Protección de datos

Sesión de formación laboral

ÍNDICE

Introducción

¿Qué es la protección de datos? (I)

“Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan”.

Art. 8 Carta Derechos Fundamentales UE

“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.” (Art. 18 Constitución Española)

Un Derecho Fundamental

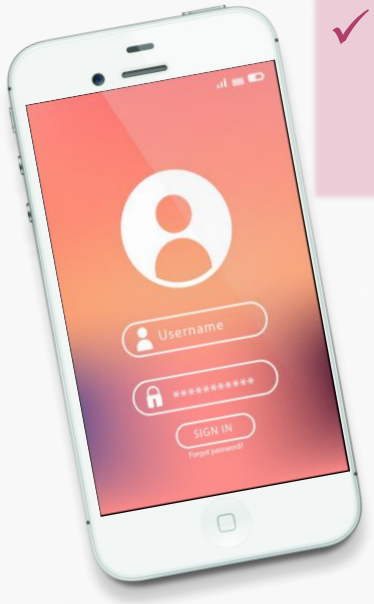
El tratamiento de datos personales debe estar concebido para servir a la humanidad. No es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Considerando 4 GDPR

¿Qué es la protección de datos? (II)

NORMATIVA APLICABLE

- ✓ Reglamento General de Protección de Datos (RGPD)
- ✓ Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)
- ✓ GDPR: nuevo modelo basado en el control del cumplimiento y el principio de responsabilidad proactiva



EL GDPR s**e aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero**

La normativa **no** protege el tratamiento de datos que se realice en el ámbito doméstico, personal y familiar.

¿Qué se considera un dato personal?

→ "Toda información sobre una **persona física identificada** o **identificable** (interesado);

Es un dato personal…

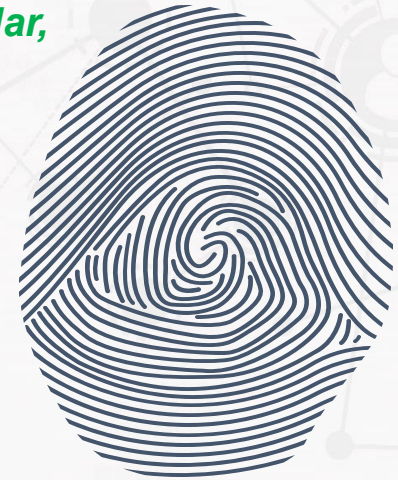
… "*un **nombre**, un **número de identificación**, datos de **localización**, un **identificador en línea** o **uno o varios elementos propios de la identidad física**, **fisiológica**, **genética**, **psíquica**, **económica**, **cultural** o **social** de dicha persona*"

