun poco conocida pero imprescindible por eso mismo el 33% de los encuestados se siente satisfecho con su posición y desearía continuar en su misma posición mientras que el otro 66% cambiaria de posición.

Analizando ese 66% que cambiaria de posición hay que destacar que más de la mayoría (52%) estaría dispuesto a ascender a un nivel ejecutivo o Directivo más alto en IT (Ej. CIO) y que el 4% no sabe o no quiere contestar sobre su futuro profesional.



El 93% reporta al CIO o departamento de IT

Un 21% de los encuestados que engloba Jurídicos, Auditoría y función de negocio se estaría alejando de las "raíces" de un CISO que serian el área de IT o Seguridad.

Del 52% que ascenderían a un nivel ejecutivo o Directivo más alto en IT el 93% reporta a alguno de los dos, esto quiere decir que la mayoría de los CISOS encuestados quieren que su siguiente paso profesional es a la persona que están reportando.

V. Presupuesto y Salario

V.1.- Presupuesto y salario

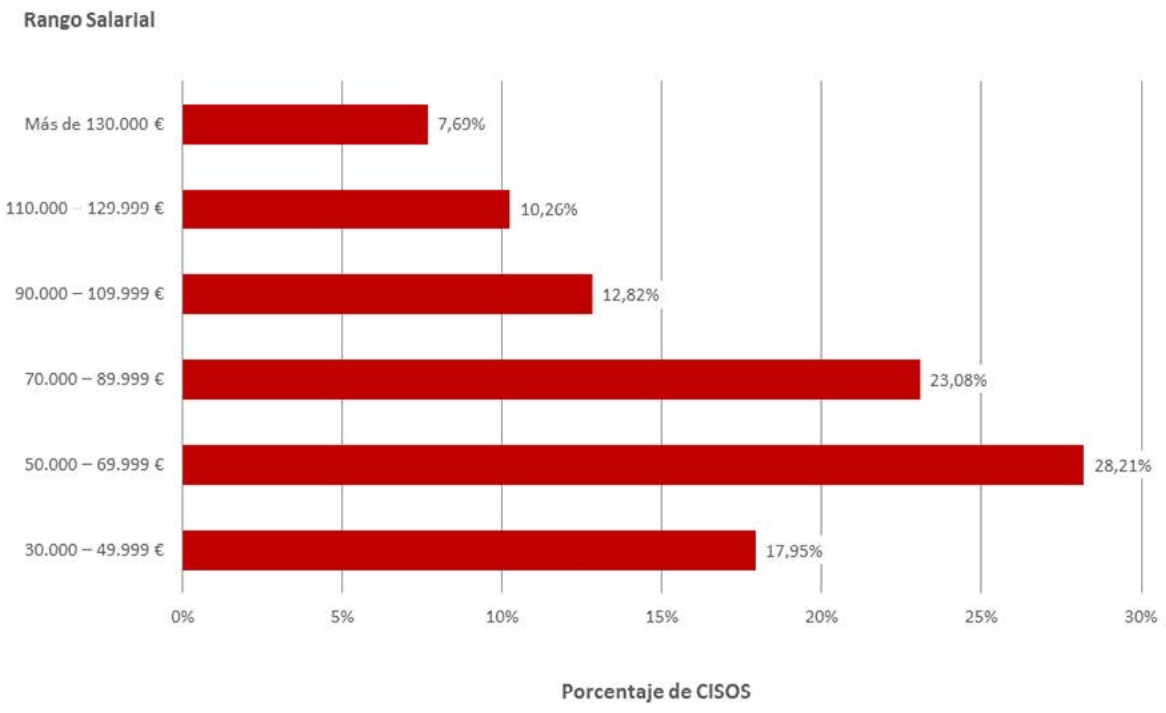
V.1.1.- ¿Cuál es el rango salarial bruto/anual en el que se encuentra actualmente?

Con el escenario actual, la figura del CISO se ha convertido en uno de los perfiles más demandados en las empresas: desde 2014, la demanda prácticamente se ha duplicado.

Dado que no es un perfil fácil de encontrar, esta descompensación entre oferta y demanda ha desembocado en salarios cada vez es más altos. Así mismo, no es fácil retener a empleados con dichos perfiles en las empresas. La inflación salarial provoca una alta movilidad laboral en busca de retribuciones siempre crecientes. Para evitar esto, la empresas están tratando de fidelizar al trabajador, ofreciéndole algo más que un buen salario.

No todos los responsables de seguridad de la información ganan lo mismo.

Con base en la encuesta, prácticamente el 50% de los consultados manifiestan tener un salario de entre 50.000 – 89.999€. Aunque se observan diferencias salariales de hasta 100.000 euros anuales entre las horquillas más altas y las más bajas, según datos publicados por diversos medios*, en general el sector de Banca y Seguros es el que mejor paga, seguido por el de Telecomunicaciones, Retail y Farmacéutico. Aunque puede haber excepciones, cuanto más grande es la empresa, más alto suele ser el salario.

