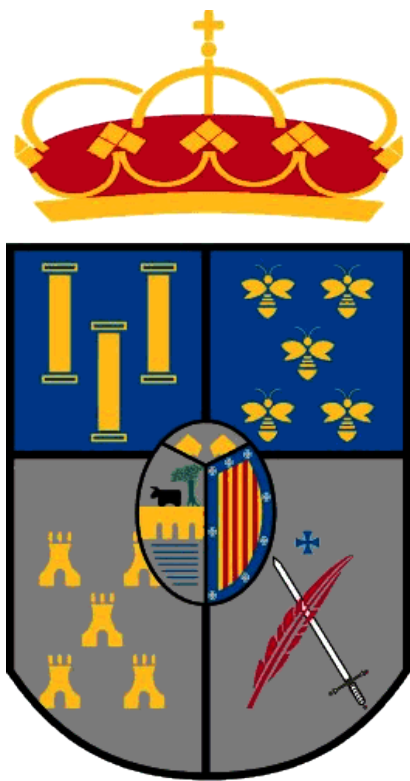


PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL



Diputación de Salamanca

ÍNDICE

1. Agencia Española de Protección de Datos
2. Marco Regulador
3. Tratamiento de datos de carácter personal
4. Legitimación del tratamiento
5. Legitimación del tratamiento: menores
6. ¿Cómo hay que tratar los datos?
7. Limitación de la finalidad
8. ¿Qué datos podemos recabar y cuanto tiempo guardarlos?
9. Plazos de conservación
10. Responsable VS Encargado
11. Obligaciones de las organizaciones públicas o privadas
12. Derechos en materia de protección de datos
13. Riesgos y buenas prácticas de los puestos de trabajo
14. Buenas prácticas
15. Protegiendo la información de la empresa
16. Video de INCIBE sobre concienciación en el puesto de trabajo.

Prevista en el CONVENIO 108 DEL CONSEJO DE EUROPA, 1981

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- Independiente
- Presupuesto propio
- Plena autonomía funcional
- Personalidad jurídica
- Plena capacidad pública y privada
- Autoridad de control
 - Creación en 1992 y comienzo de su función en 1994



Diputación
de Salamanca

- **Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ CE (Reglamento general de protección de datos RGPD).**
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, en lo no derogado por la Ley Orgánica 3/2018 (disposición transitoria primera).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, (sujeta al Derecho Administrativo tanto en el ejercicio de sus competencias como en su régimen patrimonial y de contratación).

¿QUÉ ES UN DATO PERSONAL?

Toda información sobre una persona física identificada o identificable («el interesado»).

Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente.

CATEGORÍAS ESPECIALES DE DATOS

- Los que revelen ideología, afiliación sindical, religión y creencias
- Hagan referencia al origen racial, a la salud y a la vida sexual
- Se refieran a la comisión de infracciones penales o administrativas
- Datos biométricos y genéticos

¿QUÉ SE ENTIENDE POR TRATAMIENTO DE DATOS?

Cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente, como la recogida, registro, estructuración, conservación, modificación, o consulta.

LEGITIMACIÓN DEL TRATAMIENTO

¿De quién son los datos de carácter personal?

Cada persona es titular de sus respectivos datos de carácter personal

¿Cuál es la edad para que los menores puedan prestar consentimiento para tratar sus datos personales?

RGPD **16 años**

Estados de la Unión Europea podrán rebajarlo hasta un mínimo de **13 años**.

Art 7 LOPD **14 años**, para menores de esa edad el otorgamiento lo deberán dar sus padres o tutores.

Otras bases sin necesidad de contar con la autorización de su titular en supuestos en que una norma con rango de Ley autorice el tratamiento o incluso obligue al responsable a llevarlo a cabo.

Diputación
de Salamanca

LEGITIMACIÓN DEL TRATAMIENTO: MENORES

¿Puede un menor de 14 años ejercitar los derechos contemplados en el RGPD?

Por quien ostente la patria potestad o por sus tutores.

Mayores de 14 años habilitados para el ejercicio de los derechos.

