UT 5 Detección y documentación de incidentes de ciberseguridad

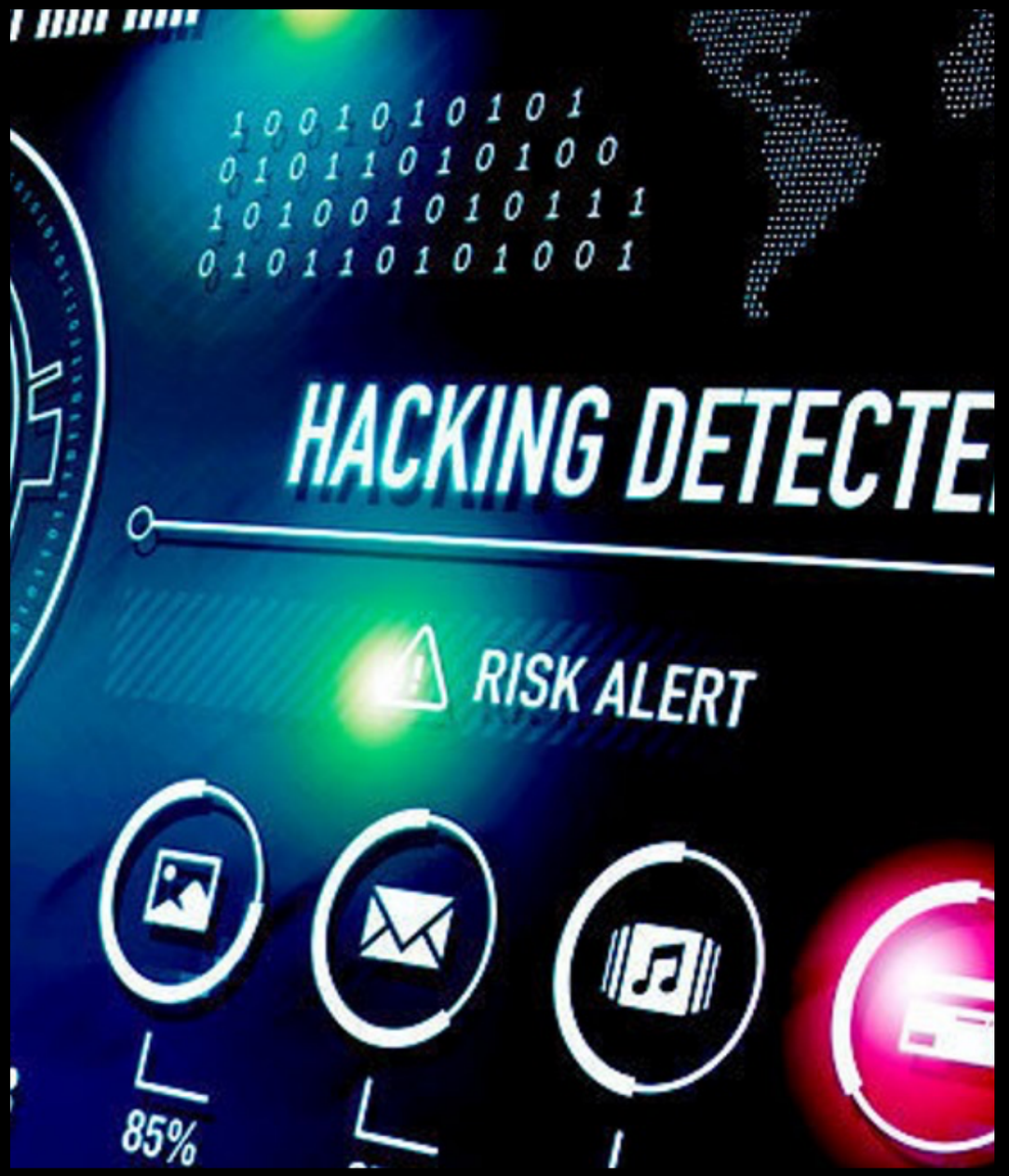
- Desarrollar procedimientos de actuación para la notificación de incidentes.
- Notificación interna de incidentes.
- Notificación de incidentes a quienes corresponda.

Tarea online

- Desarrollar brevemente el procedimiento de notificación de incidente para una organización real o ficticia.
    - Debe contemplar la notificación interna y externa.
- Supón que la organización se enfrenta a la siguiente situación:
    - "uno de los empleados ha perdido un pendrive con una hoja de cálculo con datos personales de los clientes/usuarios de la organización"
    - Describe los pasos que se producirían así como las comunicaciones que se realizarían de manera tanto interna como externa.

Procedimientos de actuación para la notificación de incidentes.

- Controles y mecanismos de seguridad
  - dentro y alrededor de las instalaciones de la organización
  - medios de acceso remoto a la información.
-



Procedimientos de actuación para la notificación de incidentes.

