# UT 5 Detección y documentación de incidentes de ciberseguridad

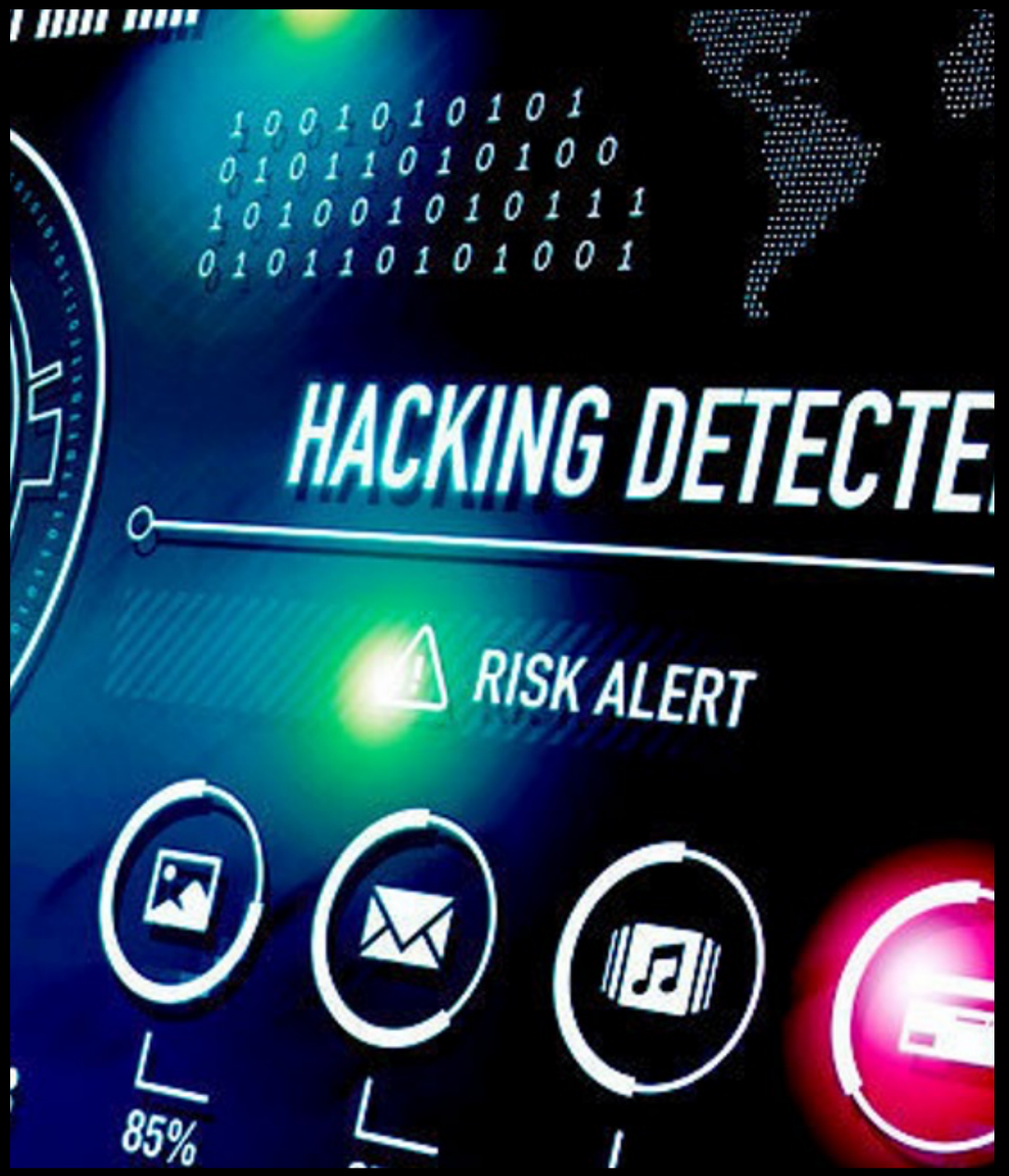
- Desarrollar procedimientos de actuación para la notificación de incidentes.
- Notificación interna de incidentes.
- Notificación de incidentes a quienes corresponda.

