Brechas de seguridad

Taller práctico

FUNDACIÓN COMPLUTENSE

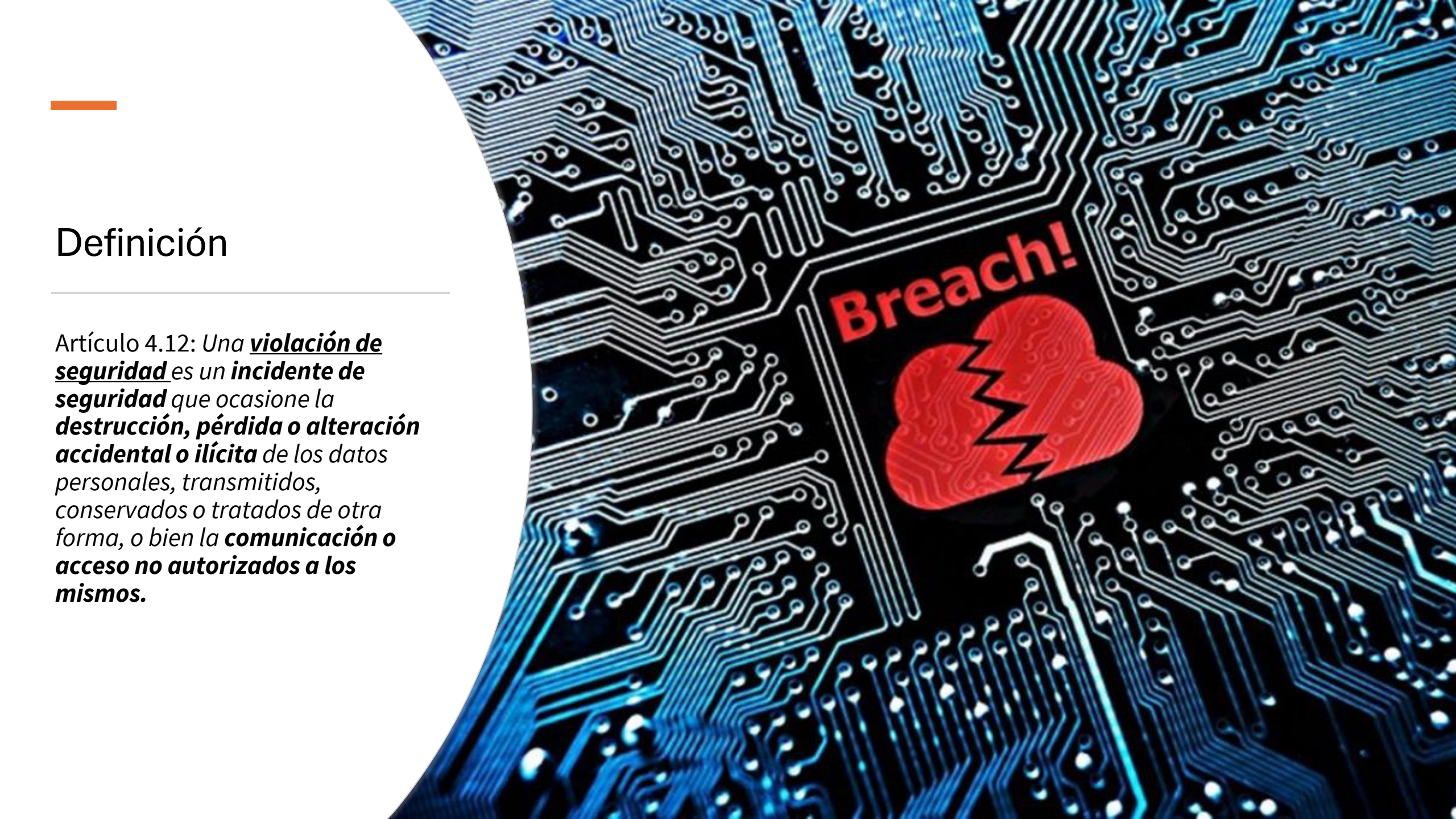
FUNDACIÓN COMPLUTENSE

INDICE

- **Teoría**
  - Incidencia
  - Incidente de seguridad
  - Brecha de Seguridad.
- **Caso Práctica 1**
  - Robo de un portátil
- **Caso Práctica 2**
  - Eliminación de un soporte físico
- **Caso Práctica 3**
  - Intrusión y Rasomware

