El Libro Blanco del CISO

Una iniciativa de

isms forum spain

CSC Cyber Security Center

Apoyo institucional

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

El Libro Blanco del CISO

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
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

I INTRODUCCIÓN Y CONTEXTO ACTUAL

I.1.- Tendencias y factores Externos.

El Foro Económico Mundial en su Informe Global de Riesgos del 2018 identifica dentro de los riesgos más preocupantes a nivel mundial por su probabilidad de ocurrencia e impacto a los ciberataques y al robo o uso fraudulento de los datos. Siendo por ello, una 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 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, 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.

Es por todo ello, por lo que 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 organizativa. 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 definir 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 recoge el rol y funciones del CISO del siglo XXI, como facilitador del negocio para alcanzar sus objetivos y aumentar su resiliencia.

I.2.- Marco normativo nacional 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.

El Anexo I incluye una lista detallada de referencias a leyes, reglamentos y normativas, tanto vigentes como en proyecto, referidos a la elaboración de este libro blanco.

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 (en adelante ENS) que, aprobado mediante Real Decreto 3/2010, 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.

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 encontramos 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 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 DE PROTECCIÓN 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 Datos (RGPD) es de ámbito europeo y, por tanto, aplicable en España donde 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.

Para referencias concretas, véase Protección de Datos en el Anexo I.

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 nivel común de seguridad de las redes y sistemas de información en la Unión y su correspondiente REAL DECRETO-LEY 12/2018, DE 7 DE SEPTIEMBRE, DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN.

La directiva NIS tiene como objetivo lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión Europea. Establece condiciones de seguridad para empresas y organismos que proporcionan 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 servicios de computación en la nube) y establece un sistema de notificación de

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.

Es importante destacar que el RD 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."

Para referencias concretas, véase Directiva NIS en el Anexo I.

Ley de Seguridad Privada.

La Ley 23/1992 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 penales, administrativas, laborales, tributarias, etc. existe la obligación de informar 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 malas prácticas, acciones deliberadas, ciberataques, etc. el CISO deberá asegurarse que existen políticas refrendadas por Asesoría Jurídica que avalen la legitimidad de la intervención de los activos informáticos de la empresa incluyéndose la intercepción de comunicaciones, inspección de ordenadores de empleados, inspección de correo electrónico para garantizar que dichas investigaciones sean legítimas.

En la actualidad, se encuentra en desarrollo el nuevo reglamento de seguridad privada dónde se incluyen expresamente referencias a las actividades de Seguridad Informática y Ciberseguridad.

Para referencias concretas, véase Ley de Seguridad Privada en el Anexo I.

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 Infraestructuras Críticas deben designar y comunicar tanto un CISO, como un CISO suplente.

Adicionalmente se crea la mesa de Ciberseguridad de Infraestructuras críticas.

La figura del CISO en este ámbito está totalmente en subordinación a la figura del Responsable de Seguridad y Enlace (este sí definido en la Ley) a la hora de relacionarse con la autoridad de control CNPIC.

Secretos comerciales.

La normativa de Protección de Secretos Comerciales obliga a las empresas a salvaguardar sus conocimientos técnicos y la información empresarial (no divulgados) contra su obtención, utilización y revelación ilícitas. La normativa es de ámbito europeo y, por tanto, directamente aplicable en España. Al igual que el resto de las directivas comunitarias, se ha de transponer en leyes nacionales en todos los países no pudiendo éstas en ningún caso contravenir sus disposiciones.

Para referencias concretas, véase Secretos Comerciales en el Anexo I.

Sector Financiero - Comercio.

Hay diversas directivas aplicables como Sarbanes-Oxley (SOX) (EEUU, pero extendida internacionalmente, que regula las funciones financieras contables y de auditoría y penaliza severamente el crimen corporativo), Basilea III, Directivas Europeas para el Crédito y la Expedición, Reglamentos Locales y Cuerpos Reguladores como Visa, MasterCard, AMEX.

Por otro lado, existe estándar de Seguridad de Datos para la Industria de Tarjeta de Pago que afecta principalmente al sector financiero y comercio en general dónde se transmita, procese o almacene información de tarjetas de crédito/debito. PCI-DSS define los requisitos mínimos de seguridad.

Respecto a los servicios de pago en la Unión Europea, es de obligado cumplimiento la directiva de servicios de pago (PSD 2) que tiene como objetivo crear un mercado único de pagos en la Unión Europea. Esta directiva conlleva cambios fundamentales en la industria al dar acceso a terceros a la infraestructura de los bancos.

Para referencias concretas, véase Sector Financiero-Comercio en el Anexo I.

Sector Juego.

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

- Ley de Regulación del Juego, al desarrollo de la misma y resoluciones técnicas relacionadas.

Para referencias concretas, véase Sector Juego en el Anexo I.

Sector Defensa.

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

- Ley de Secretos Oficiales. Su incumplimiento puede acarrear sanciones penales.

- 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)". Las normas e instrucciones SEGINFOEMP especifican 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 programas, proyectos o contratos del Ministerio.

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

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

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

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

- 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.

- Directivas de la Unión Europea. Son instrumentos jurídicos de que disponen las instituciones europeas para aplicar las políticas de la Unión Europea (UE). Constituyen un instrumento flexible que se emplea principalmente como medio para armonizar las legislaciones nacionales estableciendo obligaciones para los países pero dejándoles libertad respecto a los medios que hayan de aplicar para alcanzarlas.

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 re-exportada 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 Regulations. Regula la exportación de material militar.

- Normativa US EAR (Export Administration Regulation – regula la exportación de material de doble uso (militar/civil)

- Reglamento español de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.

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

Para referencias concretas, véase Export Control en el Anexo I.

II ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA

La seguridad de la información consiste en la protección de la información y los sistemas e infraestructuras informáticas donde se procesa, almacena y transmite, buscando mantener la confidencialidad, la disponibilidad e integridad de la información y la trazabilidad de acciones. El presente capítulo pretende identificar las actividades del CISO.

II.1.- Funciones del CISO.

El Responsable de Seguridad de la Información debe contar con la formación, la capacidad y experiencia necesaria para alinear la seguridad de las redes y sistemas de información de la empresa con los objetivos de Negocio. Esa protección de la información, de los productos y servicios de la empresa, lo hará en el desempeño de sus funciones y responsabilidades.

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 aquéllas que, en función del tipo de organización o madurez de esta, podrían recaer en otras áreas de la organización.

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

- Alinear la estrategia de seguridad de la información con los objetivos de la empresa.
- Definir la normativa de seguridad (Políticas, Normas y procedimientos) y velar por su cumplimiento.
- Gestionar los riesgos de seguridad de la información y establecer el plan de acción correspondiente.
- Velar e impulsar la identificación de requisitos 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).
- Supervisar el Nivel de seguridad, el cumplimiento de los controles y el grado de eficacia de las medidas aplicadas.
- Supervisar el cumplimiento de la legislación en los aspectos referidos a su ámbito de actuación.
- Interlocutar con la Alta Dirección en materia de seguridad de la información (métricas, reporting de riesgos, planes de acción, amenazas e incidencias)
- Interlocutar con otras empresas, instituciones, reguladores y Fuerzas y Cuerpos de Seguridad del Estado en materia de seguridad de la información.
- Formar, concienciar y sensibilizar a la organización en materia de seguridad de la información.
- Gestionar la operación de seguridad de la información, sea directa, a través de servicios externalizados o a través de otras áreas de la organización.
- Gestionar los incidentes de seguridad, sea directa, a través de servicios externalizados o a través de otras áreas de la organización.
- Prevenir el fraude, al menos el cometido a través de medios electrónicos.

Las funciones descritas anteriormente son responsabilidad del CISO en todos los casos, si bien, en función de cada entidad, puede ser delegada su ejecución a otros equipos.

II.2.- Actividades del CISO.

Para llevar a cabo estas funciones, son muchas las actividades que desarrolla el CISO, por lo que a continuación se desglosan las actividades que desarrollan las funciones del CISO.

Se ha tomado como marco de referencia el del NIST (National Institute of Standards and Technology), que es en la actualidad el más utilizado (existen otros marcos de control que servirían igualmente) si bien ampliándolo en unos casos y modificandolo en otros.

IDENTIFICAR

- Conocer el contexto de negocio.
- 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.
- Identificar los recursos necesarios (personal y presupuesto) para realizar la función de seguridad de la información adecuadamente.
- 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 derivados. En ocasiones, esta actividad cubrirá el total de gestión de riesgos de la organización.
- Identificar el nivel de riesgo aceptable para la Organización.
- Definir el Plan Estratégico de Seguridad y derivar los programas necesarios para llevarlo a cabo.

- 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, Riesgos, RRHH, etc.) y los stakeholders en general.

- Establecer los comités y grupos de trabajo necesarios para coordinar la seguridad de la información dentro de la compañía. Debería existir al menos 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.

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

PROTEGER

- Diseño e implantación de la arquitectura de seguridad.

- Seguridad en el dato/información.

- Seguridad en la infraestructura IT (perimetral, redes, servidores)

- Seguridad en dispositivos de usuario.

- Seguridad en entornos Cloud.

- Seguridad por defecto y en el diseño en aplicaciones (desarrollo seguro)

- Gestión proactiva de vulnerabilidades.

- Asegurar el cumplimiento normativo.

- Definir y participar en las actividades de formación y concienciación en Seguridad de la Información del personal de la Organización. Establecer los planes de concienciación y sensibilización a toda la organización.

- Supervisar (al menos) la seguridad y privacidad de los datos. En particular, esta función queda reforzada en tanto que el CISO ya dispone en gran medida de la cualificación y conocimientos que el RGPD requiere a la figura del DPD

DETECTAR

- Supervisión de las actividades de actualización permanente y corrección de errores en los sistemas de información de la organización, lo que incluye la realización de pruebas de penetración en los sistemas, seguimiento de actividades de parcheo y corrección de vulnerabilidades, inventario TI, etc.
- Monitorización y alertas sobre la actividad de personas, sistemas y aplicaciones.
- Monitorización activa sobre amenazas avanzadas (threat inteligence)
- Detección de activos no controlados/no corporativos.
- Detección de comportamiento normal, anomalías y desviaciones.
- Detección de ataques a la infraestructura/comunicaciones (DDoS).
- Elaboración de forenses.
- Participación en ciberejercicios (simulación ofensiva y respuesta).
- Threathunting.
- Defensa activa.

RESPONDER Y RECUPERAR

- Definir, implantar y encabezar la respuesta ante incidentes de seguridad de la información en la organización.
- Bloquear, contener, resistir y gestionar las crisis derivadas de un ciberataque.
- Denunciar ante las autoridades competentes un ciberataque.
- Realizar los informes periciales y defenderlos en sede judicial (si procede).
- Diseñar los playbooks de respuesta ante incidentes.
- 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.
- Supervisión de la continuidad de negocio de la organización, 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, Riesgos, 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.

También, cabe señalar que un CISO no debe participar de la ejecución de las operaciones en TI diarias, ni de la solución de las incidencias derivadas de la propia operación o de la merma de los activos TI por su propio uso.

Finalmente, destacaremos que es necesario que las Organizaciones definan no sólo el modelo de Organización y relacional del CISO, sino como parte de ese modelo deben establecer la segregación o no, de funciones de la seguridad de la información. Por ejemplo, el CISO puede marcar la estrategia y políticas e implementar los controles de seguridad (operar la seguridad) o bien segregar la función de estrategia, políticas y supervisión en el CISO y operar la seguridad desde otra área.