Y también

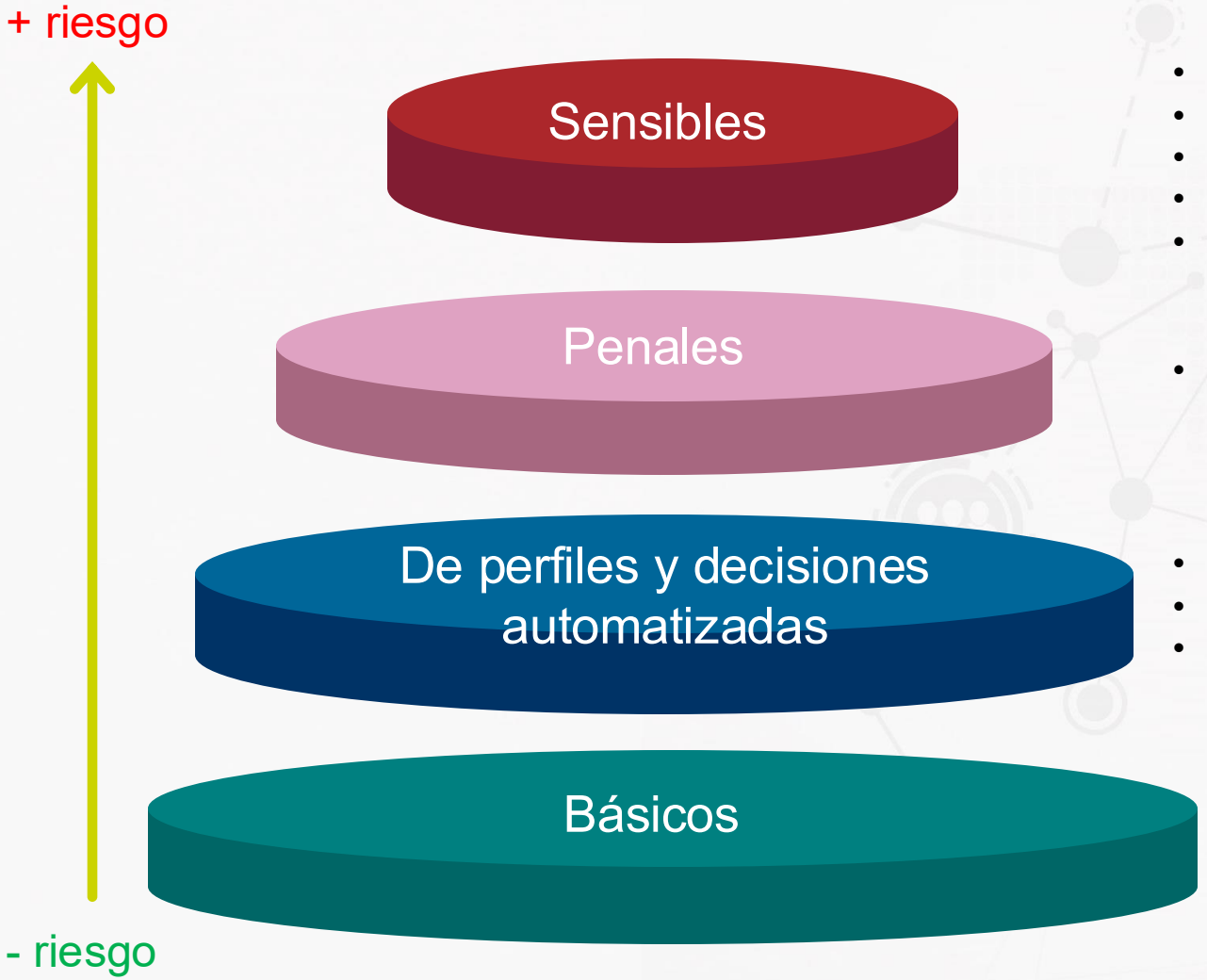
correo electrónico, nº teléfono**, **Historia clínica, huella dactilar,
IP o dirección MAC de un dispositivo móvil
Datos de cuenta bancaria y tarjeta de crédito

NO es un dato personal…

La denominación social o los datos de una sociedad



¿Qué tipos de datos personales hay?



- Opinión o ideología política
- Huella dactilar
- Datos de salud
- Creencias religiosas
- Orientación sexual

- Datos relativos a condenas e infracciones penales

- Preferencias, intereses y gustos
- Comportamiento o costumbres
- Rendimiento profesional

- Nombre y apellidos
- Nº DNI
- Nº CC y tarjeta de crédito
- Correo electrónico

Intervinientes

AUTORIDAD DE CONTROL
(Agencia Protección de Datos)

ENCARGADO DEL TRATAMIENTO

DELEGADO DE PROTECCIÓN DE DATOS

RESPONSABLE DEL TRATAMIENTO

INTERESADO
(usuario, consumidor, cliente)

¿Qué ocurre si incumplimos?

