# Laboratorio 4

Sergio Alberto Tarrifa Ramirez

Los activos críticos de información son recursos esenciales para una organización, cuya pérdida, divulgación no autorizada o alteración podría tener un impacto significativo en sus operaciones y objetivos. Estos son:

* Bases de datos de clientes: Crítico
* Servidores: Crítico
* Sitio Web: Alto
* Red interna: Alto
* Terminales de trabajo: Medio

**Phishing:** Es un tipo de ingeniería social que utiliza correos electrónicos, mensajes de texto u otros medios para engañar a las víctimas y obtener información confidencial, como contraseñas o datos de tarjetas de crédito. Los atacantes suelen falsificar identidades de empresas legítimas o personas de confianza para parecer más creíbles.

**Malware:** Es un término general para software malicioso que puede incluir virus, gusanos, troyanos y spyware. El malware puede dañar los sistemas, robar información, o tomar el control de los dispositivos infectados.

**Ransomware:** Es un tipo de malware que cifra los archivos de la víctima y exige un rescate para devolver el acceso a los datos. Los atacantes a menudo utilizan el ransomware para extorsionar a las víctimas y obtener dinero.

**DDoS (Denegación de Servicio Distribuida):** Es un ataque que intenta sobrecargar un sitio web o servicio online con tráfico masivo, haciendo que se vuelva inaccesible para los usuarios legítimos. Los ataques DDoS pueden ser utilizados para sabotear operaciones, interrumpir servicios o distraer a los equipos de seguridad.

**Líder del equipo:**

Coordina la respuesta, establece la estrategia y mantiene informadas a las partes interesadas.

**Analistas de seguridad:**

Investigan incidentes, identifican vulnerabilidades y recomiendan medidas de seguridad.

**Investigadores de amenazas:**

Recopilan información sobre las amenazas, incluyendo el panorama general de amenazas y análisis forense.

La detección y respuesta ante amenazas incluye lo siguiente:

* Detección
* Investigación
* Contención
* Erradicación
* Recuperación
* Generación de informes
* Mitigación de riesgos

Una vez que los equipos están razonablemente seguros de que se ha eliminado una ciberataque o vulnerabilidad, vuelven a poner en línea los sistemas aislados recuperando copias de seguridad de los más importantes.