



Cyber Incident Responder



¿Cuál es su papel en las organizaciones?

¿Qué hace?



Se ocupa de monitorizar el estado de la ciberseguridad de las organizaciones y de gestionar los incidentes cibernéticos, a fin de preservar la protección y el funcionamiento de los sistemas de información.

Misión



El *Cyber Incident Responder* tiene como objetivo monitorizar los sistemas de defensa de las organizaciones en aras de detectar, analizar y evaluar los incidentes de ciberseguridad y así, mitigar su impacto. Además, es el responsable de restablecer el funcionamiento de los sistemas y procesos, además de registrar todas las acciones aplicadas para ello. También, se encarga de recopilar las evidencias de lo sucedido, fase necesaria para identificar el origen de los incidentes, y a las personas implicadas.

Entregables



Plan de respuesta a incidentes.
Reporte de incidentes de ciberseguridad.

¿Qué necesita?

Habilidades

- Conoce y pone en práctica todos los aspectos relacionados con la gestión y respuesta a incidentes de ciberseguridad.
- Recopila y analiza los datos de los incidentes, identificando patrones y tendencias.
- Conoce en profundidad los diferentes tipos de incidentes de ciberseguridad y las amenazas que ponen en riesgo a las organizaciones.
- Trabaja con servidores, servicios nube, sistemas operativos y otras infraestructuras.
- Trabaja en la resolución de problemas y en la toma de decisiones bajo presión.
- Gestiona y analiza los *log files* o archivos de registro.
- Comunica e informa a las partes interesadas sobre los resultados de los análisis.