¿Se pueden recabar y tratar datos personales de menores?

Sí, siempre que se observe lo dispuesto en el RGPD

Cuando la recogida y tratamiento de datos responda al consentimiento, hay que tener en cuenta que deberá ser **expreso** y que cuando se trate de menores de 14 años lo han de prestar sus **padres o tutores**.

Los mayores de 14 años ellos mismos salvo en aquellos casos previstos legalmente en los que se exija asistencia por su padres o tutores.



¿CÓMO HAY TRATAR LOS DATOS?

LÍCITA -

LEAL -

TRANSPARENTE

Minimización de los datos

Finalidad legítima

¿PUEDE UNA INSTITUCIÓN PUBLICAR UN LISTADO DE PERSONAS INSCRITAS A UNA ACTIVIDAD?

SÍ

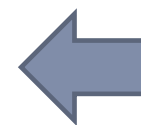
Criterio provisional para garantizar la protección frente a la divulgación del documento nacional de identidad (DNI), del número de identidad de extranjero (NIE), así como del pasaporte o documento equivalente.

- **DNI** con formato 12345678X, se publicarán los dígitos que en el formato ocupen las posiciones cuarta, quinta, sexta y séptima. Siguiendo el ejemplo anterior: ***4567**.
- **NIE** con formato L1234567X, se publicarán los dígitos que en el formato ocupen las posiciones, cuarta, quinta, sexta y séptima, evitando el primer carácter alfabético. En el ejemplo: ****4567*.

LIMITACIÓN DE LA FINALIDAD

Determinados - solo recabar los datos que necesitemos.

Explícitos - afectado debe saber para que se están recogiendo sus datos personales.



DEBER DE
INFORMAR

Legítimos - solo deberemos usar los datos personales en todo aquello a lo que estemos autorizados.

Excepciones

- con fines de archivo en interés público
- finalidad de investigación científica e histórica
- fines estadísticos

ANONIMIZACIÓN

¿QUÉ DATOS PODEMOS RECABAR Y CUANTO TIEMPO GUARDARLOS?

Criterio para guardar los datos personales **PROPORCIONALIDAD**

EXCEPCIONES:

- Interés Histórico
 - Científico
 - Informativo
- } INTERÉS GENERAL

Pautas para no extralimitarnos al recabar datos personales:

1. Autorregulación
2. Minimización
3. Utilizar herramientas automáticas de borrado
4. Utilizar métodos de almacenamiento fiables

Periodos de prescripción

Circunstancias que **por ley** nos obligan a conservar la información durante un determinado tiempo:

- Código de Comercio - 6 años
- Tributos y Seguridad Social – 4 años reclamaciones Agencia tributaria ó 5 años Seguridad Social
- Videovigilancia – no más de 1 mes, pero supuestos de Ley de Seguridad Ciudadana 3 años
- Sanidad – 1 año
- Servicios mercantiles – 4 meses

PLAZOS DE CONSERVACIÓN

El **ESTRICTAMENTE NECESARIO** para la finalidad para la que fueron recabados.

Una vez que los datos personales dejen de ser necesarios para esta finalidad, deben ser eliminados o bloqueados.

ANTES

INCUMPLIMIENTO DE PLAZO
INFRACCIÓN GRAVE – HASTA 300.000€

AHORA

LIMITACIÓN DEL PLAZO DE CONSERVACIÓN
MUY GRAVE – **HASTA 20 MILLONES € Ó CUANTÍA
EQUIVALENTE HASTA AL 4% DEL VOLUMEN DE
NEGOCIO ANUAL GLOBAL DEL EJERCICIO
FINANCIERO ANTERIOR**

Diputación
de Salamanca

RESPONSABLE VS ENCARGADO

- RESPONSABLE DEL TRATAMIENTO

Es la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso del mismo, bien por decisión directa o porque así le viene impuesto por una norma legal.



- ENCARGADO DEL TRATAMIENTO

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.



