**1.1 Revisión de Indicadores Iniciales**

Este subpaso busca reconocer los primeros signos que pueden alertar sobre un incidente de seguridad informática. El objetivo es identificar comportamientos anómalos o señales sospechosas que indiquen una posible intrusión, compromiso o vulnerabilidad.

**¿Qué información se debe reunir?**

1. **Mensajes sospechosos o fuera de contexto**
   * Correos electrónicos con errores gramaticales, remitentes desconocidos o enlaces dudosos.
   * Solicitudes urgentes de cambio de contraseña o transferencia de datos.
2. **Fallos o comportamientos anómalos en los sistemas**
   * Aplicaciones que se cierran inesperadamente.
   * Lentitud inusual en redes o servicios específicos.
   * Errores de autenticación en cuentas legítimas.
3. **Alertas o notificaciones del sistema de seguridad**
   * Antivirus que detecta software malicioso.
   * Firewalls que bloquean conexiones no autorizadas.
   * Sistemas de detección de intrusos (IDS/IPS) con registros de eventos inusuales.

**Posibles vectores de ataque asociados a los síntomas:**

* **Phishing:**  
  Relacionado con mensajes engañosos que intentan obtener credenciales o inducir al usuario a ejecutar archivos maliciosos.
* **Explotación de vulnerabilidades:**  
  Ataques que se aprovechan de errores en el software no actualizado o mal configurado.
* **Acceso no autorizado:**  
  Ingresos al sistema por parte de usuarios externos o internos sin los permisos adecuados.

**1.2 Evaluación de la Evidencia**

Una vez se detectan señales de alerta, es necesario recolectar y analizar evidencia técnica que permita determinar el vector de ataque inicial con la mayor precisión posible.

**¿Qué tipo de evidencia se puede recolectar y cómo?**

1. **Si el vector sospechoso es Phishing:**
   * **Correos electrónicos recibidos:** analizar remitente, asunto, contenido, enlaces y archivos adjuntos.
   * **Registros del servidor de correo:** verificar si otros usuarios también recibieron el mensaje.
   * **Actividad del usuario afectado:** revisar si hizo clic en enlaces o descargó archivos.
   * **Análisis del archivo adjunto o sitio web:** ejecutar en un entorno aislado (sandbox) para observar su comportamiento.
2. **Si el vector sospechoso es una vulnerabilidad:**
   * **Escaneo de puertos y servicios:** identificar servicios activos y su versión.
   * **Revisión de parches aplicados y faltantes:** detectar software sin actualizaciones recientes.
   * **Logs de error del sistema:** examinar entradas en los momentos previos al incidente.
   * **Reporte de CVEs** (Common Vulnerabilities and Exposures) relevantes a los sistemas afectados.
3. **Si el vector sospechoso es un acceso no autorizado:**
   * **Registros de autenticación:** verificar intentos fallidos, inicios de sesión en horarios no habituales o desde ubicaciones anómalas.
   * **Actividad de cuentas privilegiadas:** rastrear acciones realizadas por administradores o usuarios con muchos permisos.
   * **Cambios en la configuración del sistema o archivos:** revisar qué modificaciones se realizaron sin autorización o sin registro.

**2.1 Recolección de Logs**

En esta etapa se identifica y extrae la información de los registros (logs) generados por los sistemas afectados, que pueden contener evidencias clave del comportamiento del atacante o del origen del incidente.

**¿Qué tipos de logs se deben revisar y qué se debe buscar?**

1. **Logs del servidor de correo electrónico**
   * Correos enviados/recibidos en el momento del incidente
   * Mensajes marcados como spam o con archivos adjuntos sospechosos
   * Direcciones IP de origen de correos externos
   * Fallos de autenticación o accesos inusuales a cuentas de correo
2. **Logs del sistema de bases de datos**
   * Consultas o comandos inusuales (ej. DROP, DELETE, ALTER no autorizados)
   * Accesos fuera del horario normal o desde IPs desconocidas
   * Cambios en privilegios de usuarios o creación de nuevas cuentas
   * Repentinas exportaciones de grandes volúmenes de datos
3. **Logs de seguridad del sistema operativo o del firewall**
   * Alertas de detección de malware o intrusiones
   * Cambios en configuraciones críticas del sistema
   * Accesos remotos desde ubicaciones sospechosas
   * Ejecución de procesos desconocidos o no autorizados

**2.2 Análisis de la Actividad Maliciosa**

Una vez recopilados los logs, se realiza un análisis sistemático para identificar patrones anómalos o indicios de comportamiento malicioso.

**¿Qué se debe analizar en los logs?**

* **Correlación temporal:**  
  Comparar los registros con el momento en que se detectaron las anomalías.
* **Búsqueda de patrones inusuales:**
  + Accesos en horarios atípicos
  + Autenticaciones repetidas y fallidas
  + Cambios en archivos del sistema o bases de datos
  + Tráfico saliente elevado (posible exfiltración de datos)
* **Secuencia de eventos:**  
  Establecer una línea de tiempo de las acciones realizadas antes, durante y después del incidente.

**Herramientas recomendadas para análisis de logs:**

* **SIEM (Security Information and Event Management):**
  + Splunk
  + AlienVault
  + IBM QRadar
* **Herramientas de línea de comandos y scripts personalizados:**
  + grep, awk, sed (Linux)
  + PowerShell (Windows)
* **Otros recursos útiles:**
  + Sysinternals Suite
  + Wireshark (para correlación con tráfico de red)

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

**3.1 Identificación de Sistemas Comprometidos**

Una vez identificados los indicios de actividad maliciosa, es necesario establecer exactamente qué sistemas fueron comprometidos.

**¿Qué acciones se deben realizar?**

* **Revisión de los sistemas interconectados:**  
  Analizar si otros equipos o servidores pudieron haber sido afectados a través de conexiones de red, cuentas compartidas o servicios vinculados.
* **Evaluación del impacto en infraestructura crítica:**  
  Determinar si el incidente afectó servicios esenciales (correo, bases de datos, servidores web, backups, etc.).
* **Inventario de sistemas afectados:**  
  Elaborar un listado claro y documentado de todos los equipos impactados, incluyendo dirección IP, ubicación, servicios activos y nivel de afectación.

**3.2 Evaluación del Impacto**

El impacto se evalúa en términos de los principios básicos de la seguridad de la información:

**¿Qué se debe tener en cuenta?**

1. **Disponibilidad:**
   * ¿Se interrumpieron servicios?
   * ¿Hubo pérdida de acceso a sistemas o datos?
   * ¿Qué tiempo estuvieron inactivos?
2. **Integridad:**
   * ¿Se modificaron archivos o configuraciones sin autorización?
   * ¿Hubo alteración de datos críticos o registros?
3. **Confidencialidad:**
   * ¿Se accedió o exfiltró información sensible (clientes, empleados, contraseñas)?
   * ¿Se perdió el control sobre credenciales o claves?