# 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.

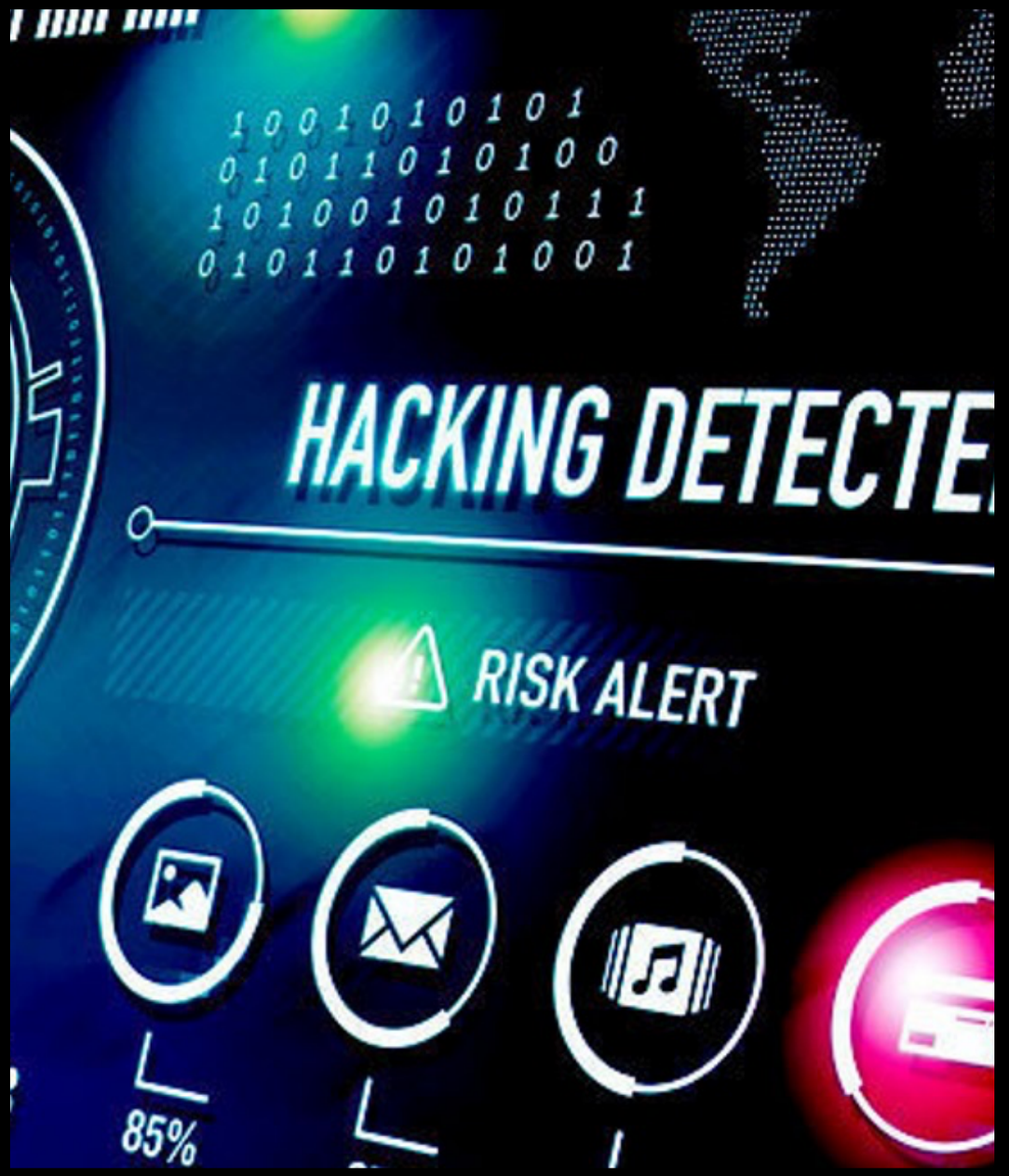
- En cuanto a los controles de ciberseguridad:
    - atendiendo a las características particulares de la organización, se puede contar con medios manuales: la notificación de problemas por parte del personal de la organización,
        - sistemas automatizados de detección de diferentes tipos: software 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.

