CIBERSEGURIDAD Y BIG DATA

Actividad integradora

¡Hemos llegado al fin del curso! Enhorabuena, has ampliado tu conocimiento en Big Data y Ciberseguridad. En esta actividad final podrás demostrar todo lo aprendido:

**CASO ATAQUE DDOS**

En un día típico en la empresa, el departamento de TI nota una serie de picos anormales en la actividad dentro de uno de sus sistemas, específicamente en el departamento de relaciones públicas. Sin embargo, es normal que ocurran fluctuaciones en la rutina, por tanto, se descartan y el día continúa como de costumbre.

Unas horas más tarde, el sitio web de la compañía se bloquea debido a un gran volumen de tráfico. El departamento de TI detecta un ataque de denegación de servicio (DDOS) lo que explica las fluctuaciones anormales presentadas anteriormente.

Tres horas después del descubrimiento inicial del ataque DDOS, un empleado de relaciones públicas recibe un correo electrónico de un hacker, quien afirma que continuará ejecutando ataques DDOS diarios a menos que la compañía les pague una alta suma de BTC. El cibercriminal también afirma tener acceso a la información de identificación personal de los empleados y clientes.

Ante este ataque contra el departamento de relaciones públicas, responda:

1. ¿En cuál protocolo deben estar los pasos a seguir en estos casos de ataque, considera que este debe ser revisado? Fundamente su respuesta con base en lo aprendido estas dos semanas.
2. ¿Cómo afecta este ataque a la empresa? ¿existen riesgos para sus empleados y clientes?
3. En su opinión, ¿este ataque pudo ser evitado? Justifique su respuesta. De ser afirmativa, indique algunas medidas que pueden ser aplicadas para ello.
4. Solventado el incidente ¿qué acciones deben tomarse para evitar un nuevo ataque? ¿Cuáles protocolos deben de ser revisado y cómo es el proceso de auditoria? Recuerde identificar los objetivos y las áreas críticas.