- Notificaciones de usuarios:
  - presencia de archivos con caracteres inusuales,
  - recepción de correos electrónicos con archivos adjuntos sospechosos,
  - comportamiento extraño de dispositivos,
  - imposibilidad de acceder a ciertos servicios,
  - extravío/robo de dispositivos de almacenamiento o equipos con información.

procedimientos de actuación para la notificación de incidentes.

- Alertas generadas por software antivirus.
- Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
- Anomalías de tráfico de red o picos de tráfico en horas inusuales.
- Alertas de sistemas de detección/prevención de intrusión (IDS/IPS).
- Alertas de sistemas de correlación de eventos.

procedimientos de actuación para la notificación de incidentes.

- Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en los cortafuegos.

- Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.

- Análisis de registros en herramientas DLP (Data Loss Prevention).

- Cualquier posible indicio de la ocurrencia de un incidente de seguridad en el futuro (OSINT)

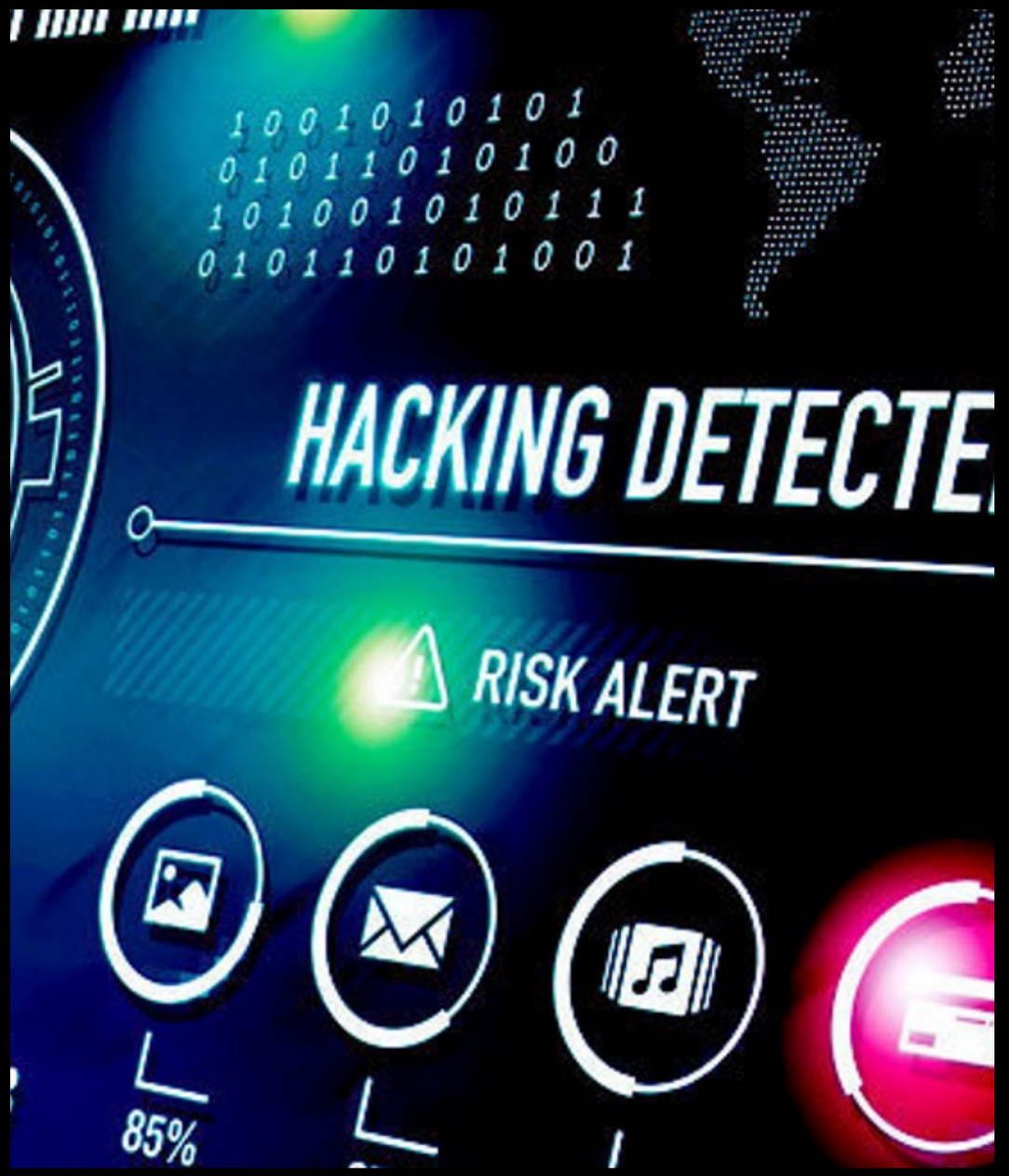
procedimientos de actuación para la notificación de incidentes.

