* Entrada de vector de ataque
* PHISHING
* Phishing
* Primero hay que mirar la dirección del remitente si es confiable o un correo real puesto que muchos de los ataques ocurren cuando no se revisa bien el emisor del correo no deseado.
* Rastrear la url raras si se ingresaron credenciales.
* Si hubo una descarga de archivos saber el tipo y el resultado de la ejecución en el dispositivo infectado.
* Nivel de afectación en datos personales del usuario como sus cuentas privadas.
* Logs de correo electrónico -> contenido del correo electrónico
* Ejecutables
* URLS
* Cuenta de correo electrónico del emisor
* Logs del Sistema de Bases de Datos
* QUERY= “SELECT \* FROM tabla WHERE “-> esto es para como están los datos

Después del ataque si la información se encuentra. Ya que el atacante pudo haber alterado la información condesada.

* Si hay información alterada borrarla con una siguiente QUERY

QUERY= “DELETE FROM TABLA WHERE” eliminamos información alterada

Y recuperamos la información con copia de seguridad

* Primero fecha y hora: esto nos dira cuando ocurrió el ataque en el momento
* Dirección del atacante: ip, correo malicioso.
* Comportamiento sospechoso: multiple ingresos al sistema de manera abrupta y de manera anormal.
* Revisar accesos repetitivos de un mismo usuario o IP (brute force o escaneo).Detectar accesos fuera del horario habitual (por ejemplo, de madrugada).

Comparar actividad actual con actividad histórica del usuario o sistema. Buscar cambios inesperados en configuraciones o archivos sensibles. Ver patrones de tráfico de red (descargas masivas, conexiones externas no usuales). Correlacionar eventos entre sistemas (por ejemplo, un login sospechoso seguido de transferencia de archivos).

Análisis de errores o fallos frecuentes que puedan ser indicio de un ataque (como errores 401/403, o logs de denegación de servicio).

* 1. Contención inmediata
* Aísla los sistemas comprometidos de la red para evitar propagación.
* Desconéctalos físicamente o aísla su tráfico mediante firewall/VLAN.
* Bloquea cuentas o accesos sospechosos asociados al incidente.

Revisión de sistemas interconectados

* Analiza conexiones entrantes y salientes del sistema comprometido.
* Verifica logs de otros servidores que hayan tenido comunicación con él.
* Identifica otros posibles sistemas comprometidos en cadena.
* Evaluar el impacto en la infraestructura crítica
* Determina si el sistema afectado forma parte de servicios esenciales (como base de datos, servidores de autenticación, redes internas)
* Evalúa la disponibilidad y la integridad de los datos alojados.
* Identifica si hubo exfiltración o modificación de información sensible.
* Clasifica el nivel de criticidad (alto, medio, bajo) del impacto sobre la operación general.

9) **. Disponibilidad**

**¿Qué revisar?**

* ¿El sistema está accesible para los usuarios?
* ¿Se ha interrumpido algún servicio crítico?
* ¿Existen backups para restaurar el sistema rápidamente?

**Resultado esperado:**

* **Disponibilidad plena o restaurada.**
* Tiempo de inactividad medido y justificado.
* Plan de recuperación activado si fue necesario.

**Integridad**

**¿Qué revisar?**

* ¿Los datos han sido alterados, manipulados o dañados?
* ¿Se detectan archivos corruptos, modificados o eliminados?
* ¿Existen registros que indiquen cambios no autorizados?

**Resultado esperado:**

* **Confirmación de que los datos no fueron alterados.**
* Verificación con hashes, copias de respaldo o logs.
* Registro de cualquier modificación detectada y medida correctiva aplicada.

**. Confidencialidad**

**¿Qué revisar?**

* ¿Se ha accedido a información sensible por usuarios no autorizados?
* ¿Se ha producido filtración de datos (por ejemplo, credenciales, información personal, financiera)?
* ¿Se han violado políticas de acceso o privilegios?

**Resultado esperado:**

* **Confirmación de que la información confidencial está segura.**
* Revisión de logs de acceso y permisos.
* Si hubo fuga de datos, informe detallado del alcance y medidas de mitigación.
  + Medidas de Contenció Inmediatas:

• Actividad: qué medidas se pueden implementar para detener el ataque y prevenir una mayor propagación.

Desconecta sistemas comprometido: Actualización de Sistemas: Cambi de Credenciales

Desconectar sistemas comprometidos como credenciales porque así se puede interrumpir la intervención del atacante en mayor medida

* + Determinar a quién se le debe informar sobre la situación, las medidas tomadas, y las siguientes etapas. o- Transparencia: que se debe realizar
  + nternamente:
  + Equipo de Seguridad TI: para acciones técnicas y mitigación.
  + Gerencia o Dirección General: para decisiones estratégicas.
  + Equipo Legal y de Cumplimiento: si hay implicancias legales o normativas.
  + Equipo de Comunicación o RRHH: si se requiere manejo de crisis o comunicación interna.
  + Externamente (según la gravedad y normativa):
  + Clientes/Usuarios afectados: si hubo exposición de sus datos.
  + Autoridades reguladoras: como entes de protección de datos (por ejemplo, GDPR, HIPAA).
  + Socios o proveedores: si los servicios compartidos se vieron comprometidos.