Régimen sancionador

Las sanciones económicas por el incumplimiento de las obligaciones en materia de protección de datos pueden ser desde:

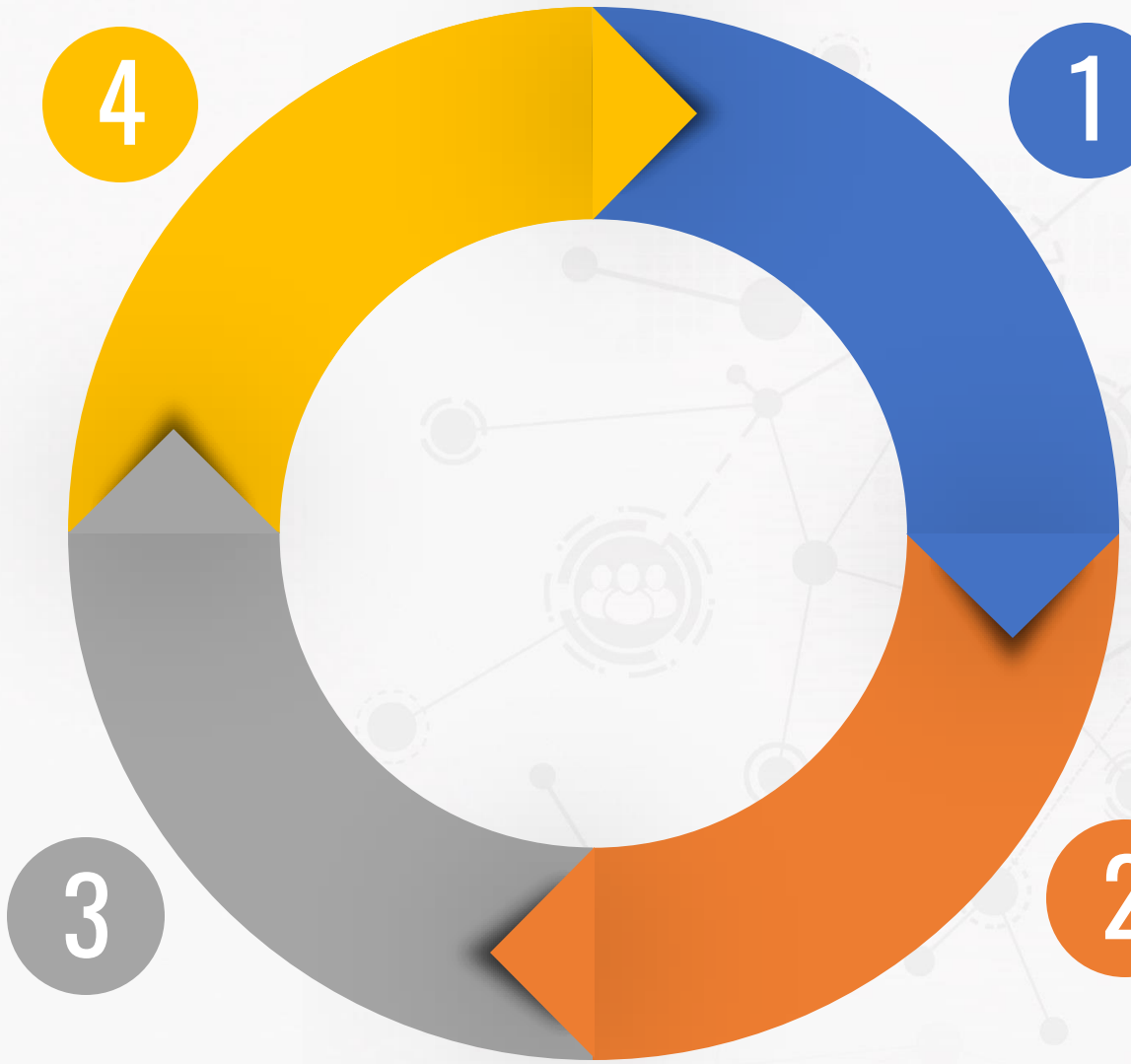
¿Qué ocurre si incumplimos? (V)

En caso de sanción,

¿quién

responde?

