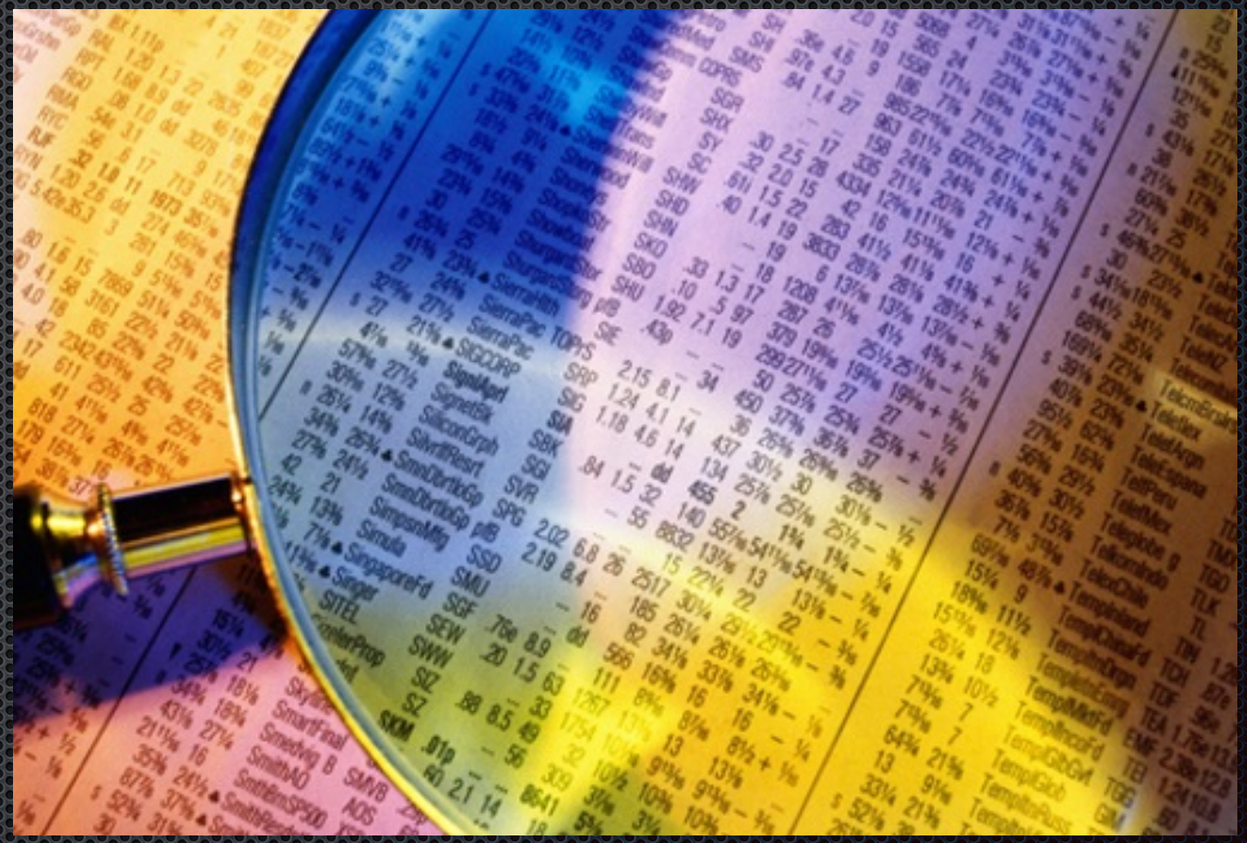
UT3 Investigación de los incidentes de ciberseguridad

- Recopilación de evidencias.
- Análisis de evidencias.
- Investigación del incidente
- Intercambio de información del incidente con proveedores u organismos competentes.
- Medidas de contención de incidentes.

