Paso 1: Identificar el Vector de Ataque Inicial.

1.1 Revisión de Indicad re Iniciales:

• Actividad: que información reunirías para identificar los primeros signos del incidente (mensajes extraños, fallos en sistemas específicos).

Phishing: Ataques que engañan a los usuarios para que proporcionen información confidencial o descarguen malware.

Se identifico porque se mando una alerta al correo de que han ingresado a mi cuenta en otro dispositivo.
El phishing ocurrió por un correo trampa en el cual caí y robaron mis credenciales.

Si el phishing es identificado Que se debe buscar:

Busca correos electrónicos con enlaces sospechosos, archivos adjuntos maliciosos o remitentes falsificados.

- Errores gramaticales y ortográficos.
- Direcciones de correo sospechosas.
- Mensajes que apelan a la urgencia o utilizan amenazas.
- Solicitudes de información confidencial.
- Enlaces o archivos adjuntos dudosos.
- Mensajes genéricos y no personalizados.

Paso 2: Analizar los Log del Sistema para Encontrar Evidencias de Actividad Maliciosa.

2.1 Recolección de Logs:

• Actividad: Describir cuales pueden ser los logs de los sistemas afectados que se deben revisar (servidores de correo electrónico, bases de datos, terminales).

Log del Servidor de Correo Electrónico: Que se debe buscar.

-Buscar múltiples intentos fallidos de inicio de sesión.

-alertas de ingresos en otros dispositivos inusuales.

-robo de credenciales.

Paso 3: Determinar el Alcance del Compromiso y los Sistemas Afectados

3.1 Identificación de Sistemas Comprometidos.

- Actividad: que se debe realizar cuando se identifica los sistemas comprometidos.

Revisa los sistemas interconectados: ver si los demás sistemas conectados al afectado fueron comprometidos.

Evaluación del Impacto.

Disponibilidad: El daño ha interrumpido el acceso a sistemas o datos importantes

Integridad: si ocurrió alguna modificación no autorizada de los datos
Confidencialidad: Si se han filtrado datos o información sensibles a usuarios no autorizados.

Paso 4: Proponer Medidas de Contención y Recuperación (10 minutos)

4.1 Medidas de Contención Inmediatas

• Actividad: Implementar medidas para detener el ataque y prevenir una mayor propagación.

Desconectar sistemas comprometidos: separar los sistemas afectados para evitar que el malware se propague por todas partes de la red.

Plan de Recuperación

Restauración las copias de seguridad: Si los sistemas y datos han sido afectados, restauramos las ultimas copias de seguridad.

Comunicación

Informar a el equipo administrativo, personal de seguridad, usuarios afectados sobre el incidente y los pasos a seguir.