La segregación de funciones en materia de seguridad de la información es en muchos casos necesaria para poder asumir en el mismo responsable, roles diferentes, como puede ser aquel que ejerza de CISO y de Delegado de protección de Datos para una misma Organización.

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

La mera inspección de las actividades de un CISO revela que sus responsabilidades 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 en entornos no TI.

Así, algunas definiciones de la función de CISO realizadas en entornos y casuísticas particulares pecan de inexactitud, al reutilizar inadecuadamente una función ya existente en las organizaciones con una misión específica, a tal entorno y casuística particular. Por ejemplo, la definición hecha por CNPIC https://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630 y https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849, define como "CISO" una función de un especialista técnico TI que ya existe con otro nombre "responsable de gestión de vulnerabilidades".

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 que toda la organización tiene acceso a la información y maneja información en sus actividades y funciones. Las medidas de protección (TI y no TI) deben ser también transversales y deben ser aplicadas en toda la organización. Y debe ser tarea del CISO dirigir esta actividad en nombre y como miembro del Consejo de Administración de la organización, proporcionando la seguridad de la información que la organización necesite en cada momento para sus objetivos de negocio. A esto es a lo que se ha definido como "Seguridad Global" y que abarca todos los aspectos de la "SEGURIDAD".

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 su necesidad de esta figura hasta tiempos recientes. 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 terceros, 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 alinear los objetivos de seguridad de la información de la entidad con sus objetivos 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 queremos 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 evolucionando los departamentos de seguridad y su nombre.

Allá por los años 90 este departamento 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 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. A continuación, hubo un movimiento en el sentido de denominar a este departamento como seguridad perimetral, ya que en aquella época era donde se ponía el foco de protección. El CISO pasó 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.

Actualmente, se ha dado un paso adelante, incorporándose el CISO a los procesos de negocio de las organizaciones y, por tanto, esta figura ha dejado de dedicarse únicamente a tareas técnicas pasando a realizar labores de organización, coordinación, supervisión y definición de todos los aspectos de la Seguridad de la Información en la Organización.

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

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 información (principal activo) y ya no sólo en los sistemas que la tratan. Finalmente, el termino Ciberseguridad es que está calando en las Organizaciones y en la Sociedad.

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 "cross" (transversal) 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 tecnológicos 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 y medios incluyen:

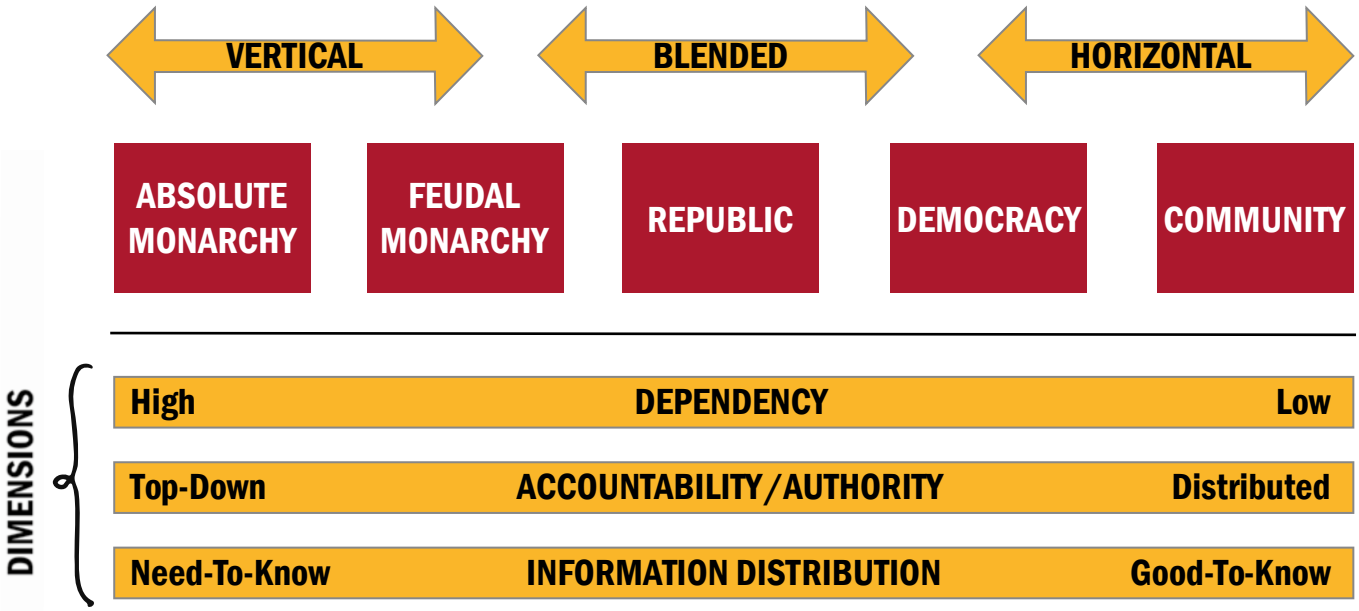
- La estrategia corporativa global.
- Políticas corporativas y sus respectivas normas, procedimientos y alineamientos.
- Planes estratégicos de acción-reacción y operativos.
- Sensibilización y capacitación.
- Administración de riesgos.
- Controles.
- Auditorías y otras actividades de aseguramiento.

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.

Los Gobiernos de Seguridad de la información forman parte de las responsabilidades del Gobierno Corporativo. La seguridad de la información no se concibe sin un sistema de gestión y un gobierno efectivo ya que los aspectos de las TI son transversales a toda la organización. Cualquier aspecto de mejora ha de abordarse de manera corporativa.