¿Qué ocurre si incumplimos? (VI)



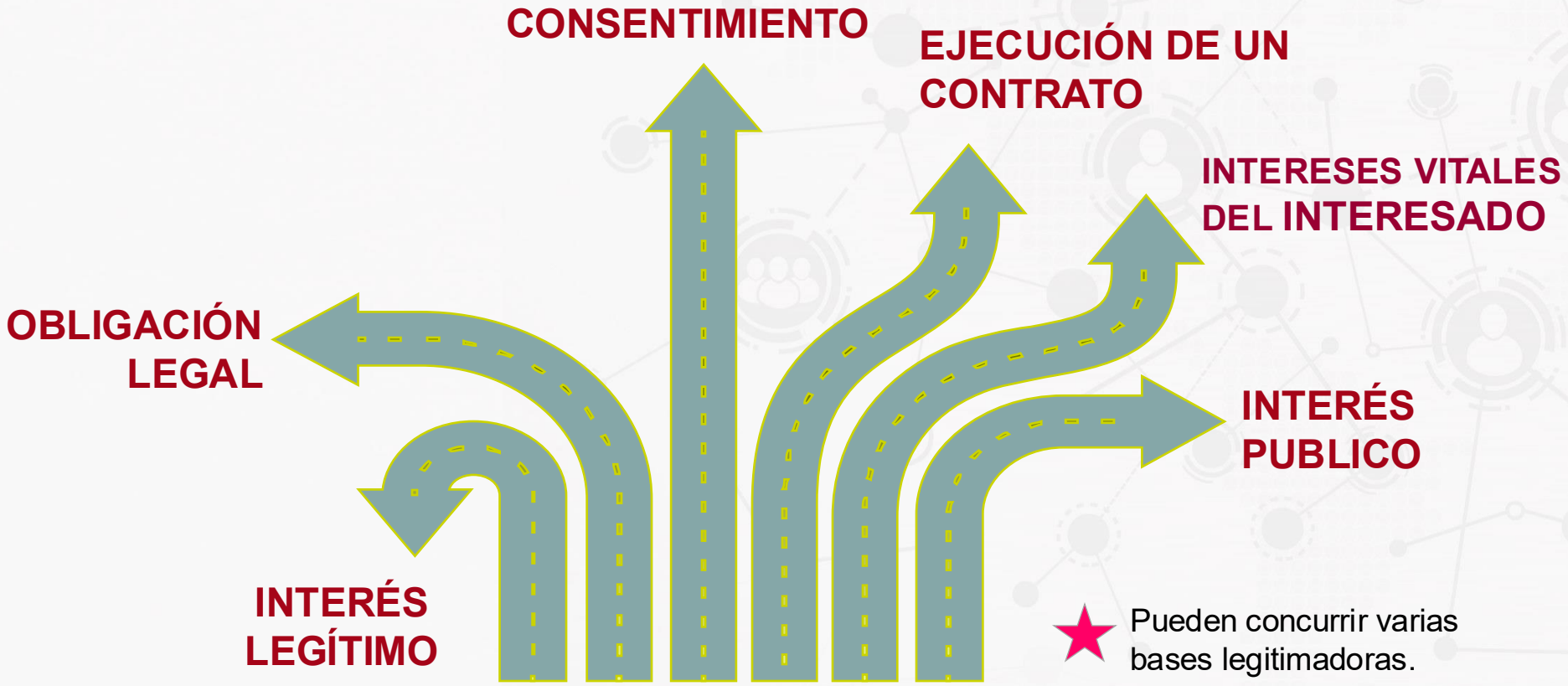
1. RESPOSABLE DE TRATAMIENTO
2. ENCARGADO DE TRATAMIENTO
3. RESPONSABLE DE SEGURIDAD
4. DELEGADO DE PROTECCIÓN DE DATOS

Tratamiento de datos

Requisitos para el tratamiento de datos

1. Base legitimadora
2. Principios legales
3. Información al usuario
4. Derechos de los interesados
5. Comunicación, transferencia y cesión de datos

1. Base legitimadora (I)



★ Pueden concurrir varias bases legitimadoras.