Diputación
de Salamanca

OBLIGACIONES DE LAS ORGANIZACIONES PÚBLICAS O PRIVADAS

- Registro de bases de actividades de tratamiento
- Adopción de medidas de seguridad y en caso necesario Análisis de riesgos.
- Notificación de brechas de seguridad a la Agencia Española de protección de Datos
- Evaluación de impacto sobre la protección de datos
- Designación interna del Delegado de Protección de Datos (DPO)
- Es recomendable la adhesión a Códigos de conducta
- Control de las Transferencias internacionales

Diputación
de Salamanca

DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS

DERECHOS:

- ACCESO
- RECTIFICACIÓN
- OPOSICIÓN
- SUPRESIÓN (DERECHO AL OLVIDO)
- LIMITACIÓN AL TRATAMIENTO
- PORTABILIDAD
- NO SER OBJETO DE DECISIONES INDIVIDUALIZADAS



¿Quiénes pueden ejercitar estos derechos?

Solo pueden ser ejercidos por sus titulares o representantes legales

¿Ante quién?

Ante los responsables del tratamiento

¿Hay obligación de contestar a los interesados?

Si, siempre

CUÁLES SON TUS DERECHOS DE PROTECCIÓN DE DATOS

La normativa de protección de datos te otorga una serie de derechos.

Para ejercerlos, debes dirigirte ante quien está tratando tus datos ("responsable")



Derecho de información

El responsable siempre debe identificarse, informarte para qué se utilizan tus datos y además decirte:

- La razón por la que tus datos son necesarios
- Hasta cuándo los conservará
- Cómo puedes ejercer tus derechos de protección de datos
- Cuál es la base jurídica del tratamiento
- Si los va a ceder a terceros o transferir a otros países
- Si los van a utilizar para elaborar perfiles tienes **derecho a oponerte si se adoptan decisiones automatizadas** que te afecten jurídicamente o de manera similar



Derecho de acceso

Utilízalo para saber si una entidad está tratando tus datos. Podrás obtener información sobre:

- Las categorías de los datos tratados, su finalidad y a quién se envían
- Si se producen transferencias internacionales de tus datos
- De quién se han obtenido y los plazos de conservación
- Si se elaboran perfiles y adoptan decisiones automatizadas
- Los derechos que te asisten



Derecho de rectificación

Te permite corregir tus datos o completarlos si son inexactos o incompletos.



Derecho de oposición

Puedes oponerte a que una entidad trate tus datos:

- Por motivos personales salvo que el responsable acredite un interés legítimo
- Cuando el tratamiento tenga por objeto el marketing directo



Derecho de supresión ("derecho al olvido")

Puedes solicitar la eliminación de tus datos personales cuando:

- Ya no sean necesarios para los fines para los que se recogieron
- Retires el consentimiento que diste, siempre que no haya otra causa que legitime el tratamiento
- Tus datos hayan sido tratados ilícitamente
- Te hayas opuesto a su tratamiento y no prevalezca el interés legítimo, o si el tratamiento tuviera por objeto el marketing directo
- Deban suprimirse para cumplir una obligación legal
- Se hayan obtenido siendo menor de edad en relación con los servicios de la sociedad de la información



Derecho a la limitación de tratamiento

Permite solicitar la suspensión del tratamiento de tus datos cuando:

- Impugnes su exactitud, durante el periodo en el que se comprueba
- Te opongas al tratamiento, mientras se verifica si prevalece el interés legítimo del responsable
- El tratamiento sea ilícito, pero te opones a su supresión y en su lugar solicitas que se limite
- Cuando los necesites para la formulación, ejercicio o defensa de reclamaciones



Derecho a la portabilidad

Cuando el tratamiento esté basado en tu consentimiento o en la ejecución de un contrato, y se efectúa por medios automatizados, puedes recibir tus datos en un formato que permita transmitirlos a otro responsable.

