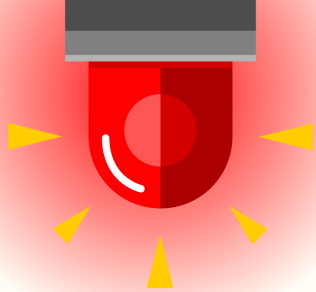


INCIDENTES DE SEGURIDAD



Un incidente de seguridad es cualquier evento que compromete la **confidencialidad**, **integridad** o **disponibilidad** de la información o los sistemas de una organización.



Existen varios tipos de incidentes

Malware



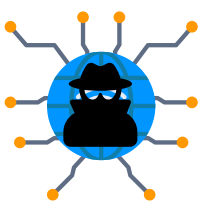
✖ Puede provocar la pérdida o filtrado de datos.
Ejemplos:
Ransomware, troyanos, virus, etc.

Ingeniería social



Puede provocar la pérdida de datos y el robo de credenciales
Ejemplo:
Phishing.

Ataques de red



Causan inaccesibilidad a los datos o espionaje.
Ejemplos:
DDoS, sniffing, MITM, etc.

Accesos no autorizados



Puede provocar violación o filtrado de datos.
Ejemplos:
Piggybacking, tailgating y clonación de credenciales.

Fuga de información



Puede exponer datos sensibles.
Ejemplos:
USB extraviado, dumpster diving, etc.

Errores humanos



Pueden comprometer el sistema.
Ejemplos:
Configuración errónea, borrado accidental, etc.

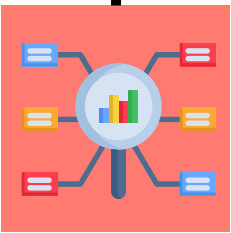


Para manejar un incidente se recomienda seguir el siguiente procedimiento:

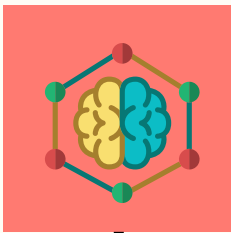
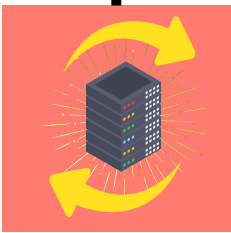
Preparación: Se deben crear políticas y herramientas para la prevención de incidentes, al igual que proporcionar entrenamiento a todos los empleados.



Análisis y clasificación: Se debe determinar el tipo de incidente, su alcance e impacto.



Erradicación y recuperación: Se debe eliminar la causa de la incidencia y restaurar sistemas.



Detección y notificación: Se debe identificar de manera oportuna comportamientos anormales y realizar el reporte correspondiente.



Contención: Se debe aislar el incidente y evitar su propagación.



Aprendizaje: Se deben mejorar los controles y políticas actuales para que la incidencia no se repita.

Los incidentes de seguridad representan riesgos reales para la información.

Su correcta detección, análisis y respuesta son esenciales para mantener la continuidad de los sistemas.



Bibliografía
Neil, I. (2020). CompTIA Security+ : SY0-601 Certification Guide: Complete coverage of the new CompTIA Security+ exam to help you pass on the first attempt (2nd ed.). Packt Publishing.