1. Base legitimadora (II)

CONSENTIMIENTO

LIBRE → INEQUÍVOCO → ESPECÍFICO → INFORMADO

- ☐ ACEPTO (la política de privacidad / las Condiciones de Uso / el envío de información comercial, etc.)
- ☒ Marque esta casilla si NO quiere (recibir publicidad / que sus datos sean tratados con la siguiente finalidad)
- ☒ Si no dice nada en el plazo de 30 días, entenderemos que usted acepta el tratamiento de sus datos

1. Base legitimadora (III)

INTERÉS LEGÍTIMO

Tarjetas de visita y datos de contacto

Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes:

***SALVO QUE NOS PODAMOS BASAR** una relacion comercial preexistente y para ofrecer servicios relacionados con nuestra actividad empresarial.*

Art 21.2 LSSI (Ley de servicios de la sociedad de la información y de comercio electrónico)

1. Base legitimadora (III)

INTERÉS LEGÍTIMO

Tarjetas de visita y datos de contacto

Se pueden tratar cuándo:

a) *el tratamiento se refiera únicamente a los datos necesarios para la localización profesional y,*

b) *la finalidad del tratamiento sea únicamente para mantener relaciones de cualquier índole con la persona jurídica donde el afectado preste sus servicios.*

Art 19 LOPDGDD

Vale para trabajadores por cuenta ajena y por cuenta propia (autónomos)

1. Base legitimadora (III)

INTERÉS LEGÍTIMO

Tarjetas de visita y datos de contacto

Se prohíbe la realización de llamadas comerciales a no ser que nos basemos en el consentimiento o en un interés legítimo.

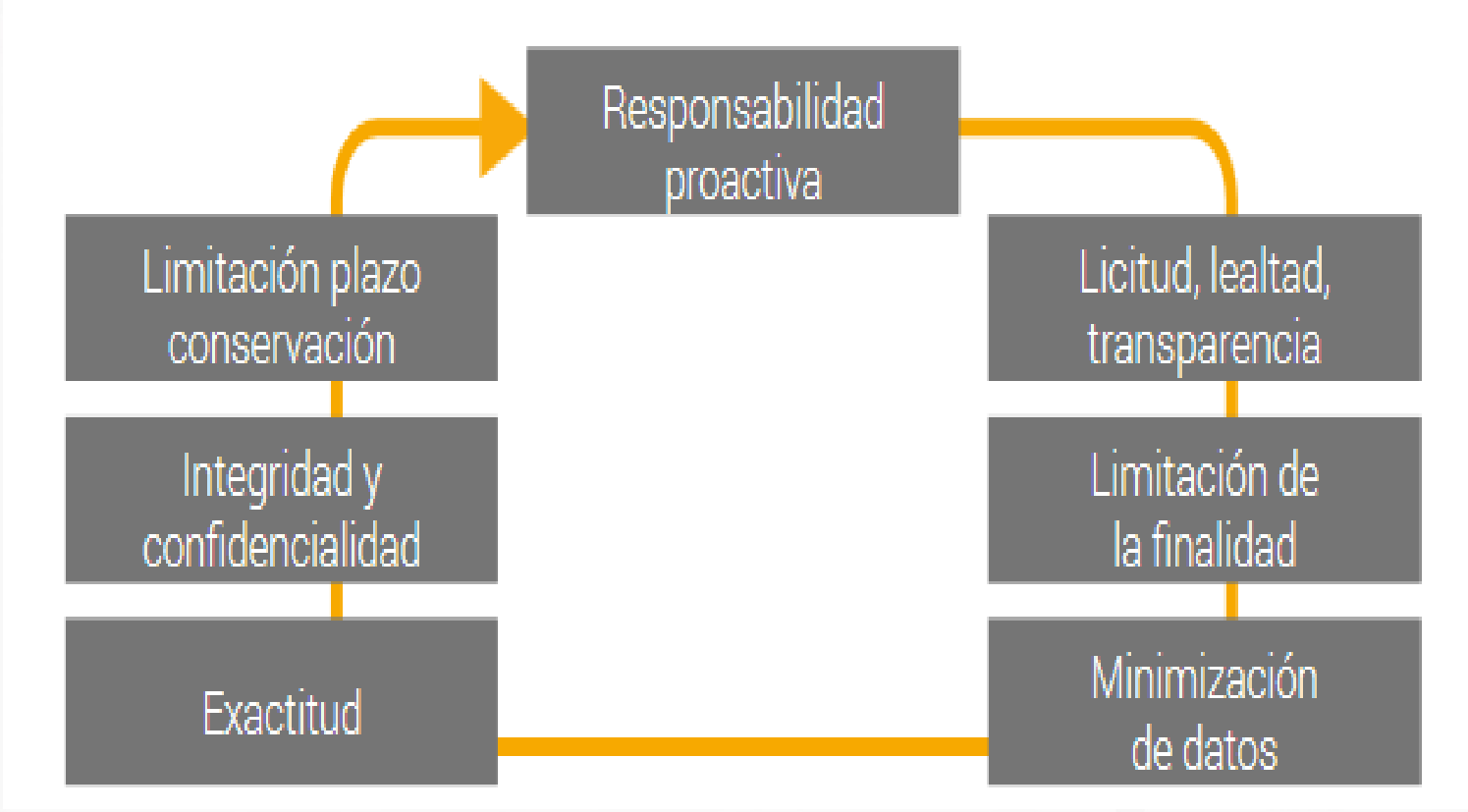
El artículo 19 LOPD legítima el tratamiento de datos de contacto profesional de personas físicas siempre que la FINALIDAD sea mantener relaciones profesionales con su empresa.