- todo el proceso de respuesta al incidente debe quedar documentado,
- las conclusiones de los técnicos y responsables del equipo para
- lecciones aprendidas y ser incluidas
- informe de resolución.



# Notificación interna de incidentes.

- Se recomienda disponer de la siguiente información para poder elaborar el citado informe:
  - Descripción objetiva del incidente.
  - Controles existentes en el momento del incidente.
  - Enumeración de medidas efectivas de respuesta.

# Notificación interna de incidentes.

- Determinar si a igual casuística el incidente se repetiría.
- Medidas de detección aplicadas para identificar nuevos casos.
- Registro de comunicaciones durante la respuesta.
- Comunicación: dirección y partes interesadas.

# Notificación interna de incidentes

- La comunicación es fundamental durante todo el ciclo de vida del proceso de respuesta,

- hacerse de una manera continua de modo que la dirección y responsables de seguridad tengan una visibilidad clara tanto del incidente como de las acciones tomadas para afrontarlo.

- Es especialmente importante cuando el incidente trasciende el perímetro de la organización y toma relevancia pública.

    - muy posiblemente los directivos serán preguntados por las acciones que se están llevando a cabo y posibles consecuencias

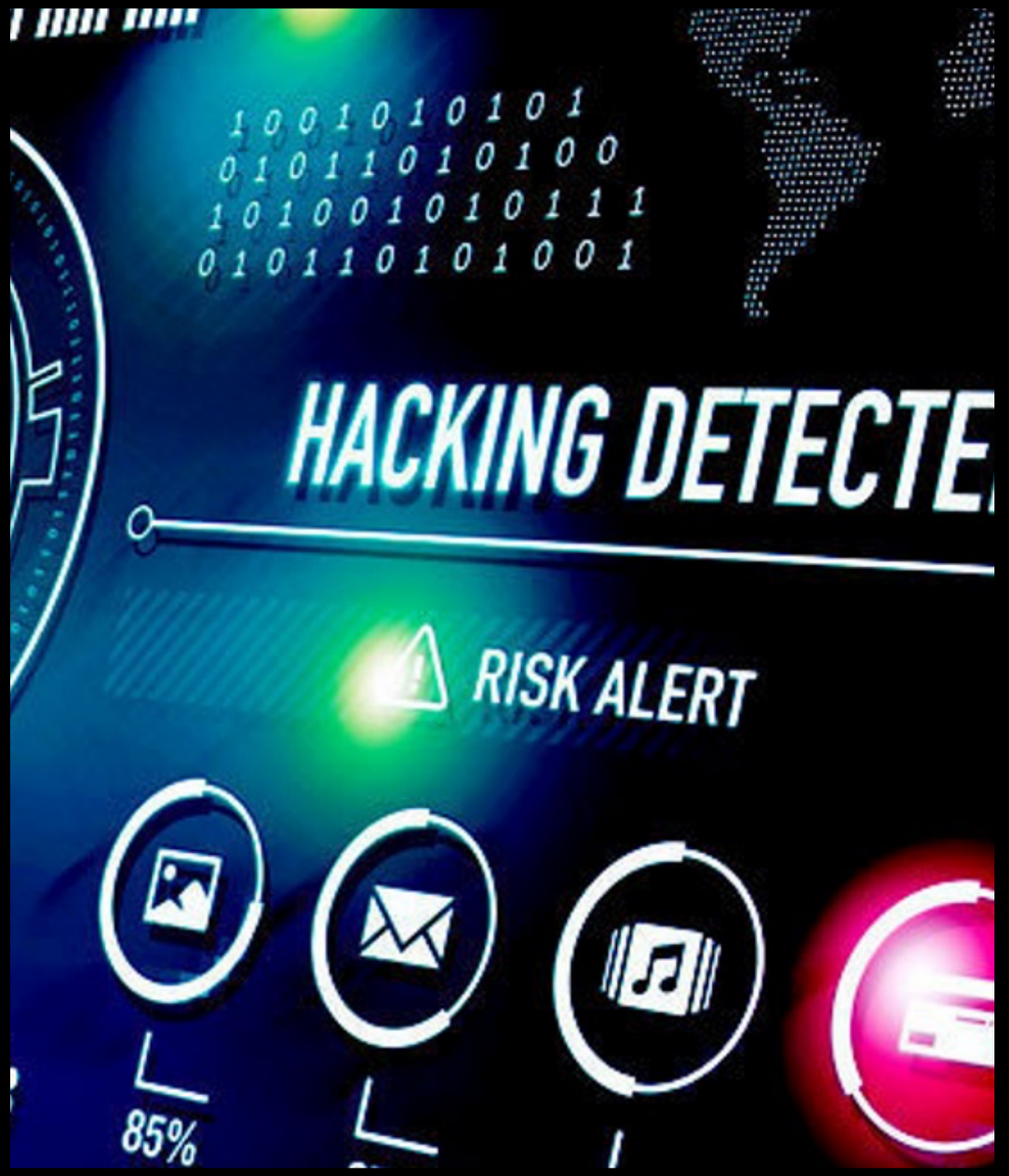
-

# Notificación interna de incidentes

- Las tareas de comunicación no buscan la aprobación de la gerencia ni su toma de decisiones,
    - simplemente se trata de un cuaderno de bitácora lo suficientemente actualizado para informar a la dirección y otras partes interesadas,
    - que también puedan cumplir con sus propias obligaciones.
- BUSCAR EJEMPLO DE MALA COMUNICACION