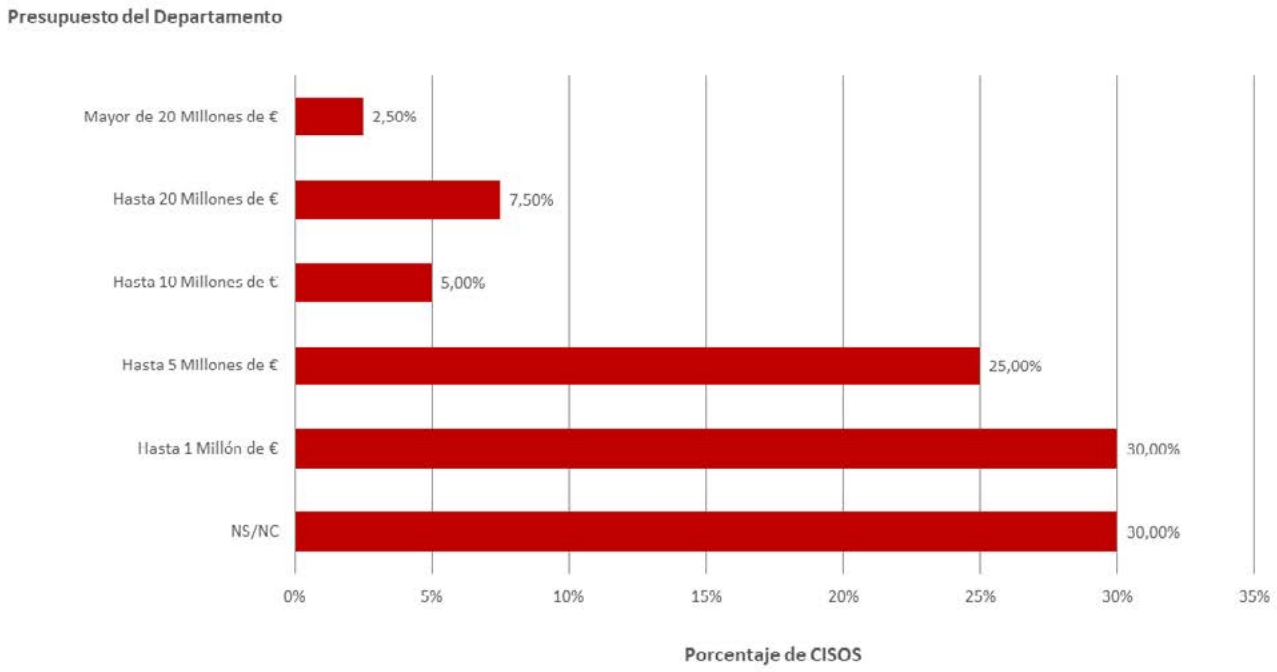


*¿Cuánto puede ganar un CISO? Sectores mejor pagados.
https://www.itdigitalsecurity.es/actualidad/2018/01/cuanto-puede-ganar-un-ciso

V.1.2.- ¿Cuál es el presupuesto de su departamento?

Se estima, que únicamente el 24% de las organizaciones se pueden considerar estar razonablemente preparadas para hacer frente a ciberataques. Teniendo en cuenta la transversalidad y la importancia que ha adquirido la Ciberseguridad dentro de las estrategias de transformación digital, la figura del CISO esta tomando cada vez más peso en las decisiones de negocio.

Este cambio de cultura, que pasa de tener únicamente en cuenta la prevención a poner foco también en el ámbito de la detección y la respuesta, implica una mayor concienciación del riesgo, lo que directamente implica aumento de presupuestos para los departamentos dedicados a gestionarlo. Diversos medios* han publicado que se calcula, que el 83% de directivos invertirá al menos un 10% de su presupuesto TI en Ciberseguridad a lo largo de los próximos 3 años. Una buena tendencia, aunque quizás aun insuficiente, si tenemos en cuenta que los errores humanos se pagan caros en ciberseguridad.