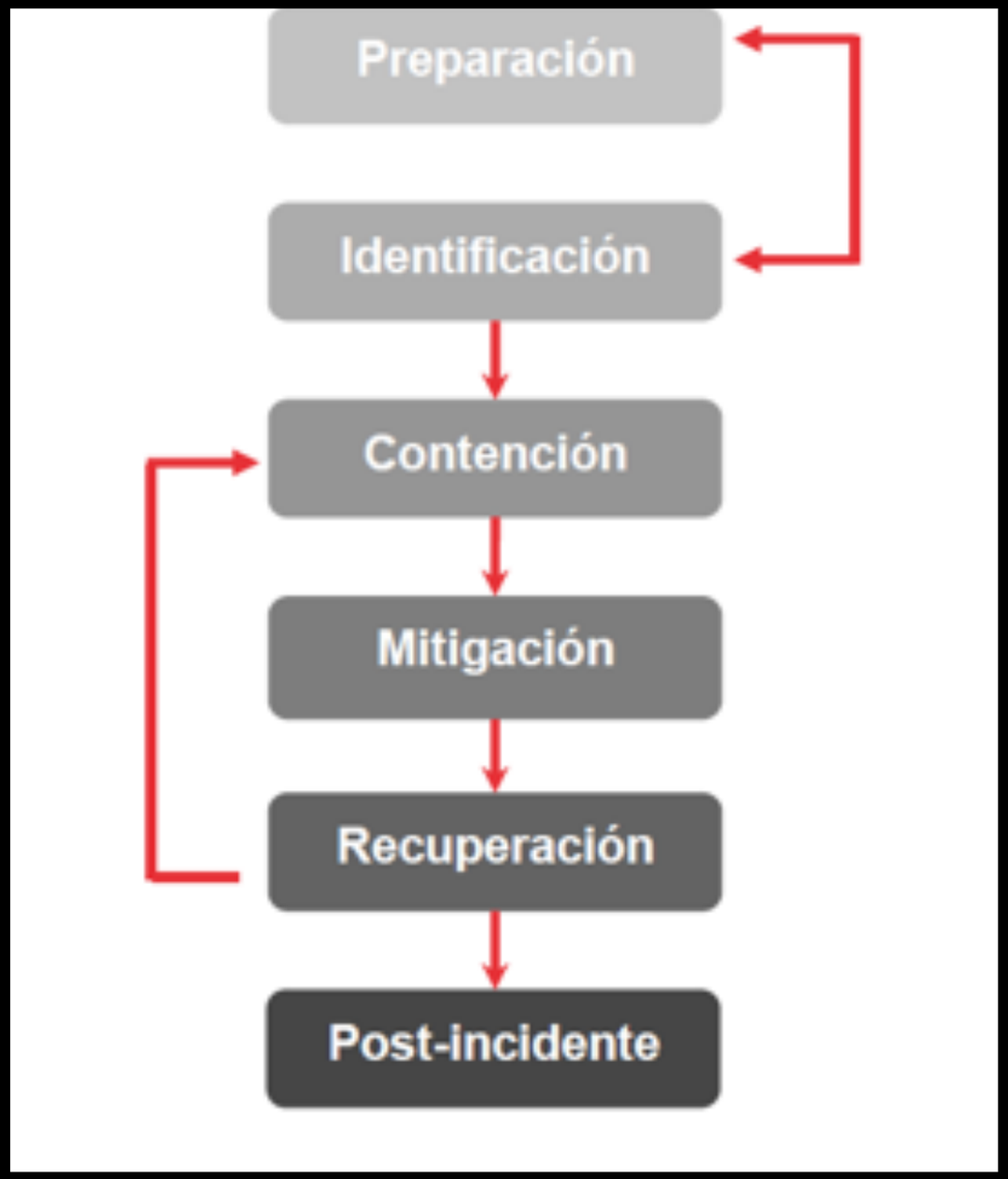


Tarea online

- Realizar el informe ejecutivo y técnico de un incidente de Ciberseguridad:
  - Un incidente real del que se haya tenido conocimiento.
  - Incidente real del que haya suficiente bibliografía
  - Incidente ficticio: Ataque pishing al IES
  - Incidente ficticio: documentar.

Fases de la gestión de un incidente

- Preparación: previamente
- Identificación: detectar el incidente
- Contención:primeras medidas, evitar que se expanda.
- Mitigación: Medidas para salir el efecto
- Recuperación: volver a la situación anterior
- Post-incidente: documentar el incidente, hacer cambios, lecciones aprendidas.