- En cuanto a los controles de ciberseguridad:
    - atendiendo a las características particulares de la organización, se puede contar con medios manuales: la notificación de problemas por parte del personal de la organización,
        - sistemas automatizados de detección de diferentes tipos: software antivirus analizadores de logs.
- Un incidente que tenga lugar en el ámbito de la seguridad física puede también
    - tener repercusión en el contexto de la ciberseguridad
    - en los tratamientos de datos personales, d
    - mantener cierto grado de coordinación entre los responsables de la seguridad física y la ciberseguridad.

procedimientos de actuación para la notificación de incidentes.

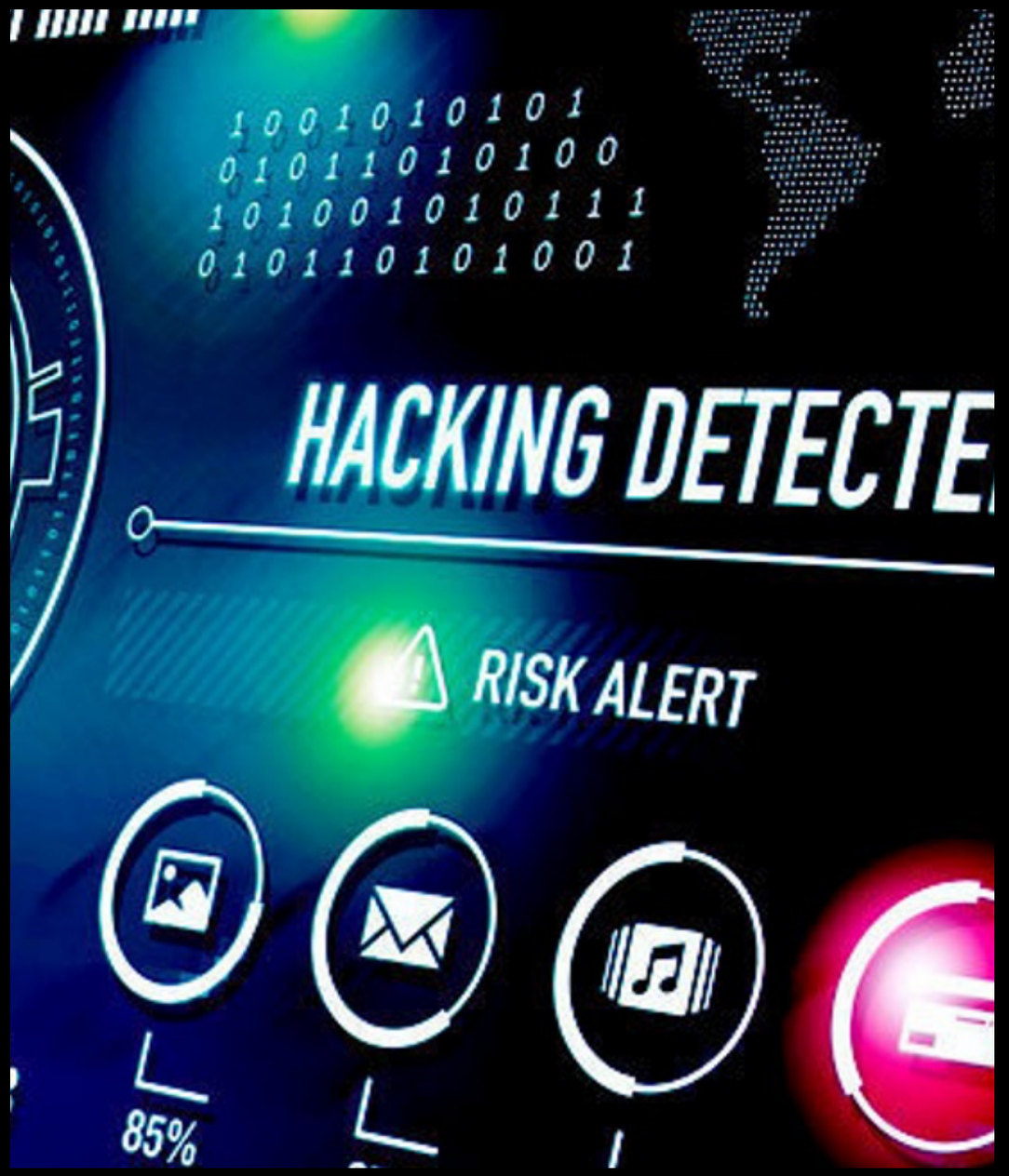
- Desde el punto de vista de la seguridad física, la detección se produciría ante el incumplimiento o vulneración de las medidas de seguridad adoptadas:
    - Políticas específicas de mesas limpias, bloqueo de pantallas, accesos con usuario y contraseña, etc
- Controles físicos como detección de intrusos, videovigilancia, control y registro de accesos a determinadas zonas, etc
- Controles y procedimientos frente a daños ambientales o desastres naturales.
    - concienciación y formación de todo el personal de la organización para
        - evitar situaciones de riesgo
        - detectarlas y notificarlas.

Notificación interna de incidentes.



Notificación interna de incidentes.

Notificación externa de incidentes.



Notificación externa de incidentes.