Por tanto, ésta será la única finalidad por la cual puedan tratarse dichos datos en base al interés legítimo, siendo irrelevante que se realicen por medios electrónicos o no.

Vale para emails y llamadas

Nueva Ley de Telecomunicaciones: art. 66 y Circular AEPD

2. Principios



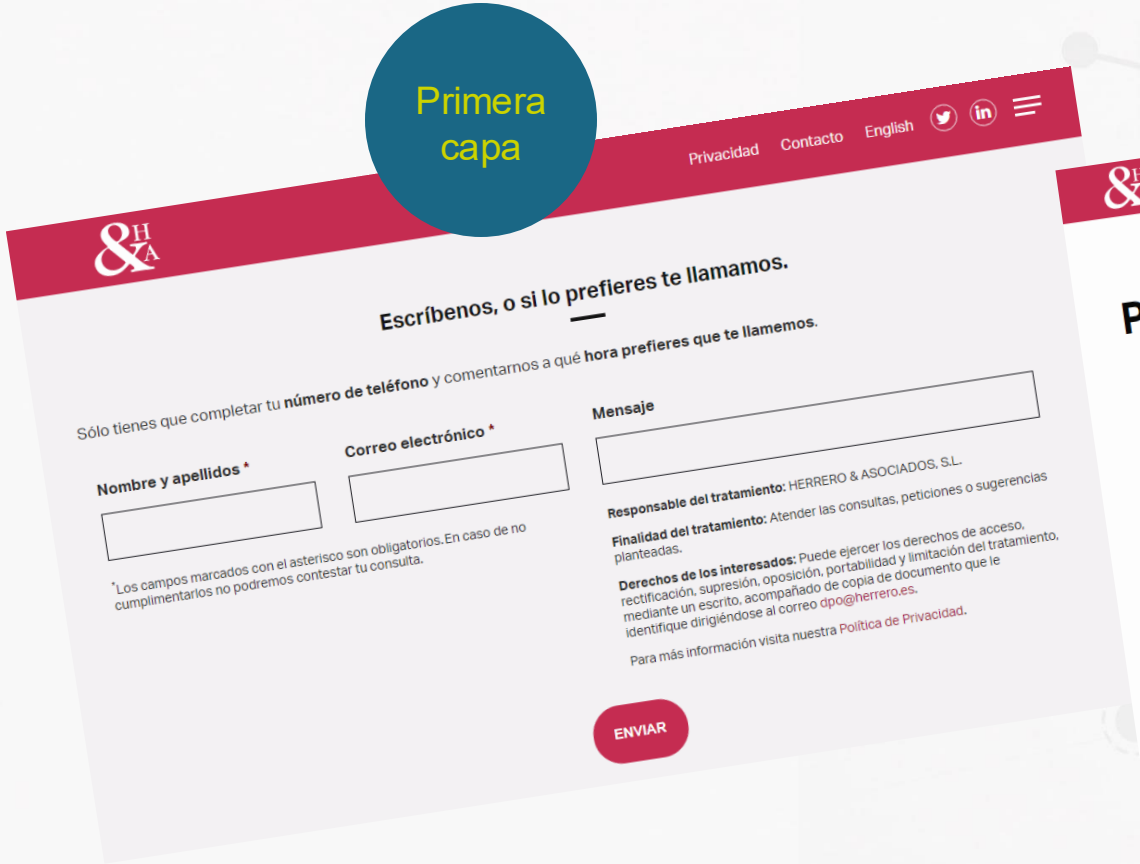
3. Información (I)