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 que tenga en consideración la legislación vigente y las regulaciones.

Es muy importante conocer cuáles son los grados de autoridad y responsabilidad, así como la interacción entre las distintas jerarquías de la organización.



A nivel general 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 el centro de datos 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: Elaborar Programa Seguridad acorde a los Requisitos Estratégicos.
• Gestión: Ejecuta el Programa de Seguridad (funciones, procesos y tácticas).
• Operación: Ejecuta los Procesos 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 reporting 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 reporte de la valoración periódica de su organización en términos del:

— Nivel de protección.

— Los mecanismos de vigilancia de que dispone.

— La preparación que tienen para dar respuesta y recuperar 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 reporte debe ser entendible, conciso y comparable.

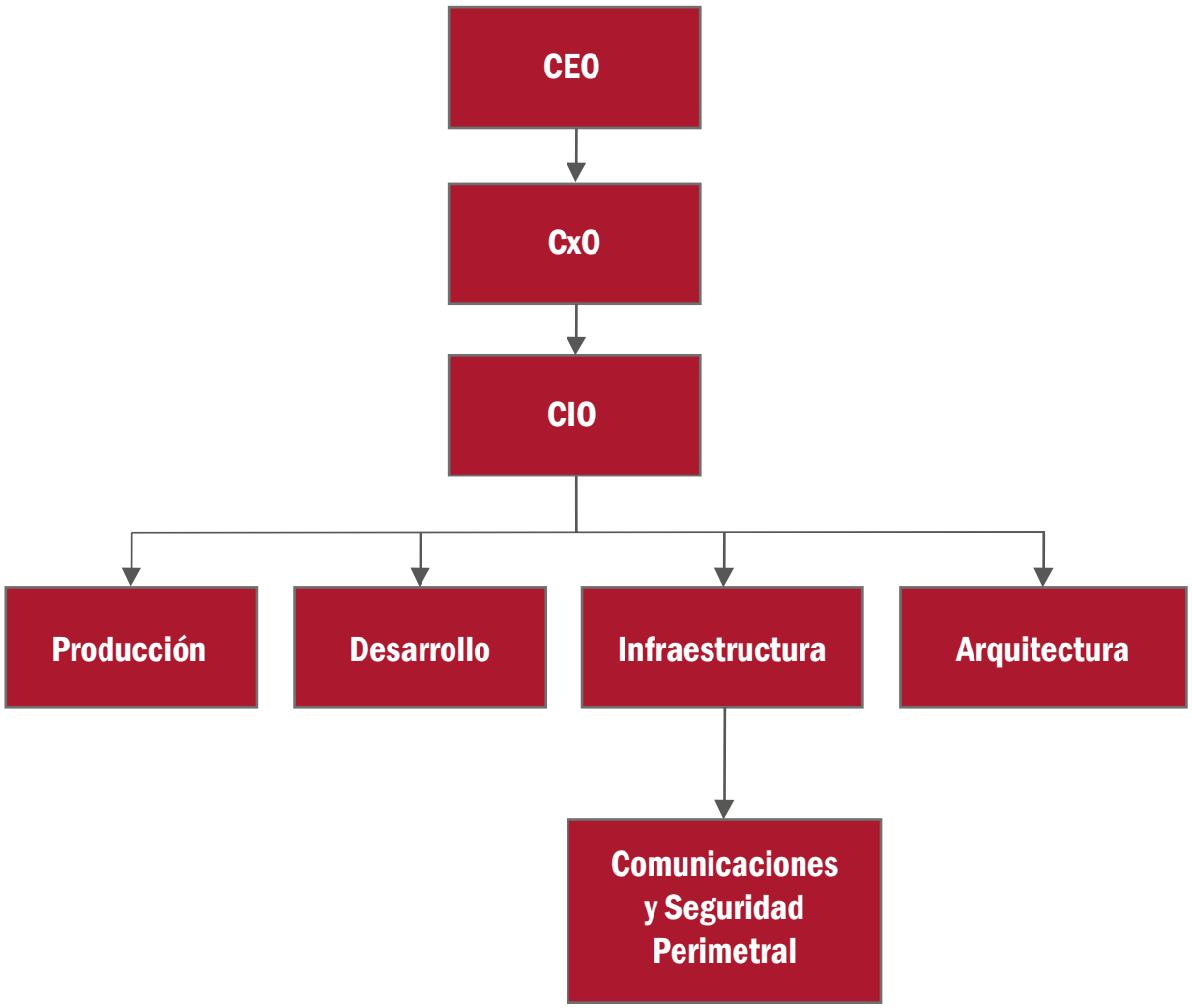
El conocimiento y la capacidad de acción de un CISO viene de una forma determinante impuesta por su ubicación en el Organigrama de la empresa y en su capacidad de influencia y concienciación.

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

IV MODELOS ORGANIZATIVOS Y RELACIONALES

IV.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 que todavía no consideran la seguridad de la información como un aspecto suficientemente importante como para dotarlo de personalidad propia. La figura del CISO, en este modelo, se considera como un administrador de los sistemas de seguridad.