Recopilación de evidencias

- Procedimiento de toma y preservación de evidencias.
- Similar al análisis forense: en este caso se hace en producción.
- Estandarizados en la RFC 3227

Recopilación de evidencias

- Durante la recolección:
  - Principios:
    - Imagen fiel de sistema
    - Notas detalladas fechas y horas (y horario)
    - Minimizar cambios.
    - *Recolección* VS análisis.
    - Cada dispositivo tiene mejor manera de hacer la recogida de datos
    - Recoger según orden de volatilidad

Recopilación de evidencias

- Orden de volatilidad.
    - Período en el que esta accesible la información:
    - Registros y caché
    - Enrutamiento, ARP, Procesos, estadísticas Kernel, memoria
    - Información temporal del sistema
    - Disco
    - Logs
    - Documentos física de la red
    - Documentos

Recopilación de evidencias

- Acciones a evitar: que no invaliden el proceso, preservar la integridad.
  - No apagar equipo
  - No confiar en la información proporcionada por los programas del sistema
  - No ejecutar programas que modifiquen la fecha y hora

Recopilación de evidencias

- Consideraciones sobre la privacidad
    - Pautas de la Organización
        - Autorización por escrito
            - Información confidencial o vital
            - Disponibilidad afectada.
        - No entrometerse en la privacidad de las personas sin una justificación.
            - No recopilar información sin razón

Recopilación de evidencias

- Procedimiento de recolección
- Transparencia y reproducibilidad.
- Testeado por expertos independientes
-

Recopilación de evidencias

- Procedimiento de recolección. Pasos

- ¿Dónde está la evidencia?.
- Fijar el orden de volatilidad
- Obtener la información de acuerdo al orden establecido.
- Comprobar sincronización del reloj
- ¿ qué más puede ser una evidencia?
- Documentar cada paso.
- Documentar personas presentes

Recopilación de evidencias

- Procedimiento de recolección. Herramientas

- Externas al sistema
- Alteren lo mínimo el escenario
- Ubicado dispositivos de solo lectura
- Adecuado a los sistemas
- Incluir:
    - Examinar procesos
    - Examinar estado del sistema
    - Copias bit a bit

Análisis de evidencias

- Análisis de evidencias:
  - Objetivo
  - Qué o quien
  - Cómo
  - Afectación de los sistemas
- Concluir informes bien documentados

Análisis de evidencias

- A tener en cuenta:
  - Nuca trabajar con datos originales
  - Respetar la ley
  - Resultados verificables y reproducibles
    - Entorno donde reproducir la investigación

Documentación necesaria

- Sistema operativo
- Programas instalados
- Hardware, accesorios y periféricos
- Datos conectividad:
  - Firewall
  - Topología de la red
- Datos generales de configuración

Fases del análisis

- No hay un proceso estándar:
  - Depende del tipo de evento, sistema, etc.
- Pasos:
  - Preparar entorno de trabajo.
  - Reconstruir linea incidente
  - Identificar autor
  - Evaluar el impacto.
-

Preparación del entorno

- Caliente o frío.
- Riesgos del análisis (modo solo lectora)
- Frío: uso VM: Se puede actuar sin “miedo”
    - Es más costoso, a veces no se puede hacer.

Recreación de la linea temporal

- Suele ser la primera acción.
- Utiliza tiempos MACD (modificación, acceso, Creación, borrado)
- Ojo fechas reales y del sistema (Impacto en las pruebas)
- Fecha de instalación: origen
- Ficheros “visibles”: instalación de programas, etc.
- Archivos ocultos, borrados, Esteanografía,…
- Análisis de archivos borrados: herramientas específicas.
- Finalmente crear un cronograma.

¡COMO ACTUARON LOS ATACANTES?

- Volcado de memoria.
    - Procesos ejecución aparentemente legítimos.
        - Procesos sin padre, log, enlaces.
        - Tipo de Malware.
        - Secuencia de comandos de la consola.
-

¿Quienes fueron?

- Conexiones de red abiertas: IP a las que se conectan
    - Actuar con prudencia: IPS camufladas, redes de boots, etc.
    - Perfiles de atacantes:
        - Motivos económicos
        - Motivos personales.
        - Hackers grises
- Finalidad inculpatoria o correctiva (no interesa motivación)

Investigación del incidente

Intercambio de información

Medidas de contención