Definición

Artículo 4.12: *Una* ***violación de seguridad*** *es un* ***incidente de seguridad*** *que ocasione la* ***destrucción, pérdida o alteración accidental o ilícita*** *de los datos personales, transmitidos, conservados o tratados de otra forma, o bien la* ***comunicación o acceso no autorizados a los mismos.***



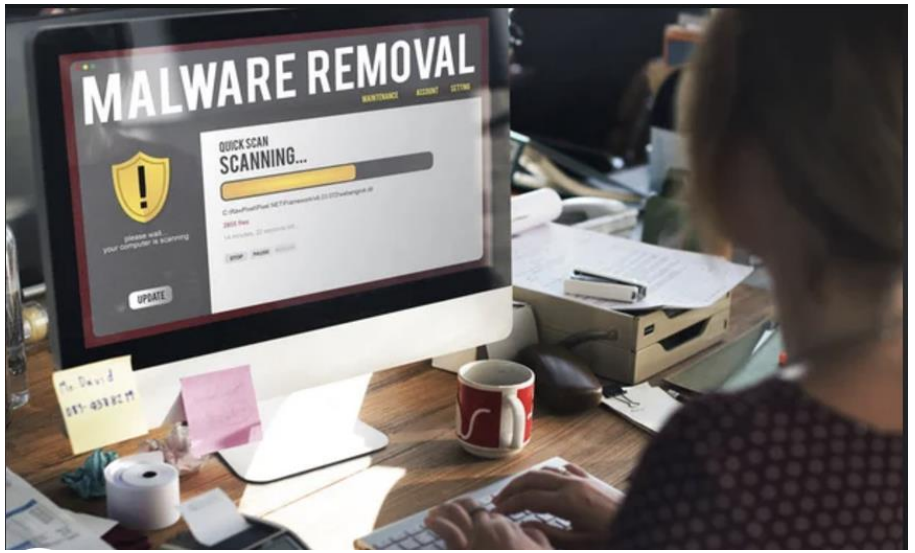
No es brecha de seguridad

Ámbito doméstico

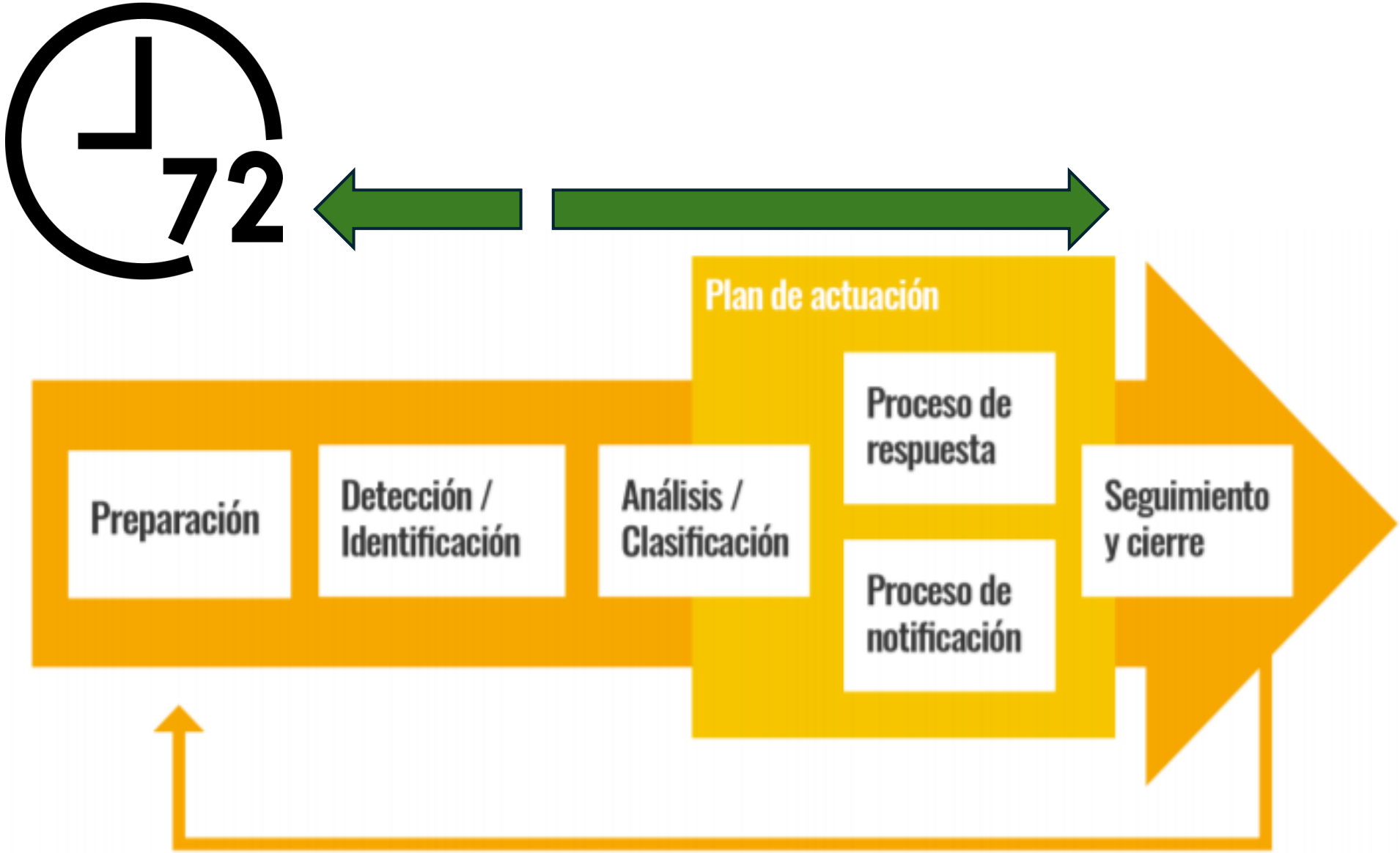