Ventajas

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

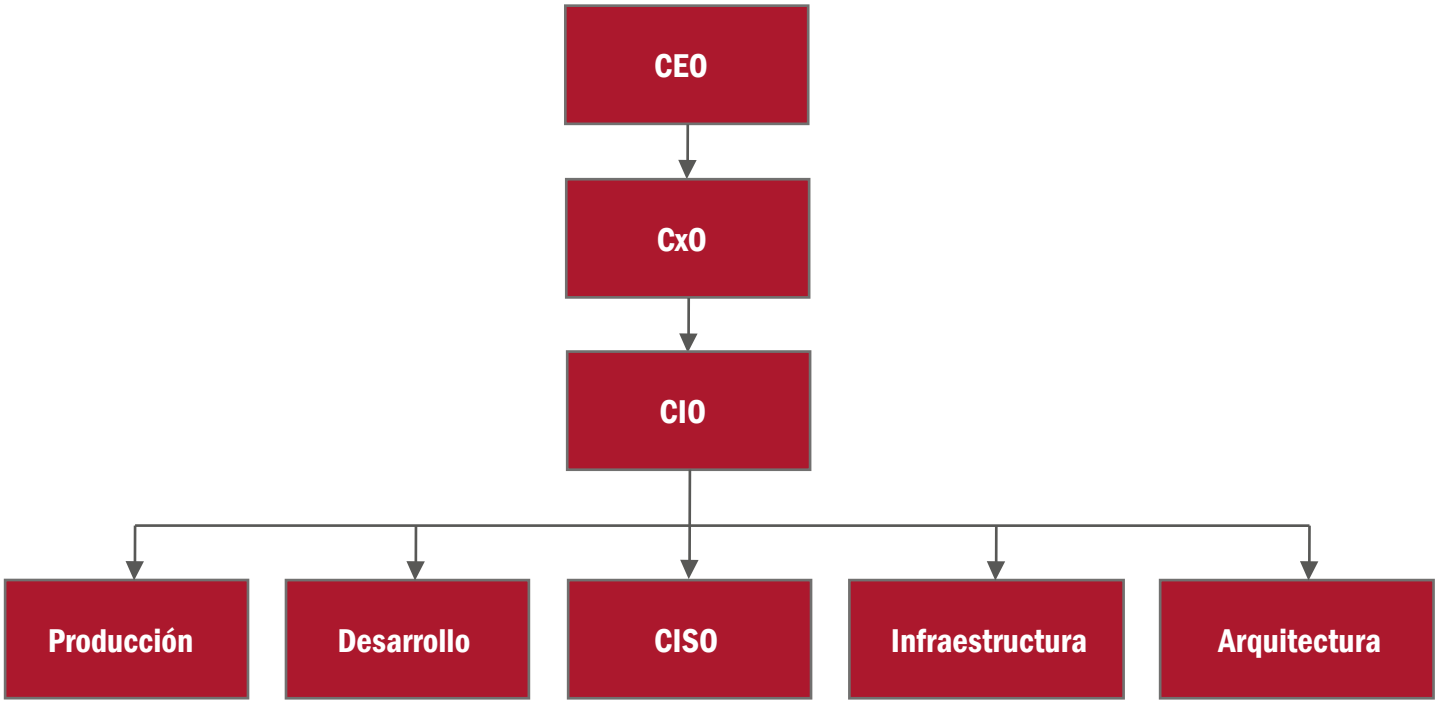
Inconvenientes

- Menor capacidad de decisión.
- Menor visibilidad.
- Posible conflicto de intereses.

IV.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.

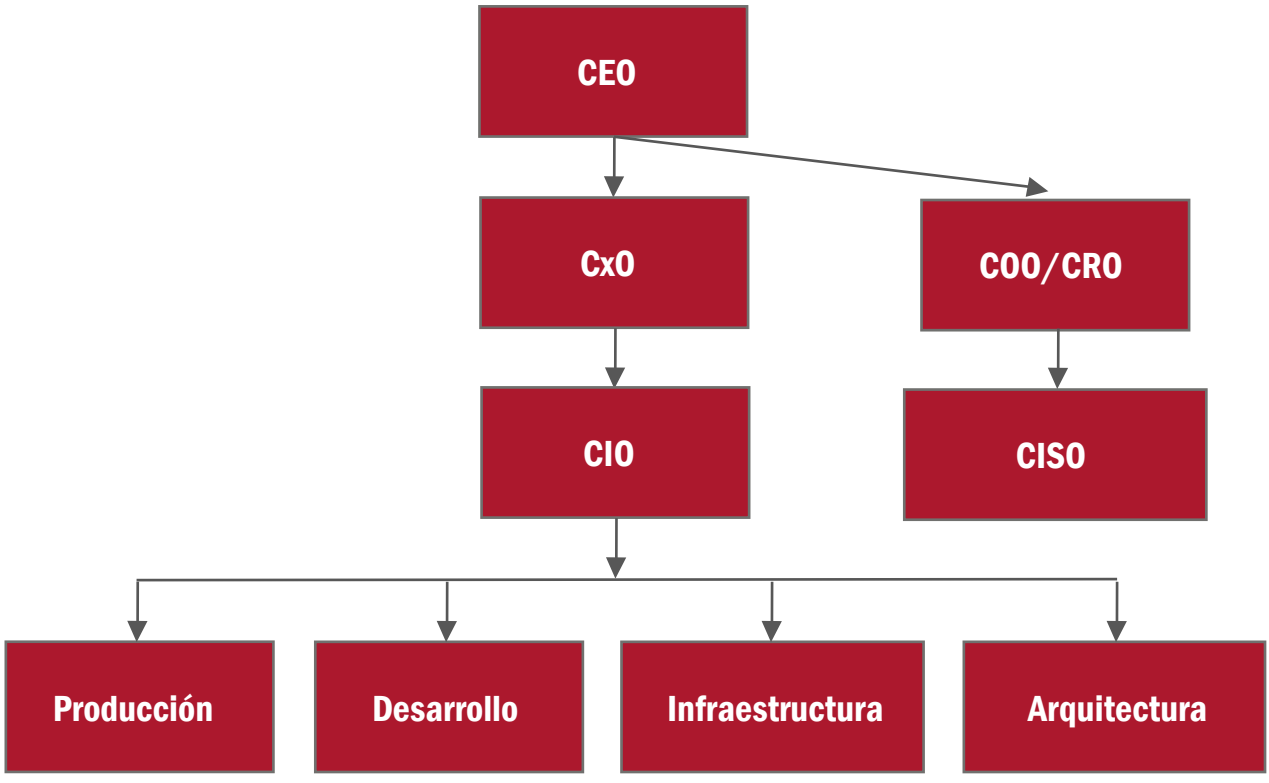
Inconvenientes

- Menor visibilidad.
- Posible conflicto de intereses.