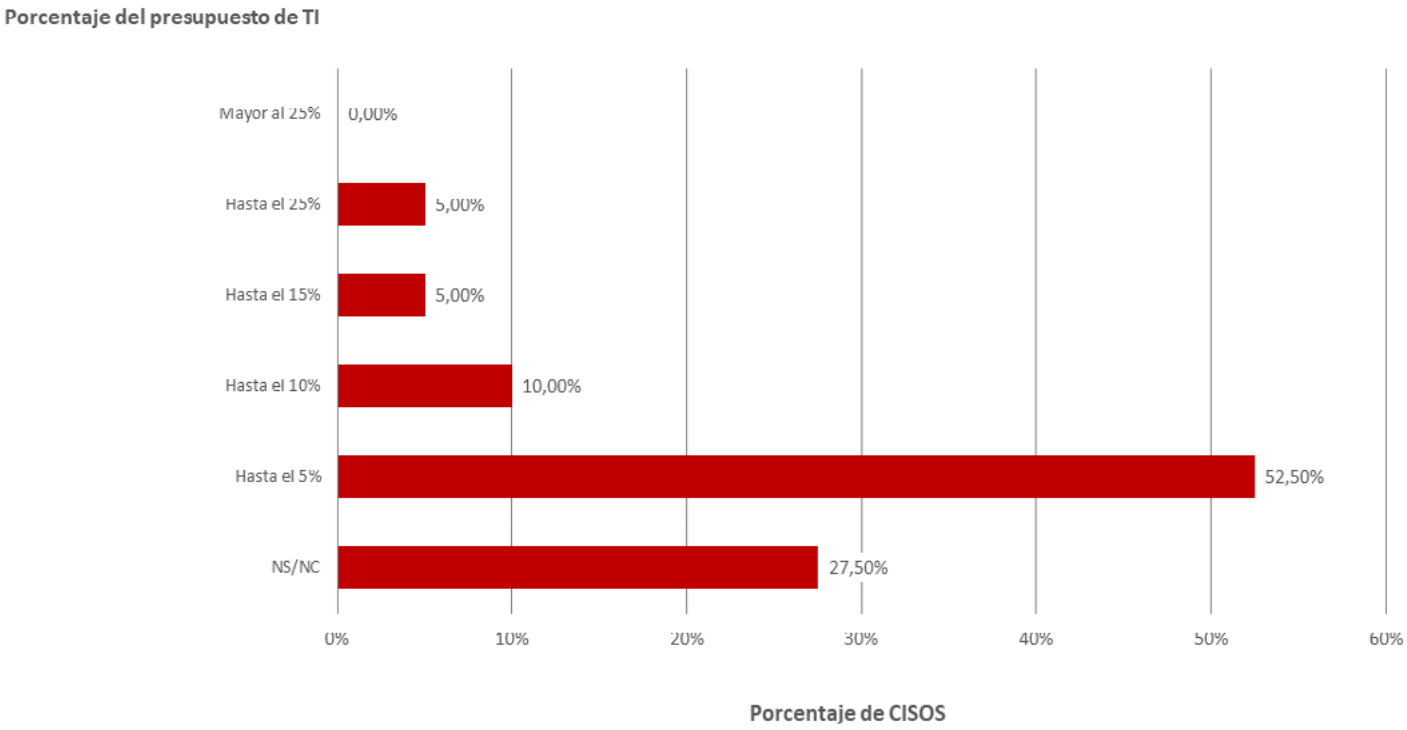
V.3.- Porcentaje respecto a TI

V.3.1.- ¿Qué porcentaje implica el presupuesto de su departamento

La inversión en Ciberseguridad ha crecido. La visión de "Coste operacional" que han tenido tradicionalmente las empresas hacia este sector, esta evolucionando hacia una consideración de "Inversión estratégica" independientemente del retorno de la inversión, de tal modo que los presupuestos de Ciberseguridad se están haciendo con un porcentaje creciente de la inversión TI. Este modelo ya esta presente en empresas de todos los tamaños, incluidas las pequeñas, donde los recursos son bastante escasos.

*The Vodafone Cyber Ready Barometer 2018
http://img.en25.com/Web/VodafoneGroupPLC/%7b1dd2abd4-17b9-4e81-9b23-347f2b41f338%7d_Vodafone-Cyber-Ready-Barometer-research-report-2018.pdf

No debemos pasar por alto que contar con una buena reputación en seguridad es muy positivo a la hora de que el negocio pueda ganar nuevos clientes. La implantación de tecnologías que aporten seguridad adaptada a las necesidades del negocio es la mejor opción para conseguirlo. A este respecto, se han publicado datos* de gran relevancia que ponen de manifiesto dicha tendencia, como el hecho de que el 48% de las empresas bien preparadas en términos de seguridad TI han conseguido un aumento de facturación de más del 5% del total.



VI. RESUMEN EJECUTIVO

VI.1.- Conclusiones principales

A continuación se exponen las ideas más relevantes que se han obtenido tras realizar el presente estudio:

- El tiempo dedicado a las funciones del CISO relacionadas con la Dirección estratégica y planificación, la Elaboración de políticas, y la Gestión de los presupuestos concuerda con la prioridad que se le da a las mismas. 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 encuestados, también son dos de las tareas que conllevan mayor implicación de tiempo por su parte.

- El tiempo dedicado a las funciones del CISO relacionadas con la Dirección estratégica y planificación, la Elaboración de políticas, y la Gestión de los presupuestos concuerda con la prioridad que se le da a las mismas. 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 encuestados, también son dos de las tareas que conllevan mayor implicación de tiempo por su parte.

- Para desarrollar el papel que desempeña el CISO en las organizaciones, es necesario tener en la misma medida conocimientos de negocio como técnicos. No obstante, menos del 15% de los encuestados identifica su trabajo o sus estudios con el área de negocio. Al tratarse de un rol bastante reciente, la gran mayoría de los CISOs provienen de áreas técnicas o de seguridad de la información.

- Según los encuestados casi el 80% de los CISOS considera que debería reportar siguiendo alguno de los modelos básicos de gobierno para su posición y reporte, como reportar directamente a la alta dirección o al COO/CRO/Comité de Dirección.

Más información en

isms forum spain

CSC Cyber Security Center

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.ismsforum.es

www.incibe.es/en