No afecten a datos personales

Incidencia informática

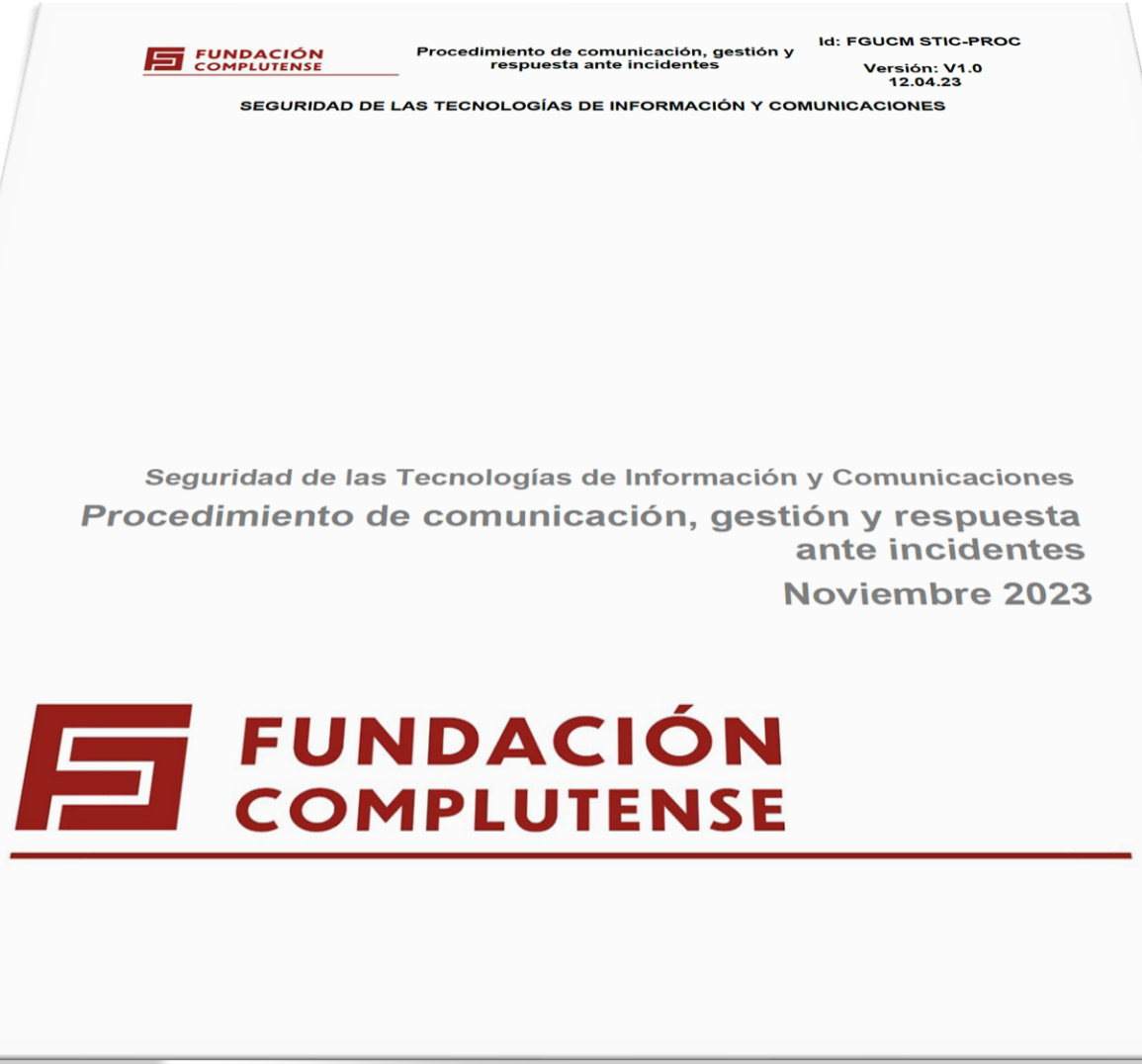
Es incidencia pero no brecha



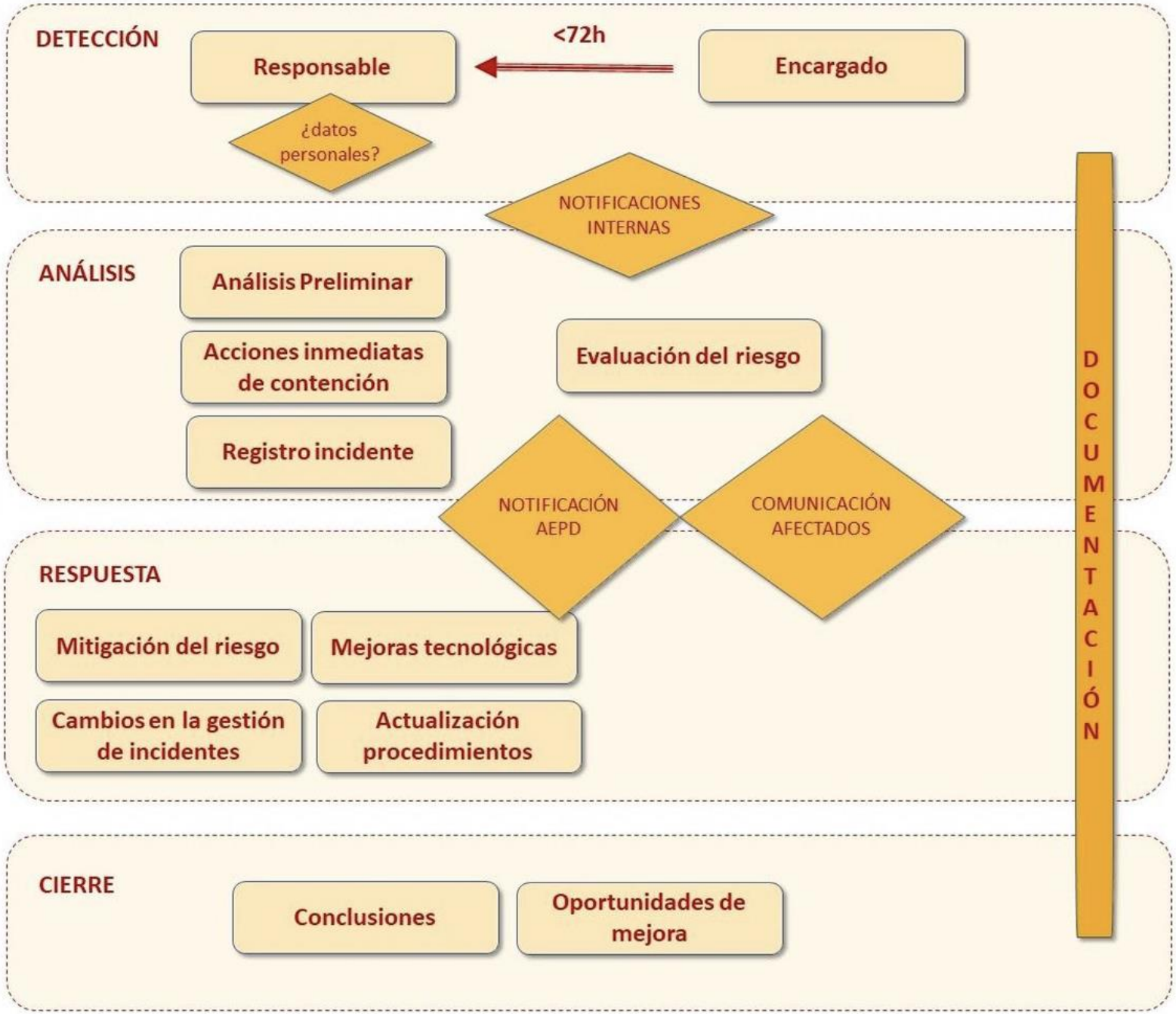
Proceso general de detección y reporte



¿Y en la Fundación?

