ANÁLISIS DEL INFORME DEL INCIDENTE

Resumen	La empresa sufrió un incidente de seguridad en el que todos los servicios de red dejaron de funcionar repentinamente. El equipo de ciberseguridad identificó que la causa fue un ataque de denegación de servicio distribuido (DDoS) mediante una inundación de paquetes ICMP. Para mitigar el ataque, el equipo bloqueó la amenaza y desactivó todos los servicios de red no esenciales, permitiendo la recuperación de los servicios críticos.
Identificar	Unos actores malintencionados ejecutaron un ataque de inundación ICMP contra la empresa, afectando toda la red interna. Fue necesario asegurar y restaurar todos los recursos críticos de la red.
Proteger	El equipo de ciberseguridad implementó una nueva regla en el firewall para limitar la tasa de paquetes ICMP entrantes y desplegó un sistema IDS/IPS para filtrar el tráfico ICMP con características sospechosas.
Detectar	Se configuró el firewall para verificar las direcciones IP de origen de los paquetes ICMP entrantes, con el fin de identificar direcciones IP falsas. Además, se implementó un software de monitoreo de red para detectar patrones de tráfico anormales.
Responder	Para futuros incidentes de seguridad, el equipo de ciberseguridad planea aislar los sistemas afectados para evitar interrupciones adicionales en la red. Se enfocarán en restaurar sistemas y servicios críticos afectados por el incidente y analizarán los registros de la red en busca de actividad anormal. También se informará sobre los incidentes a la alta dirección y, si es necesario, a las autoridades legales.
Recuperar	Para recuperarse de un ataque DDoS por inundación de ICMP, se debe restaurar el acceso a los servicios de red a un estado normal. En futuros incidentes, los ataques de inundación ICMP externos se bloquearán en el firewall. Durante un ataque, los servicios de red no críticos se detendrán para reducir el tráfico

	interno, priorizando la restauración de los servicios críticos. Una vez que el flujo de paquetes ICMP disminuya, se reactivarán los sistemas y servicios no críticos.