IV.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.

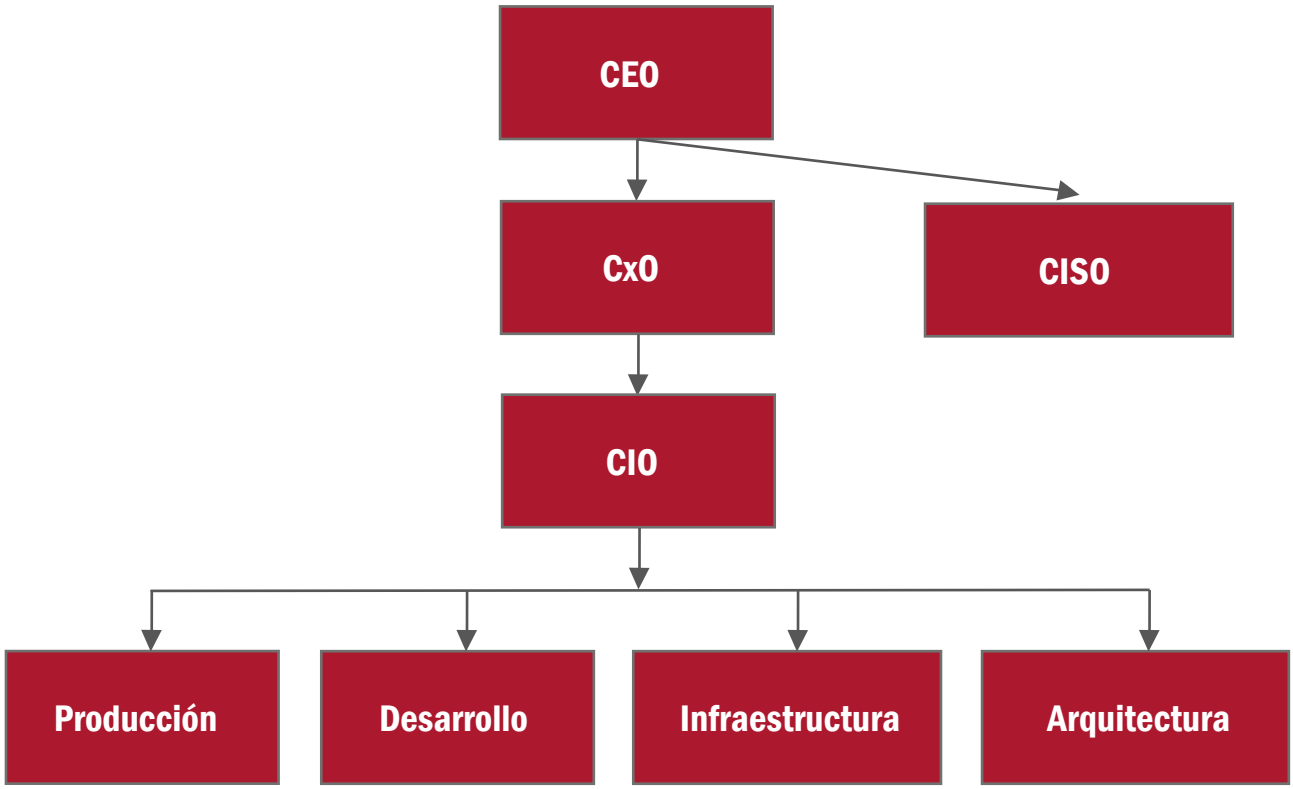
Inconvenientes

- 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 considerado un ejecutivo de alto nivel y, por tanto, pertenece al comité de dirección. 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.

Inconvenientes

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

IV.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 controles, 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 tecnológica (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).

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.

IV.6.- Características de un CISO.

El CISO es una posición a nivel ejecutivo cuya misión es proporcionar al órgano de gobierno de una compañía (normalmente comité de dirección) apoyo y asesoramiento experto en materia de seguridad de la información y protección 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 información 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 gestión 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.

IV.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 líneas 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/cybersecurity/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.

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.

IV.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 societaria
- 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 políticas 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.

IV.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 cobertura 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 pueden realizarse por medios tecnológicos, podrían recaer en el futuro por una misma persona o tratarse en un mismo departamento de "Seguridad 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".

V PERFIL DEL CISO

V.I. FORMACIÓN Y CAPACITACIÓN

En el capítulo II, apartado 1 describiendo las funciones del director de Seguridad de la Información se hace referencia los roles de CISO (figura el plano de la autoridad formal) y CTSO (responsable tecnológico de la seguridad en el terreno de la seguridad informática). 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) 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…) y estándares para la seguridad de la información (ISO 27001) que deberá trasponer a las 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).

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 es posible su intervención en incidentes con trascendencia legal por delegación de éste. 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, debería ser asesorado por éste y su equipo técnico especializado.

Si CISO y CTSO convergen en la misma persona el espectro de conocimiento del CISO es más amplio.

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.

- Formación en idiomas: el inglés es un elemento de trabajo casi imprescindible porque tanto publicaciones como foros, eventos, etc. se desarrollan 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. Certificación 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 Association - Asociación de Control y Auditoría de Sistemas de Información).

