INCIBE

Libro Blanco del CISO

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
- Apoyo de la Alta Dirección, con una definición clara de ámbitos y responsabilidades.

2

ACTIVIDADES DE SEGURIDAD I

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.

3

ACTIVIDADES DE SEGURIDAD II

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.

4

ACTIVIDADES DE SEGURIDAD III

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).

5

ACTIVIDADES DE SEGURIDAD IV

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.

6

ACTIVIDADES DEL CISO – IDENTIFICAR I

- 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 derivados. En ocasiones, esta actividad cubrirá el total de gestión de riesgos de la organización.

7

ACTIVIDADES DEL CISO – IDENTIFICAR II

- Identificar el nivel de riesgo aceptable para la Organización; es decir que umbral de riesgo está 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, Riesgos, RRHH, etc.) y stakeholders relacionados.
- 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. 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.

8

ACTIVIDADES DEL CISO – **PROTEGER**

- Diseñar e implantar 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 los 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).

9

ACTIVIDADES DEL CISO – DETECTAR

- Supervisar 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.
- Monitorizar y gestionar alertas sobre la actividad de personas, sistemas y aplicaciones.
- Monitorizar sobre amenazas avanzadas (threat inteligence) así como detectar activos no controlados/no corporativos.
- Detectar 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 respuesta).
- Ejecutar acciones de threat hunting (búsqueda proactiva de amenazas avanzadas en redes internas que evaden las medidas de protección habituales).
- Establecer medidas de defensa activa.

10

ACTIVIDADES DEL CISO – 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.

11

ACTIVIDADES DEL CISO – INFORMAR Y COORDINAR

- 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 Corporativos, Comunicación, Recursos Humanos.
- Coordinarse con otros centros de respuesta a incidentes.
- Colaborar en grupos de interés en esta materia

12

El CISO como Directivo

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).

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.