Escenario

Analiza el siguiente caso.

Eres un analista de ciberseguridad que trabaja para una empresa multimedia que ofrece servicios de diseño web, diseño gráfico y soluciones de marketing en redes sociales para pequeñas empresas. Tu organización experimentó recientemente un ataque DDoS, que comprometió la red interna durante dos horas hasta que se resolvió.

Durante el ataque, los servicios de red de tu organización dejaron de responder repentinamente debido a una avalancha de paquetes ICMP entrantes. El tráfico normal de la red interna no pudo acceder a ningún recurso de la red. El equipo de gestión de incidentes respondió bloqueando los paquetes ICMP entrantes, deteniendo todos los servicios de red no críticos fuera de línea y restableciendo los servicios de red críticos.

A continuación, el equipo de ciberseguridad de la empresa investigó el incidente de seguridad. Descubrieron que un actor malicioso había enviado una avalancha de pings ICMP a la red de la empresa a través de un firewall no configurado. Esta vulnerabilidad permitió al atacante malicioso saturar la red de la empresa mediante un ataque de denegación de servicio distribuido (DDoS).

Para hacer frente a este problema de seguridad, el equipo de seguridad de red implementó:

- Una nueva regla de firewall para limitar la tasa de paquetes ICMP entrantes.
- La verificación de la dirección IP de origen en el firewall para comprobar si hay direcciones IP falsas en los paquetes ICMP entrantes.
- Un software de monitoreo de red para detectar patrones de tráfico anómalos.
- Un sistema IDS/IPS para filtrar parte del tráfico ICMP basándose en características sospechosas.

Como analista de ciberseguridad, se te asigna la tarea de utilizar este evento de seguridad para crear un plan para mejorar la seguridad de red de tu empresa, siguiendo el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST). Utilizarás el CSF para ayudarte a navegar por los diferentes pasos del análisis de este incidente de ciberseguridad e integrar tu análisis en una estrategia general de seguridad:

- **Identificar** los riesgos de seguridad a través de auditorías periódicas de las redes internas, los sistemas, los dispositivos y los privilegios de acceso para identificar posibles brechas en la seguridad.
- **Proteger** los activos internos mediante la aplicación de políticas, procedimientos, capacitación y herramientas que ayuden a mitigar las amenazas de ciberseguridad.
- **Detectar** posibles incidentes de seguridad y mejorar las capacidades de monitoreo para aumentar la rapidez y la eficiencia de las detecciones.
- **Responder** para contener, neutralizar y analizar incidentes de seguridad; implementar mejoras en el proceso de seguridad.
- **Recuperar** el funcionamiento normal de los sistemas afectados y restaurar los datos y/o activos de los sistemas que se hayan visto afectados por un incidente.