    - 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 autoritas, el reconocimiento del rol y su valor por parte de los demás; y la potestas, 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 conformará 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 presupuestos, instalaciones, operatividad de recursos, plazos, cumplimiento contractual, legislativo y normativo y dependerán en gran manera de él los riesgos 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 empresa, 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 organización. Las habilidades interpersonales (inteligencia emocional), la formalidad y el respeto son claves para un buen desempeño de su función y la delegación es un factor 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.

Por último, hay una característica que nunca debe faltar en cualquier persona 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 rectitud. La confianza –digamos- se tiene por defecto pero, si se pierde, nunca se recupera.

VI CONCLUSIONES

El rol del CISO como máximo responsable de seguridad de la información es cada vez más necesario en todas las entidades. La Transformación Digital, y la proliferación de marcos normativos en materia de seguridad de la información y comunicaciones lo están poniendo de manifiesto.

El rol del CISO es un rol Directivo, especializado en seguridad de la información, pero con las mismas atribuciones que el resto de directivos en sus áreas respectivas. Por tanto, es el máximo responsable de asesorar a la alta Dirección para orientar y dirigir la organización en 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 acordado.

El rol del CISO es sin embargo tan imprescindible como aun insuficientemente conocido o reconocido por la propia organización. Por ello, en el pasado se han tomado diversas decisiones de ubicación de la función de CISO en el organigrama que no explotan suficientemente la transversalidad del CISO, de sus conocimientos, de su visión, orientación ni la capacidad de aportación de valor a la organización. Una transversalidad de la función derivada de la transversalidad propia de la seguridad de la información, dado que las organizaciones son tan inseguras como la más insegura de sus partes. Por ello, el CISO debe conocer materias tan variadas como seguridad física, derecho de las Tecnologías, seguridad de las personas, detección y respuesta a incidentes, privacidad, continuidad de negocio, gestión de terceras partes, partiendo de un conocimiento central y profundo de 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. Una experiencia que no puede ser obviada para definir correctamente esta función.

Sirva este Libro Blanco para ayudar a la Administración a armonizar la función del CISO en su regulación y a las entidades a definir la función 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)**

ANEXO I - NORMATIVAS APLICABLES A LA FUNCIÓN DE CISO A FECHA DE 20 DE OCTUBRE DE 2018

Ley de Seguridad Privada

- Ley 5/2014, de 4 de abril, de Seguridad Privada
  https://www.boe.es/buscar/pdf/2014/BOE-A-2014-3649-consolidado.pdf

- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.
  https://www.boe.es/buscar/pdf/1995/BOE-A-1995-608-consolidado.pdf

- Nuevo borrador de reglamento disponible, que incluye expresamente referencias a la Seguridad Informática y Ciberseguridad.
  https://www.policia.es/actualidad/pdf/texto_borrador_seg_pri.pdf

Esquema Nacional de Seguridad

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos que establece el Esquema Nacional de Seguridad.
  https://www.ccn.cni.es/images/stories/normas/pdf/ley_11_2007_acceso_electronico_ciudadanos.pdf

- Real Decreto 3/2010, de 8 de enero, que aprueba el ENS.
  https://www.ccn-cert.cni.es/publico/ens/BOE-A-2010-1330.pdf

  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

- Real Decreto 951/2015, de 23 de octubre, que modifica el ENS.
  https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-11881

Protección de datos

- Reglamento (UE) 2016/679 (GDPR / RGPD). Por su naturaleza, directamente aplicable a todos los países de la UE, exista o no ley nacional.
  https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0943&from=en

- Proyecto de Ley Orgánica de Protección de Datos de Carácter. Personal.
  http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-3.PDF

- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
  https://www.boe.es/boe/dias/2018/07/30/pdfs/BOE-A-2018-10751.pdf

Secretos Comerciales

- Directiva (EU) 2016/943 (Trade Secrets)
  http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016L0943

- Anteproyecto de ley de secretos empresariales disponible, editada el 8 de febrero de 2018
  http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428696156?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DInformacion_publica_APL_secretos_empresariales_Texto.PDF

Directiva NIS

- Directiva (EU) 2016/1148 (NIS) aplicable a entidades que proporcionan servicios esenciales en concordancia con lo dispuesto en la ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Esta Directiva traspone las disposiciones de la 2008/114/CE, esencial para la cooperación en materia de infraestructuras críticas en el seno de la Unión Europea.
  https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

— Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257

— Legislación aplicable a los diferentes sectores y subsectores de infraestructuras críticas:
http://www.cnpic.es/Legislacion_Aplicable/index.html

Sector Financiero - Comercio

— Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago, PCI-DSS.:
https://es.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

— PSD 2. Servicios de pago. Directiva (EU) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015. En vigor desde el 12 de enero de 2016.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L2366&from=EN

Directiva sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n o 1093/2010 y se deroga la Directiva 2007/64/CE

— Ley Sarbanes-Oxley (SOX). Traducción al español de U.S. Congress Sarbanes-Oxley Act of 2002 U.S. InterAmerican Community Affairs:
http://interamerican-usa.com/articulos/Leyes/Ley-Sar-Oxley.htm

— Basilea III: marco regulador internacional para los bancos
https://www.bis.org/publ/bcbs189_es.pdf

Sector Juego

— Ley 13/2011, de 27 de mayo, de regulación del Juego y RD de desarrollo de la Ley del Juego (Real Decreto 1613/2011, de 14 de noviembre)
https://www.boe.es/buscar/act.php?id=BOE-A-2011-9280
https://www.boe.es/buscar/act.php?id=BOE-A-2011-17835

— 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)
https://www.boe.es/buscar/doc.php?id=BOE-A-2011-15092

— 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.)
https://www.boe.es/buscar/doc.php?id=BOE-A-2014-10302

Sector Defensa

Leyes y normativas nacionales

— Ley 9/1968, de 5 de abril, sobre secretos oficiales
https://www.boe.es/buscar/pdf/1968/BOE-A-1968-444-consolidado.pdf