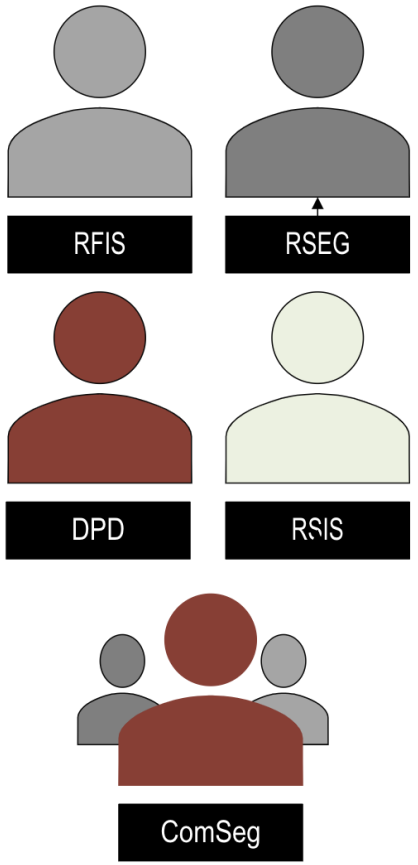


detalles que permitan comunicar de forma efectiva.



FUNDACIÓN COMPLUTENSE

Detección y reporte



Plazo

¿A partir de qué momento?

Debe considerarse que un responsable del tratamiento **«tiene constancia»** cuando tenga **un grado razonable de certeza** de **que se ha producido un suceso que compromete datos personales.**

Tipología según RGPD

Confidencialidad

Cuando se produce una **revelación no autorizada** o accidental de los datos personales, o el acceso a los mismos

Disponibilidad

Cuando se produce una **pérdida de acceso** accidental o no autorizada a los datos personales, o la destrucción de los mismos

Integridad

cuando se produce una **alteración no autorizada** o accidental de los datos personales

FUNDACIÓN COMPLUTENSE

¿A quién notificar?

aepd agencia española protección datos

IMPACTO EN LA ORGANIZACIÓN

CRÍTICO	CCN-CERT centro criptológico nacional
MUY ALTO	
ALTO	
MEDIO	NO ES OBLIGATORIO
BAJO	

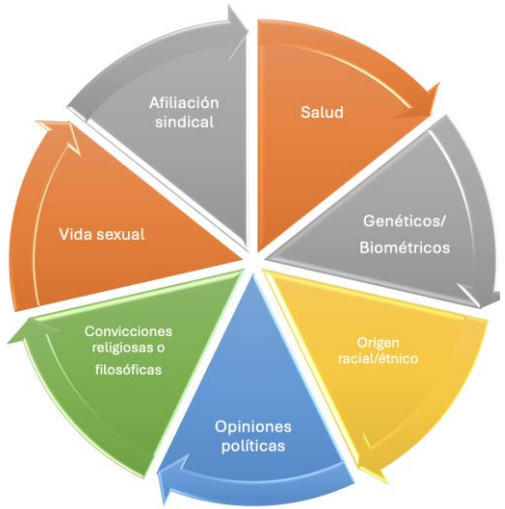
No es obligatorio notificar todas las brechas. El RGPD prevé una **excepción** a esta obligación **cuando**, conforme al principio de responsabilidad **podamos garantizar que es improbable que la brecha entrañe un riesgo para los derechos y las libertades** de las personas físicas.

PROBABILIDAD

	Baja/Limitada	Media	Alta	Muy Alta
Muy alta	VALORAR COMUNICACIÓN	OBLIGATORIA COMUNICACIÓN		
Alta				
Baja				
Improbable				
	Inconvenientes muy limitados y reversibles	Daño limitado, que podrán superar a pesar de algunas dificultades	Las consecuencias afectan a derechos fundamentales, pero pueden revertirse	Daña derechos fundamentales y libertades públicas de forma irreversible

GRAVEDAD DEL IMPACTO

Datos especialmente protegidos (Artículo 9)



CASO PRÁCTICO 1º

ROBO DE PORTATIL

Exposición

Los empleados de una empresa proveedora de servicios tienen permitido la salida y uso de los dispositivos de trabajo fuera de la ubicación principal.