"***Información clara y lenguaje sencillo***"

- Identidad y datos de contacto del Responsable y del DPO
- Finalidad y base legitimadora
- Destinatarios de los datos
- Plazo de conservación de los datos
- Existencia de los derechos que posee el interesado
- Origen y fuente de los datos (si no los proporciona el propio interesado)
- Existencia de decisiones automatizadas o elaboración de perfiles

3. Información (II)

Primera capa



Segunda capa

4. Derechos de los interesados

5. Comunicación, transferencia y cesión de datos

ENCARGADO DEL TRATAMIENTO

Los proveedores que nos prestan un servicio necesario para nuestro negocio. Es necesario firmar un contrato de Encargado del Tratamiento.

CESIÓN DE DATOS

La responsabilidad del tratamiento pasa a la empresa a quien se ceden los datos. Se requiere el consentimiento de los interesados.

TRANSFERENCIAS INTERNACIONALES

Transferencias de datos fuera del EEE. Se requieren medidas adicionales.

6. Medidas de seguridad

Jurídicas

- Registro de Actividades del Tratamiento
- Política de privacidad
- Acuerdos de confidencialidad empleados y contratos de Encargados del Tratamiento

Auditoría y control

- Análisis de riesgos
- Evaluaciones de Impacto
- Detección de incidentes y brechas de seguridad

Técnicas

- Copias de seguridad
- Encriptación de los datos sensibles
- Control de accesos
- Seguridad en el correo electrónico