— 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/estatal/290506_OM_Seg_Informacion.pdf
http://www.defensa.gob.es/portalservicios/servicios/industriadefensa/seginfoemp/

— 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/Instruccion_52_2013.pdf

— 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 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/Resolucion_DIGAM_Procedimientos_de_SEGINFOEMP.pdf

— Normas de la Autoridad Nacional para la protección de la información clasificada
https://www.cni.es/comun/recursos/descargas/DOCUMENTO_5_-_Normas_de_la_Autoridad.pdf

— Normativa y guías CCN-STIC del Centro Criptológico Nacional
https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html
Normativa de Seguridad (no todas son de dominio público)

Normativa de Seguridad OTAN

De especial relevancia:

— Documento C-M(2002)49
https://www.cni.es/comun/recursos/descargas/DOCUMENTO_21_-_Security_within_NATO_-_C-M49-COR1-12.pdf
y directivas asociadas:

- AC/35-D/2000 Directive on Personnel Security
http://www.dksi.bg/NR/rdonlyres/852F2C9E-7CC8-441B-A63A-4A456D42E59D/0/Personnel_SecurityAC35D2000REV7.pdf

- AC/35-D/2001 Directive on Physical Security
http://www.dksi.bg/NR/rdonlyres/9D0EE24C-86D9-4C90-8084-70F5BC14B03B/0/Physical_SecurityAC35D2001REV2.pdf

- AC/35-D/2002 Directive on Security of Information
http://www.dksi.bg/NR/rdonlyres/DA629957-ECB2-40D6-9094-0F20396E5780/0/Information_SecurityAC35D2002REV4.pdf

- AC/35-D/2000 Directive on Personnel Security
  http://www.dksi.bg/NR/rdonlyres/852F2C9E-7CC8-441B-A63A-4A456D42E59D/0/Personnel_SecurityAC35D2000REV7.pdf

- AC/35-D/2001 Directive on Physical Security
  http://www.dksi.bg/NR/rdonlyres/9D0EE24C-86D9-4C90-8084-70F5BC14B03B/0/Physical_SecurityAC35D2001REV2.pdf

- AC/35-D/2002 Directive on Security of Information
  http://www.dksi.bg/NR/rdonlyres/DA629957-ECB2-40D6-9094-0F20396E5780/0/Information_SecurityAC35D2002REV4.pdf

- AC/35-D/2003 Directive on Industrial Security
  http://www.dksi.bg/NR/rdonlyres/47AC8675-F285-4812-B6FC-761D1B0D97CB/0/AC35D2003REV5.pdf

- AC/35-D/2004 Primary Directive on INFOSEC
  http://www.dksi.bg/NR/rdonlyres/6DC49C44-5C52-47A2-8773-6BF11C59E53C/0/Primary_CIS_SecurityAC35D2004REV3.pdf

- AC/35-D/2005 INFOSEC Management Directive for CIS
  https://www.nbu.cz/download/pravni-predpisy---nato/AC_35-D_2005-REV3.pdf

Normativa OCCAR

http://www.occar.int/occar-rules

Normativa ESA

ESA Security Regulations
https://download.esa.int/docs/eso/esa-reg-004e.pdf

Normativa LoI/FA EDIR (Letter of Intent / Framework Agreement for European Defence Industrial Restructuration)

https://www.gov.uk/guidance/letter-of-intent-restructuring-the-european-defence-industry
https://www.gov.uk/government/publications/letter-of-intent-sub-committee-3

Export Control

Estados Unidos de América

— Normativa US ITAR (Part 130)
https://www.pmddtc.state.gov/regulations_laws/documents/official_itar/2016/ITAR_Part_130.pdf

— Normativa EAR
US. Export Administration Regulation (EAR)
https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

Europa

— Normativa de doble uso de la Unión Europea, aplicable para todos los países miembros.
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1527179601283&uri=CELEX:02009R0428-20171216

España

— Real Decreto 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.
https://www.boe.es/boe/dias/2014/08/26/pdfs/BOE-A-2014-8926.pdf

Alemania

— Ordenanza Alemana de comercio exterior y pagos (Außenwirtschaftsverordnung,
http://www.gesetze-im-internet.de/englisch_awv/index.html),
aplicable para armas, munición y artículos de defensa así como bienes de doble uso bajo control nacional.

— Acto de control de armas de guerra (Kriegswaffenkontrollgesetz, KrWaffKontrG)
https://germanlawarchive.iuscomp.org/?p=741

— Véase también:
http://www.bafa.de/EN/Foreign_Trade/Export_Control/export_control_node.html

Francia

- Control de bienes de doble uso:
  http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/desarmement-et-non-proliferation/la-france-et-le-controle-des-exportations-sensibles/article/controle-des-biens-et-technologies

- Control de material bélico:
  http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/desarmement-et-non-proliferation/la-france-et-le-controle-des-exportations-sensibles/article/controle-des-exportations-de-materiels-de-guerre

- Sistema Online de licencias (EGIDE):
  http://www.entreprises.gouv.fr/biens-double-usage/procedures-et-licences-et-circuit

Reino Unido

- Export Control Act 2002, Export Control Order 2008 y corrección 2010
  https://www.legislation.gov.uk/ukpga/2002/28/pdfs/ukpga_20020028_en.pdf
  http://www.legislation.gov.uk/uksi/2008/3231/pdfs/uksi_20083231_en.pdf
  http://www.legislation.gov.uk/uksi/2008/3231/pdfs/uksics_20083231_en.pdf

Una iniciativa de

Apoyo institucional

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Más información en

isms forum spain

CSC Cyber Security Center

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

www.ismsforum.es

www.incibe.es/en