**Realiza un trabajo sobre los roles profesionales relacionados con la seguridad. Contenido y extensión a criterio del alumnado.**

La ciberseguridad es una de las principales preocupaciones de las empresas de todo el mundo, y más cuanto más digital sea. Lo que nos trae la transformación digital son empresas con poca experiencia en temas de seguridad que, de repente, sin saberlo, se convierten en objetivo de los delincuentes.



Por ese motivo es muy importante que haya una buena estructura, ya sea dentro de la empresa, o subcontratando servicios, que haga frente a los retos de seguridad. Estos retos son cada día más y están más avanzados, así que hay que ponerse manos a la obra

Para facilitar las cosas, voy a recopilar los principales roles de ciberseguridad actuales. De esta manera se puede consultar en cualquier momento qué papel juega cada uno de ellos, cuáles son sus tareas o áreas de responsabilidad, y quienes son los imprescindibles en cualquier empresa. Empezamos con los perfiles más directivos, para pasar luego a los perfiles técnicos.

**ÍNDICE**

[Roles profesionales en ciberseguridad 2](#_55quiq5r7vfv)

[**CISO 3**](#_sq4wulbn1lf6)

[**CSO 3**](#_mfa7u2gfk14g)

[**CTO 3**](#_bfeoglslo2mm)

[**CIO 3**](#_9zwrt0e3pm6l)

[**DPO 4**](#_3sbzi1ua1g6l)

[**Arquitecto de ciberseguridad 4**](#_cp7g3m2e61gh)

[**Analista de seguridad 4**](#_ncv4q4xxdmbr)

[**Informático Forense 4**](#_5b42w2fcu0sy)

[**Hacker 5**](#_j7m3oyl56tf)

[**Analista de Inteligencia de Amenazas 5**](#_app05zi7zzw4)

[**DevSecOps (Development, Security, Operations) 5**](#_7k642o8wa9yp)

[**Administrador de Identidad y Acceso 5**](#_sipz3umgkcax)

[**Ingeniero de Red Segura 6**](#_qgixhmsexuj8)

[Importancia y Campos de Trabajo 6](#_zbgnfig9wtel)

[Un papel vital en la protección digital 7](#_q1r1md11rwwj)

## **Roles profesionales en ciberseguridad**



# **CISO**

El Chief Information Security Officer, o CISO, sería el director de ciberseguridad. Es decir, es el responsable máximo de la estrategia de ciberseguridad corporativa desde la fase de planificación, pasando por su desarrollo, ejecución y el control. Como cargo directivo tiene a su cargo a los perfiles técnicos, y ha de comunicar a otros directores o al departamento que corresponda, todas las acciones y logros en ciberseguridad. A veces, se debe reportar directamente al CEO. Se trata de un cargo que combina el mundo técnico y el de negocio, y desarrolla la titánica tarea de comunicar y hacer ver a la dirección de la empresa que la ciberseguridad es rentable.

# **CSO**

El Chief Security Officer, o CSO, es otro cargo directivo que, a veces, se confunde con el CISO (o, directamente, son la misma persona en empresas pequeñas). El CSO es el responsable de la seguridad de la organización. Debe tener visión de negocio; comprender los riesgos que afronta la organización y cómo tratarlos; establecer planes de continuidad y recuperación ante desastres y muchas otras funciones importantes.

# **CTO**

Este es el perfil responsable de implementar las nuevas tecnologías dentro de la empresa, así que debe colaborar con el CISO y trabajar conjuntamente con él para asegurar la protección de los datos en el manejo de dichas tecnologías.

# **CIO**

El Chief Information Officer (CIO) es el director de tecnología de la información y asegura que las estrategias de TI estén alineadas con los objetivos de la organización. Este rol se centra en garantizar que los recursos tecnológicos estén disponibles y sean eficientes, además de trabajar en conjunto con el CISO y el CTO para fortalecer la seguridad de los sistemas.

# **DPO**

El Data Protection Officer (DPO) es el encargado de garantizar el cumplimiento de las normativas legales sobre protección de datos, como el Reglamento General de Protección de Datos (RGPD). Aunque no es el responsable del tratamiento de los datos, el DPO asesora sobre las mejores prácticas y crea una cultura de protección de datos dentro de la empresa. Es un rol crucial para garantizar la privacidad y la seguridad de los datos personales.

# **Arquitecto de ciberseguridad**

El arquitecto de seguridad es el responsable de crear las estructuras de seguridad complejas y hacer que funcionen. Se suele decir (acertadamente) que un buen arquitecto debe pensar como un hacker o, si somos más precisos, como un ciberdelincuente, para así adelantarse a cualquier posible ataque.

