Actividad 13. Gestión de ciber incidentes

1. Explica los incidentes más habituales en las organizaciones e indica una clasificación por nivel de peligrosidad con ejemplos

Los **incidentes en una organización** son cualquier suceso no planificado que interrumpe las operaciones normales, en el que causa daños, pérdidas o pone en riesgo la salud, seguridad o el bienestar de las personas involucradas. Estos pueden ocurrir en cualquier área de la empresa y pueden ser de diversa naturaleza.

CLASIFICACIÓN POR NIVEL DE PELIGROSIDAD:

- ***INCIDENTES MENORES:***
  - **Ejemplo**: Corte de energía breve que afecta a algunas áreas de la oficina, un error en un documento que se detecta a tiempo y se corrige, un pequeño derrame de líquido en un laboratorio.
  - **Características**: Estos incidentes suelen tener un impacto limitado, que se resuelven rápidamente y no causan grandes pérdidas.

- ***INCIDENTES MODERADOS:***
  - **Ejemplo**: Un pequeño incendio que se controla rápidamente, una falla en un sistema informático que provoca la interrupción temporal del servicio, un accidente laboral que causa una lesión leve.

- **Características**: Estos incidentes suelen causar disrupciones significativas en las operaciones, pero se pueden gestionar con los recursos internos de la organización.

- ***INCIDENTES MAYORES:***
  - **Ejemplo**: Un ciberataque que compromete a los datos sensibles, un accidente industrial grave que causa múltiples lesiones, un desastre natural que afecta a las instalaciones de la empresa.
  - **Características**: Estos incidentes tienen un impacto a largo plazo en la organización, que pueden causar pérdidas financieras significativas y requieren la intervención de los equipos especializados, y en algunos casos, de las autoridades.

- ***INCIDENTES CATASTRÓFICOS:***
  - **Ejemplo**: Una explosión en una planta industrial que causa múltiples víctimas fatales y daños ambientales a gran escala, un colapso estructural de un edificio que resulta en la pérdida de vidas humanas.
  - **Características**: Estos incidentes tienen consecuencias devastadoras para la organización, la comunidad y el medio ambiente, y pueden llevar a la quiebra de la empresa.

INCIDENTES MÁS HABITUALES EN LAS ORGANIZACIONES:

- ***SEGURIDAD***: Accidentes laborales, robos, actos de vandalismo, violencia en el lugar de trabajo.
- ***INFORMÁTICA***: Ciberataques, fallas en el sistema, pérdida de datos, errores humanos.
- ***OPERACIONES***: Incendios, inundaciones, fallas en equipos, interrupciones en la cadena de suministro.
- ***RECURSOS HUMANOS***: Conflictos laborales, discriminación, acoso, bajas por enfermedad.
- ***REPUTACIÓN***: Crisis de imagen, escándalos, publicidad negativa.

2. Relaciona y explica las fases a seguir en un plan de gestión de incidentes

Un plan de gestión de incidentes es esencial para cualquier organización, ya que permite responder de manera rápida y eficaz ante cualquier situación que pueda interrumpir sus operaciones.

FASES DE UN PLAN DE GESTIÓN DE INCIDENTES:

1. ***PREPARACIÓN:***
    a. ***Definición de Roles y Responsabilidades:*** Se establece quiénes formarán parte del equipo de respuesta a incidente y cuáles serán sus funciones específicas.
    b. ***Establecimiento de Procedimientos:*** Se documentan los pasos a seguir en cada fase del proceso (desde la detección hasta la resolución).
    c. ***Creación de una Base de Conocimientos:*** Se recopila la información sobre los sistemas, aplicaciones y procesos críticos para la organización.
    d. ***Desarrollo de Planes de Comunicación:*** Se definen los canales y los mensajes clave para comunicar el incidente a los diferentes grupos de interés (empleados, clientes, etc.).
    e. ***Pruebas del Plan:*** Se realizan simulacros para identificar posibles fallos y mejorar la eficiencia del plan.
2. ***DETECCIÓN Y ANÁLISIS:***
    a. ***Monitoreo Continuo:*** Se utilizan herramientas para detectar cualquier anomalía o desviación de los normal en los sistemas.
    b. ***Análisis de la Información:*** Se evalúa la naturaleza y el alcance del incidente para determinar su impacto en la organización.
    c. ***Escalamiento:*** Se notifica el incidente a los responsables correspondientes y se activa el equipo de respuesta.
3. ***CONTENCIÓN:***
    a. ***Aislamiento del Incidente:*** Se toman las medidas para limitar la propagación del incidente y evitar que afecte a otros sistemas o datos.
    b. ***Mitigación de Daños:*** Se implanten acciones para minimizar el impacto del incidente en las operaciones de la organización.
4. ***ERRADICACIÓN Y RECUPERACIÓN:***
    a. ***Identificación de la Causa Raíz:*** Se investiga a fondo para determinar qué originó el incidente.
    b. ***Eliminación de la Causa:*** Se implantan las medidas correctivas necesarias para solucionar el problema de raíz.

   c. ***Restauración de los Sistemas:*** Se recuperan los datos y se restablecen los servicios afectados.

5. ***APRENDIZAJE Y MEJORA:***
   a. ***Análisis Post-Incidente:*** Se evalúa la respuesta al incidente para identificar las áreas de mejora.
   b. ***Actualización del Plan:*** Se realizan los ajustes necesarios al plan de gestión de incidentes para aumentar su eficacia.

En definitiva, un plan de gestión de incidentes es un ciclo continuo que comienza con la preparación, pasa por la detección, contención y erradicación del incidente, y concluye con el aprendizaje y mejora. Cada fase es crucial para garantizar una respuesta rápida y efectiva ante cualquier situación de crisis.