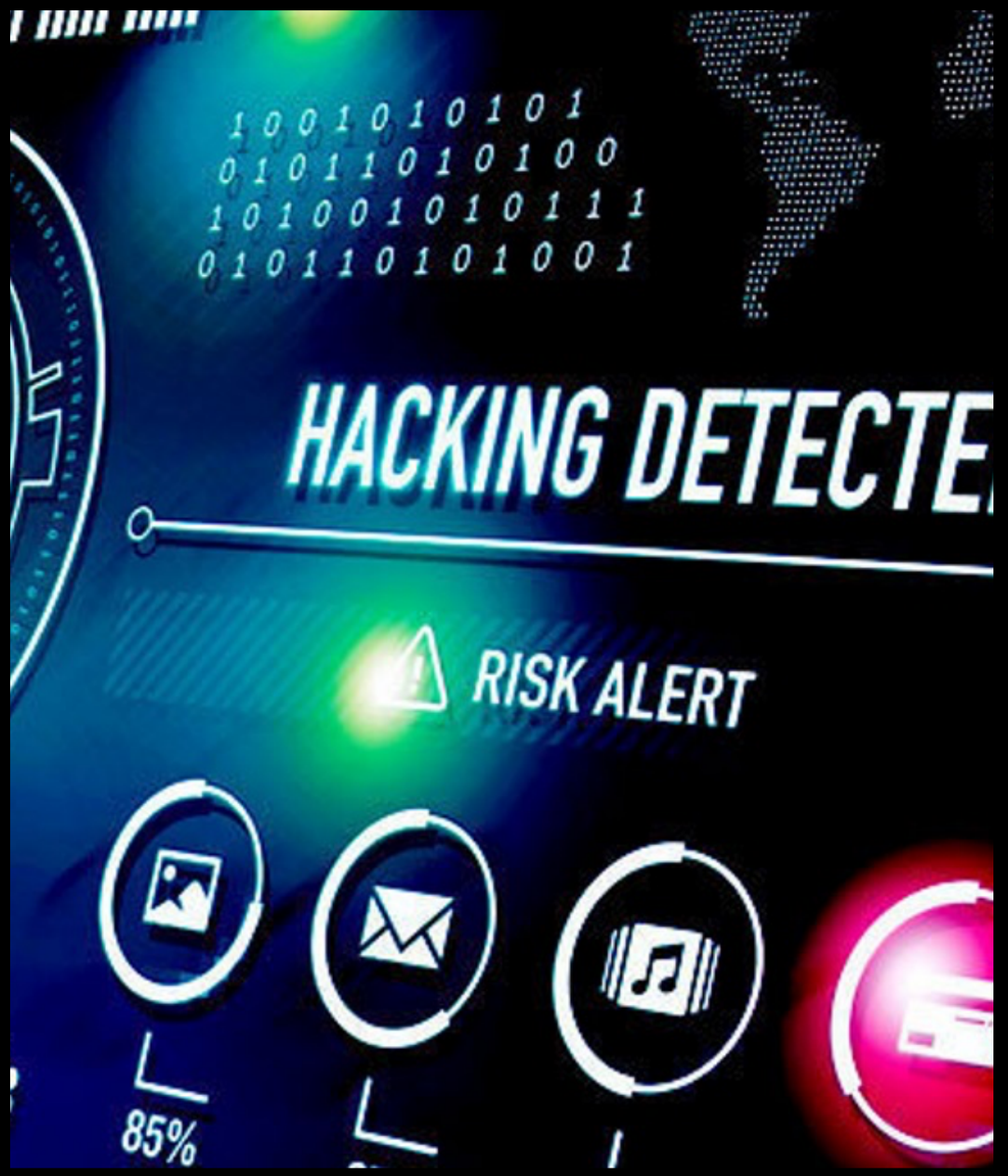
# Notificación externa de incidentes.

- Artículo 33 del RGPD,
  - brecha de la seguridad que afecte a los datos personales,
  - responsable del tratamiento la notificará a la autoridad de control competente sin dilación
  - a más tardar 72 horas después de que haya tenido constancia de ella.
  - a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.



# Notificación externa de incidentes.

- Así mismo, el artículo 34 del RGPD
  - cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas,
  - el responsable del tratamiento la comunicará a los afectados.



# Notificación externa de incidentes.

- formalizar un procedimiento de notificación, en el que se establezca el proceso a seguir para comunicar las brechas de seguridad de los datos personales a
- las autoridades de control
- en casos graves, a los afectados.
- Dicho procedimiento, que ha de ser conocido entre quienes deban utilizarlo
- debe describir la manera en la que se comunica, e identificar al representante dentro de la organización (podrá ser el Delegado de Protección de Datos en el caso de que lo hubiera)

# Notificación externa de incidentes.

- En caso de empresas pequeñas:

- El responsable podrá ser el propio responsable del tratamiento o a quien éste designe para ser el punto de contacto con la autoridad de control.

- La existencia de una política de notificaciones de brechas de seguridad e disponer de un criterio común a todos los tratamientos de datos personales que consten en el registro de actividades de tratamiento de una organización

- . En cada caso se debe de valorar los umbrales bajo los cuales el responsable procederá a la notificación.

# Notificación externa de incidentes.

- Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe, sin dilación y, a más tardar en las 72 horas siguientes a tener constancia, efectuar la correspondiente notificación a la Autoridad de Control.