Organizativas

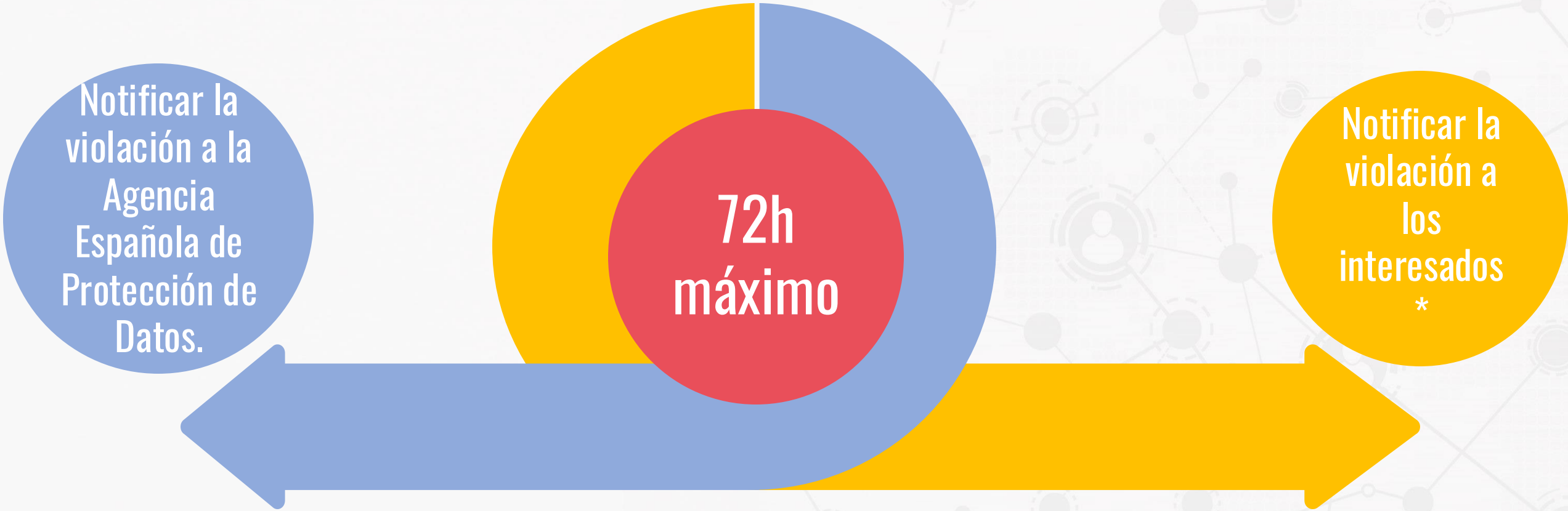
- Formación y concienciación a los empleados
- Procedimientos internos
- Delegado de protección de datos

6. Medidas de seguridad jurídicas y organizativas

Protocolos

- ✓ Política de privacidad
- ✓ Protocolo para el ejercicio de los derechos de los interesados
- ✓ Plazos legales de conservación
- ✓ Protocolo de actualización y conservación de datos
- ✓ Protocolo para el bloqueo de datos
- ✓ Procedimiento de notificación de violaciones de seguridad de datos a la autoridad de control

Procedimiento actuación ante brechas de seguridad



* a no ser que se hayan aplicado medidas técnicas y organizativas apropiadas de protección para hacer ininteligibles los datos a personas no autorizadas, y/o se hayan minimizado los riesgos

6. Medidas de seguridad técnicas

Phishing

spam

6. Medidas de seguridad técnicas

INGENIERÍA SOCIAL

PROBLEMA

INTERNO: ROBO DE DATOS

EXTERNO: REPUTACIÓN DE MARCA

6. Medidas de seguridad técnicas (XII)

- Uso de software únicamente autorizado.
- No abrir ningún enlace ni descargar ficheros sospechosos.
- Cifrar los envíos de información sensible.
- Utilizar contraseñas seguras en función de la criticidad de la información.
- Hacer un borrado seguro de la información que ya no sea necesaria, teniendo en cuenta los plazos legales de conservación.
- No utilizar plataformas como Dropbox o WeTransfer para enviar información con datos personales o información empresarial.
- Bloquear nuestra sesión cuando no estemos en nuestro puesto de trabajo.
- Uso de pendrives solo para información no confidencial o encriptados.
- Informar de cualquier violación de seguridad que detectes al equipo responsable.

Lucía Martín-Sanz

Abogada
Asesoria Jurídica,
Responsable Derecho Digital y NNTT
lmartin@herrero.es

Mario Romero

Responsable ciberseguridad
mromero@herrero.es

España:

- MADRID
- ALICANTE
- BARCELONA
- BILBAO
- CORUÑA
- LEÓN
- MURCIA
- MÁLAGA
- SEVILLA
- VALENCIA
- VIGO

Oficinas Internacionales:

- LISBOA
- CIUDAD DE MÉXICO
- RÍO DE JANEIRO
- BUENOS AIRES
- BOGOTÁ