Tras un desplazamiento a la sede de uno de sus clientes, el ordenador portátil de uno de esos empleados fue sustraído, junto con otros enseres, y sospecha que fue en el tren, al quedarse dormido tras una dura jornada de trabajo.

- El dispositivo contenía nombres, apellidos, sexo, direcciones y fecha de nacimiento de más de 100.000 clientes.
- Debido a la indisponibilidad del dispositivo robado, no fue posible determinar si también se habían visto afectadas otras categorías de datos personales.
- El acceso al disco duro del ordenador **no estaba protegido** por ninguna contraseña.
- Los datos personales pudieron recuperarse de las copias de seguridad disponibles diariamente.

INCIDENCIA ☑

BRECHA ☑

DISPONIBILIDAD ☒

INTEGRIDAD ☒

CONFIDENCIALIDAD ☑

aepd agencia española protección datos ☑

CCN-CERT centro criptológico nacional ☒

- **Revisión de las directivas de seguridad de los soportes (permisos de administrador)**
- **Inventariado de activos.**
- **Publicación en página web corporativa**

CASO PRÁCTICO 2º

ELIMINACIÓN DE UN SOPORTE FÍSICO

Exposición

Durante una mudanza por cambio de ubicación, se pierden varios archivadores de papel de un centro de rehabilitación de drogodependientes.

Se conoce que sólo ha sido un archivador porque no figura en el inventario de entrada (sí en el de salida) y hasta que no haya una identificación por parte del titular de la persona a quien pertenecía, no se dispone de la información suficiente acerca de si hay datos personales vinculados

FUNDACIÓN COMPLUTENSE

- Los archivadores contenían **datos básicos de identidad** de familiares de los pacientes admitidos en el centro, sin llevar datos de salud aparejados.
- Los datos **solo se almacenaban en papel** y el personal de administración no disponía de ninguna copia de seguridad.
- Los archivadores estaban guardados en un cajón o una sala cerrados, y el centro no disponía de un **régimen de control de acceso** ni de ninguna otra medida de salvaguardia para la documentación en papel.

INCIDENCIA ☑

BRECHA ☑

DISPONIBILIDAD ☑

INTEGRIDAD ☒

CONFIDENCIALIDAD ☑

aepd agencia española protección datos ☑

CCN-CERT centro criptológico nacional ☒

- Revisión de la **normativa sobre almacenamiento y procesos de archivo**
- **Revisión de ubicaciones y armarios** para comprobación de cerraduras/medidas de control de acceso.

CASO PRÁCTICO 3º

INTRUSIÓN Y RAMSONWARE

Exposición

Uno de los servidores utilizados por una empresa municipal fue objeto de un ataque con programas de secuestro y al atacante cifró sus datos (ramsonware).

Se desconoce el proceso de intrusión, pero se considera que uno de los ordenadores conectados a la red carecía de credenciales o permitía el acceso con contraseñas poco robustas.

Se comprueba que no se ha pedido rescate ni se amenaza con la publicación de la incidencia en Internet

FUNDACIÓN COMPLUTENSE

- Se abre investigación interna asistida por la empresa de ciberseguridad.
- Solo han **cifrado los datos, sin exfiltrarlos** (Los registros no muestran ningún flujo de datos de salida en el intervalo del ataque).
- Los datos personales afectados por la violación se refieren a los empleados y usuarios, unas pocas decenas de personas en total. No se han visto afectadas categorías especiales de datos.
- No se disponía de copias de seguridad en formato electrónico.
- La mayoría de los datos se recuperaron a partir de copias de seguridad en papel. La recuperación de los datos duró cinco días laborables y provocó retrasos menores

INCIDENCIA ☑

BRECHA ☑

DISPONIBILIDAD ☑

INTEGRIDAD ☒

CONFIDENCIALIDAD ☒

aepd agencia española protección datos ☑

CCN-CERT centro criptológico nacional ☑

- **Análisis del motivo que provoca el acceso no autorizado**
- **Actualización de los procesos de backup**
- **Comprobar viabilidad de cifrado en reposos.**

FUNDACIÓN COMPLUTENSE

¿Preguntas?