22/06/2023

Roles en ciberseguridad: desde el CEO a los usuarios finales

La**seguridad de la información** se ha convertido en una cuestión esencial para la continuidad de negocio de las empresas.

Es por ello que es imprescindible contar con un equipo de seguridad especializado que se encargue de proteger los activos en línea de las empresas y de concienciación en ciberseguridad para todos los empleados de la empresa.

En este ámbito, aparecen diferentes roles y equipos, cuyos nombres, en ocasiones, pueden crear confusión. A continuación, conoceremos cada uno de ellos, además de las funciones y responsabilidades que les corresponden en materia de ciberseguridad.

CEO

El **CEO** *(Chief Executive Officer)* es el **cargo más alto** dentro del organigrama de la empresa.

En cuanto a la ciberseguridad, **el papel del CEO es crucial** para la protección de la empresa e implementación de una cultura de concienciación en este ámbito, y debe colaborar con el resto de los líderes para asegurar la defensa de la información y de los activos digitales de la organización.

Además, deberá garantizar los recursos adecuados para implementar dicha estrategia: contratación del personal experto en ciberseguridad, implementación de herramientas y formación en ciberseguridad para todos los empleados.

CSO

El **CSO** *(Chief Security Officer)*, también denominado **responsable de seguridad corporativa**, es el responsable de la seguridad de la empresa, **tanto física como tecnológica**. Este rol es habitual en las grandes corporaciones, principalmente en el sector bancario y energético.

CISO

El **CISO** *(Chief Information Security Officer)* es el responsable de la **seguridad de la información** de la empresa. En algunas empresas, sobre todo en las más pequeñas, esta figura puede coincidir con la del CSO pero, aunque ambos roles están relacionados, tienen algunas diferencias. De hecho, la «I» de «información» en su nombre marca la diferencia principal, **centrando la responsabilidad del CISO en la seguridad de la información** en concreto. Algunas de sus funciones son:

- **Desarrollar y gestionar la estrategia de seguridad de la información de la empresa.**
- **Identificar y gestionar los riesgos de seguridad de la información.**
- **Desarrollar, implementar y supervisar las políticas de ciberseguridad alineadas con la misión y visión de la empresa**
- **Coordinar el equipo de ciberseguridad de la empresa.**
- **Fomentar la concienciación de todos los empleados en ciberseguridad.**

La formación básica que se requiere habitualmente para trabajar como CISO son estudios de ingeniería informática, telecomunicaciones o similares, partiendo de la base de que se tienen sólidos conocimientos en ciberseguridad.

Por otro lado, deberá contar con otro tipo de habilidades denominadas soft skills, como: contar con visión empresarial, estar al tanto de las últimas tendencias tecnológicas empresariales, capacidad de oratoria y persuasión y manejo de trabajo multidisciplinario.

En los últimos años, su papel dentro de la empresa ha evolucionado de ser un perfil técnico a un perfil involucrado en la estrategia empresarial de la empresa, con el objetivo de alinear la gestión empresarial con la ciberseguridad.

Este objetivo permite conseguir un mayor nivel de ciber resiliencia en las organizaciones.

Cabe destacar que, la imposición del RD 43/2021 dota al **CISO** de una condición de eje central de la ciberseguridad de las empresas. Dicho marco legislativo establece las atribuciones que tiene la figura del CISO, remarcando su valor como figura reguladora de la ciberseguridad de las organizaciones.

Algunos de los**beneficios** de contar con este perfil en la empresa son:

- **Planificación de ciberseguridad acorde a las necesidades y labores de la organización.**
- **Mejor sensibilización y formación laboral acerca de temas de seguridad digital.**
- **Capacidad de investigación y análisis de amenazas como brechas de seguridad.**
- **Mayor conocimiento de las tendencias en riesgos y mayor protección ante estos.**
- **Mejoría de la imagen de la empresa por contar con especialistas que dotan de confianza a los clientes y accionistas.**
- **Aseguramiento del cumplimiento normativo y de los estándares y regulaciones de seguridad de la información.**
-

CIO

El **CIO** *(Chief Information Officer)* es el líder de la **tecnología de la información** de una empresa. Su responsabilidad es asegurar la efectividad de la tecnología de la información de la empresa. También es un rol que ha evolucionado por la transformación digital acelerada de los últimos años, dando lugar a una posición del CIO más estratégica que en el pasado.

