1. Activos importantes

* base de datos de los clientes->nivel crítico --- prioridad 1
* sitios web ->nivel intermedio --- prioridad 2
* servidor -> nivel critico --- prioridad 3

1. phishing-> correo mailicioso con remitente diferente al correo institucionalmente diferente al de la empresa
2. Presentar la estructura y funciones de un equipo de respuesta a incidentes.

* Consultar fuente de procedencia del correo del remitente
* Cortar la conexión con el sistema de la empresa ante el ataque
* Recuperar la información afectada por el ataque

1. Describir las herramientas y técnicas para monitoreo de logs, detección de anomalías, y sistemas de alertas.

Monitoreo de logs

Objetivo: Registrar, analizar y visualizar eventos del sistema

* **Logstash**: recolecta y procesa logs.
* **Elasticsearch**: almacena y permite búsquedas rápidas.
* **Kibana**: visualiza los datos en dashboards.
* **Graylog**: plataforma de análisis y gestión de logs, similar a ELK pero más ligera.
* **Fluentd**: herramienta de recolección y envío de logs, compatible con muchas plataformas.
* **Splunk**: solución comercial muy poderosa para indexar, buscar y analizar log

1. La importancia de contingencia es precisamente responder de la manera mas adecuada a ataques de esta índole lo que va permitir que los niveles críticos no sufran de sobremanera que en el ataque se pierdan los datos
2. Evaluación Inicial del Incidente

* Identificar y clasificar la amenaza detectada: malware, ataque de red, exfiltración de datos, etc.
* Determinar el alcance del incidente (sistemas, usuarios, redes afectadas).
* Iniciar el protocolo de respuesta

**Aislamiento de Sistemas Afectados**

* **Objetivo:** evitar que el ataque se propague a otros sistemas.

**Acciones:**

* Desconectar inmediatamente los equipos afectados de la red (Wi-Fi, Ethernet, VPN).
* Si es un servidor, aislarlo virtualmente mediante firewall o VLAN.
* Detener servicios críticos solo si no se compromete la recuperación posterior.
* No apagar el equipo si se requiere conservar evidencias.

**Desconexión de Redes**

* **Objetivo:** limitar la propagación de amenazas a través de la red.

**Acciones:**

* Bloquear direcciones IP sospechosas desde el firewall.
* Cerrar puertos abiertos innecesarios.
* Cortar temporalmente la red segmentada donde ocurrió el incidente.
* Deshabilitar el acceso remoto (RDP, SSH) hasta investigar completamente.

**Notificación al Equipo de Respuesta**

* Activar al **Equipo de Respuesta a Incidentes (CSIRT o equivalente)**.

**Contenido de la notificación:**

* Descripción breve del incidente.
* Sistemas o usuarios afectados.
* Hora de detección.
* Evidencias recopiladas (logs, capturas, archivos sospechosos).
* Medidas ya tomadas.

**Medios de notificación:**

* Canal de emergencia (correo, teléfono, app segura).
* Activación de protocolo de crisis si aplica (según el nivel de severidad).