- Se considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

- El criterio a tener en cuenta para determinar si un incidente ha producido “una brecha de la seguridad de los datos personales” se recoge en el propio RGPD, e incluye “todas aquellas brechas de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

# Notificación externa de incidentes.

- Esta comunicación deberá contener la siguiente información:

- Datos identificativos y de contacto de: Entidad / Responsable del tratamiento, Delegado de Protección de Datos (si está designado) o persona de contacto. Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de una notificación parcial indicar si se trata de una primera notificación o una notificación complementaria.

- Información sobre la brecha de seguridad de datos personales: Fecha y hora en la que se detecta.Fecha y hora en la que se produce el incidente y su duración. Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.)

- Naturaleza y contenido de los datos personales en cuestión.

# Notificación externa de incidentes.

- Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).

- Posibles consecuencias y efectos negativos en los afectados.

- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento según el apartado 33.2d) del RGPD.

- Categoría de los datos afectados y número de registros afectados.

- Categoría y número de individuos afectados.

- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

# Notificación externa de incidentes.

- Si en el momento de la notificación, no fuese posible facilitar toda la información, podrá facilitarse posteriormente, de manera gradual en distintas fases. La primera notificación se realizará en las primeras 72h, y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente.

- Cuando el responsable realice la primera notificación deberá informar si proporcionará más información a posteriori. También podrá aportar información adicional mediante comunicaciones intermedias a la autoridad de control bajo petición de esta, o cuando el responsable considere adecuado actualizar la situación de la misma.

# Notificación externa de incidentes.

- Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación deberá realizarse igualmente, y en ella deberán constar y justificarse los motivos de la dilación.

- Las notificaciones deben ser sean claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

- Es necesario que cualquier brecha de la seguridad de los datos personales, hechos relacionados, efectos y las medidas correctivas adoptadas así como la propia notificación, se registre y justifique documentalmente por el responsable, de modo que esta documentación permita a la autoridad de control verificar el cumplimiento de la obligación de notificación en todo su contenido.

# Notificación externa de incidentes.

- La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la sede electrónica de la agencia, en https://sedeagpd.gob.es/sede-electronica-web/

- A cada notificación se le asignará una referencia que el responsable deberá mantener e incluir en las sucesivas comunicaciones relacionadas si las hubiera, con el fin de proporcionar un seguimiento completo del incidente.

# Notificación externa de incidentes.

- Cuando la brecha de seguridad pueda entrañar un alto riesgo para los derechos y libertades de los titulares de los datos, el responsable del tratamiento deberá comunicar a los afectados, sin dilación indebida, la brecha de seguridad.

- Existen diversos factores a tener en consideración para decidir si se ha de realizar la comunicación a las personas afectadas:

- · Cuáles son las obligaciones legales y contractuales.

- · Riesgos que comporta la pérdida de los datos: daños físicos, daños reputacionales, etc.

- · Existe un riesgo razonable de suplantación de identidad o fraude (en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información estaba seudonimizada o cifrada).

- · Hasta qué punto la persona afectada puede evitar o mitigar posibles daños posteriores.

# Notificación externa de incidentes.

- Si después del análisis correspondiente es necesario realizar la notificación pero se prevé que la comunicación a los afectados puede comprometer el resultado de una investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la autoridad de control.

- La comunicación a los afectados se realizará a la mayor brevedad posible, en un lenguaje claro y sencillo y siempre en estrecha cooperación con la autoridad de control y las autoridades policiales, de acuerdo con sus orientaciones.

# Notificación externa de incidentes.

- Esta comunicación, debería contener como mínimo:
- · Datos de contacto del Delegado de Protección de Datos, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- · Descripción general del incidente y momento en que se ha producido.
- · Las posibles consecuencias de la brecha de la seguridad de los datos personales.
- · Descripción de los datos e información personal afectados.
-

# Notificación externa de incidentes.

- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.

- · Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

- La notificación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

- La notificación indirecta, a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa, se utilizará cuando para la notificación directa los costos sean excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo porque se desconocen, o los datos de contacto no están actualizados).