Entre sus funciones se encuentran:

- **Gestionar la estrategia TI de la empresa**, incluyendo la adopción de tecnologías emergentes y soluciones tecnológicas innovadoras con el objetivo de mejorar la gestión empresarial apuntando hacia la transformación digital del negocio.
- **Supervisar los proyectos TI y mentorizar al resto de responsables** de la empresa en la adopción de nuevas tecnologías.
- **Garantizar la seguridad de la información** junto con el CISO.

CTO

El **CTO** *(Chief Technology Officer)* es el responsable de la **tecnología** y la **innovación** de la empresa. Es el responsable de desarrollar la estrategia tecnológica de la empresa, y de impulsar el crecimiento tecnológico de la misma. Va muy alineado con la función del CIO, pero con un perfil más técnico. Sus funciones pueden estar entremezcladas, siendo algunas de ellas:

- **Planificar y desarrollar la estrategia TI** de la empresa junto al CIO.
- **Investigar y desarrollar** nuevos avances y tendencias tecnológicas.
- **Gestionar** los proyectos tecnológicos.
- **Garantizar** la seguridad tecnológica.

CDO

El **CDO** *(Chief Data Officer)* es el encargado de asegurar el correcto **tratamiento de los datos** dentro de la empresa, es decir, se encarga de garantizar la **protección de los datos** y de que se cumpla con las leyes y regulaciones correspondientes al tratamiento de datos. Algunas de sus funciones son:

- Gestionar la seguridad y privacidad de los datos, junto con el CISO.
- Gestionar y analizar los datos de la empresa para obtener información.
- Establecer e implementar la estrategia de datos de la empresa.
- Asegurar el cumplimiento en materia de protección de datos.

HACKER ÉTICO

Es un perfil novedoso para las pymes que complementa al equipo de ciberseguridad, fortaleciendo las capacidades de ciberseguridad de la empresa, asesorando, haciendo pruebas y tests de penetración para anticipar la identificación de vulnerabilidades, amenazas y riesgos de todos los departamentos de la empresa. Puede ser un perfil interno o subcontratado.

DPD

El **DPD** *(Data Protection Officer)* o delegado de privacidad asegura el cumplimento de la normativa en protección de datos.

Puede ser una figura interna, externa o compartida entre más empresas.

Para las pymes y autónomos, la Agencia Española de Protección de Datos ha elaborado la herramientaFACILITA GRPD y ha puesto a disposición de las empresas más recursos para el cumplimiento de la protección de datos de cada empresa.

Equipo de concienciación en ciberseguridad

Siguiendo las recomendaciones deENISA - Awareness raising in a box para implementar una**estrategia de concienciación en ciberseguridad** en una empresa, se identifican los siguientes roles que deben conformar el equipo de concienciación en ciberseguridad. Todos ellos son igual de importantes y satisfacen diferentes necesidades y funciones durante el ciclo de vida la estrategia de concienciación en ciberseguridad:

Responsable de ciberseguridad: ejecutivo de alto nivel encargado del desarrollo e implementación del programa de seguridad de la información.

Responsable de comunicación: encargado de transmitir los conocimientos al resto de empleados, así como de dar difusión a los logros y avances en materia de ciberseguridad.

Responsable de tecnología de sistemas de la información: con capacidad de desarrollar, implementar y mantener sistemas a gran escala para asegurar la correcta continuidad de las organizaciones.

Responsable del equipo de respuesta a incidentes: con capacidad para prevenir, detectar y responder resolutivamente a los incidentes de seguridad que puedan ocasionarse en los sistemas informáticos.

Responsable de recursos humanos: dedicado al diseño de los puestos de trabajo, así como sus funciones, responsabilidades, cualificaciones y habilidades requeridas.

La **colaboración** de todos estos roles es esencial para el correcto funcionamiento de la seguridad en la empresa.

Cumplir con las políticas y buenas prácticas desarrolladas por los roles descritos anteriormente y aplicar la formación en ciberseguridad es fundamental para todos los **empleados** de una empresa.

Como hemos visto, la colaboración entre los diferentes **roles** y la concienciación de los empleados es vital para la seguridad de la empresa. Los equipos deben trabajar en línea con los responsables de la seguridad para crear una **cultura de ciberseguridad** en la empresa, donde esta sea prioritaria.

Fuente: Incibe.es

LINK DE LA NOTICIA