# **Analista de seguridad**

El analista de seguridad de la información es un rol importante en la ciberseguridad. Su principal responsabilidad es identificar y evaluar las vulnerabilidades en los sistemas, redes y aplicaciones de una organización. Utilizan técnicas de monitoreo y análisis para detectar intrusiones y asegurarse de que se tomen medidas correctivas. Además, desarrollan políticas y procedimientos de seguridad, así como también brindan capacitación y concienciación a los empleados sobre buenas prácticas de seguridad.

# **Informático Forense**

Como su propio nombre sugiere, el informático forense lo va a saber todo acerca de adquirir, preservar, obtener y presentar datos que hayan sido procesados y guardados en soportes digitales. Con sus conocimientos va a poder desentrañar el origen, las consecuencias principales e, incluso, las motivaciones de un ciberataque.

# **Hacker**

El término hacker se suele utilizar mal cuando se usa como sinónimo de ciberdelincuente, pero nada más lejos de la realidad. Los hackers son piezas clave en la ciberseguridad porque son perfiles muy técnicos capaces de encontrar cualquier brecha, fisura o debilidad en un sistema… y comunicarlo, así como dar las posibles soluciones para eliminar esos riesgos.

# **Analista de Inteligencia de Amenazas**

El analista de inteligencia de amenazas recopila y analiza información sobre posibles ataques cibernéticos. Su trabajo ayuda a las empresas a anticiparse a las amenazas y diseñar estrategias de protección más eficaces. Este rol requiere conocimientos avanzados sobre tácticas y herramientas utilizadas por los atacantes.

# **DevSecOps (Development, Security, Operations)**

El DevSecOps integra la seguridad en el ciclo de vida del desarrollo de software. Este rol combina habilidades de desarrollo, operaciones de TI y ciberseguridad para garantizar que las aplicaciones sean seguras desde su creación. La filosofía DevSecOps promueve la colaboración entre equipos y la automatización de procesos de seguridad.

# **Administrador de Identidad y Acceso**

El administrador de identidad y acceso es responsable de gestionar quién tiene acceso a los recursos de la organización. Este rol garantiza que solo las personas autorizadas puedan acceder a sistemas y datos, utilizando tecnologías como autenticación multifactor y políticas de control de acceso.

# **Ingeniero de Red Segura**

El ingeniero de red segura diseña y mantiene infraestructuras de red robustas. Implementa tecnologías como firewalls, VPNs, segmentación de red y sistemas de detección de intrusos para proteger las comunicaciones y datos de la organización.

## **Importancia y Campos de Trabajo**

La importancia de los roles profesionales en ciberseguridad radica en la protección de los datos confidenciales, la prevención de brechas de seguridad y la mitigación de riesgos cibernéticos. Estos profesionales desempeñan un papel crucial en la protección de la integridad de los sistemas y la privacidad de la información. Trabajan en una amplia gama de campos, que incluyen:

* **Empresas y organizaciones gubernamentales:** Los roles profesionales en ciberseguridad son esenciales para proteger la información confidencial de las empresas y los datos gubernamentales sensibles
* **Instituciones financieras:** El sector financiero maneja grandes cantidades de datos financieros y personales, lo que lo convierte en un objetivo atractivo para los ciberdelincuentes. Los profesionales en ciberseguridad son fundamentales para garantizar la protección de los activos financieros y la confidencialidad de los clientes
* **Sector de la salud:** Las instituciones de atención médica manejan registros médicos electrónicos y otra información sensible. Los profesionales en ciberseguridad ayudan a proteger esta información y asegurarse de que cumpla con los estándares de privacidad y seguridad

## **Un papel vital en la protección digital**

Los roles profesionales en ciberseguridad desempeñan un papel vital en la protección contra las amenazas cibernéticas en el mundo actual. Cada uno de estos roles tiene responsabilidades y áreas de enfoque únicas, pero todos comparten el objetivo común de garantizar la seguridad de los sistemas y la información confidencial. Los analistas, ingenieros, consultores y administradores de seguridad desempeñan funciones clave en la identificación de vulnerabilidades, la implementación de soluciones de seguridad, la evaluación de riesgos y la gestión diaria de las políticas de seguridad.



En un entorno digital cada vez más interconectado, la demanda de profesionales en ciberseguridad está en constante crecimiento. La importancia de estos roles radica en la protección de los datos, la prevención de brechas de seguridad y la mitigación de riesgos cibernéticos en diversos campos, como empresas, instituciones financieras y el sector de la salud.

Si estás interesado en una carrera en ciberseguridad, es esencial adquirir habilidades y conocimientos especializados en áreas como análisis de seguridad, diseño de soluciones, consultoría y gestión de políticas. Además, mantenerse actualizado sobre las últimas tendencias y amenazas en ciberseguridad es fundamental para ofrecer una protección efectiva.