Más información sobre tus derechos y cómo ejercerlos en:

<https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos>

RIESGOS Y BUENAS PRÁCTICAS DE LOS PUESTOS DE TRABAJO

RIESGOS DE LOS PUESTOS DE TRABAJO:

- Información en papel al alcance de cualquier
- Falta de confidencialidad de los medios de comunicación tradicionales como el teléfono
- Accesos no autorizados a los dispositivos
- Infecciones por malware
- Robo de información

BUENAS
PRÁCTICAS



MESAS LIMPIAS

- Al acabar la jornada se debe guardar la documentación que se encuentre a la vista
- No apuntar a la vista usuarios y contraseñas
- No dejar al alcance de terceros dispositivos informáticos que se puedan desconectar como USB o discos duros.

BLOQUEO DE SESION

- Los dispositivos con los que se esté trabajando siempre deben estar bloqueados a no ser que esté en presencia de ellos.

SOFTWARE ACTUALIZADO

- Un dispositivo desactualizado es un riesgo para la seguridad de la organización, ya que un ciberdelincuente puede aprovechar vulnerabilidades.

ANTIVIRUS Y FIREWALL

- Herramientas que nos ayudan a proteger los sistemas informáticos.

DOCUMENTACIÓN SENSIBLE

- Guardar en un lugar seguro
- Accesible únicamente para personal autorizado
- No dejarla en impresoras y escáneres
- Almacenamiento adecuado
- Destrucción al terminar su ciclo de vida

CONTRATO DE CONFIDENCIALIDAD

- Acuerdos con las empresas que establecen compromiso de aplicar medidas de seguridad.

USO ADECUADO DE INTERNET Y SISTEMAS CORPORATIVOS

- Sitios no seguros y uso ilícito de recursos de la Diputación pueden conllevar incidentes de seguridad

SOFTWARE LEGÍTIMO

- Software ilegal puede terminar en una infección por malware del equipo

REPORTAR INCIDENTES DE SEGURIDAD

- Accesos no autorizados, denegaciones de servicio, infección por malware, robo de información de la empresa

USO SEGURO DE DISPOSITIVOS DE ALMACENAMIENTO EXTRAIBLE



PROTEGIENDO LA INFORMACIÓN DE LA EMPRESA

Hay 3 tipos de incidentes de seguridad que pueden afectar a la información de la empresa: **accidentales**, **intencionados** por parte de empleados por motivos propios o bajo la influencia o el soborno de ciberdelincuentes y **causados por ciberdelincuentes** a través de códigos maliciosos o malware.

¿Cómo podemos proteger nuestra información?

LOS TRES PILARES DE LA SEGURIDAD

Disponibilidad: hace referencia a que la información esté accesible cuando la necesitamos.

Integridad: característica de la información que protegemos para que esté libre de modificaciones y errores que impliquen cambios en su contenido.

Confidencialidad: propiedad por la que la información no se pone a disposición o no se revela a individuos, entidades o procesos no autorizados.



CLASIFICACIÓN DE LA INFORMACIÓN

Una de las partes más importantes para proteger la información de una empresa es clasificarla:

- Inventariado de los activos** con los que cuenta la organización, tanto en formato físico como en formato digital. Es conveniente catalogar otras características de los activos como su tamaño, ubicación o departamentos que intervienen en su gestión.
- Crear criterios de clasificación** para las actividades principales de la empresa, por ejemplo: *confidencial*, *restringida*, *uso interno* o *pública*.
- Etiquetar cada activo** según los criterios definidos, por ejemplo *[confidencial]Proyectos_2020.docx*, *[restringido]nóminas_2018.xlsx*
- Elaborar un listado** con los controles de seguridad que se llevarán cabo para proteger cada activo.



CIFRADO DE LA INFORMACIÓN

Mediante el cifrado de la información podemos ofuscar cualquier fichero y hacerlo inaccesible a otras personas que no sepan la clave de descifrado.



METADATOS, RIESGOS Y CÓMO ELIMINARLOS

Los metadatos son información muy valiosa que incluyen los ficheros digitales, como *nombres de usuario*, *fechas de creación o modificación de los documentos*, *ubicación de las fotografías*, *aplicación utilizada*, etc. Por eso es importante eliminarlos antes de enviar cualquier fichero o subirlo a la nube, ya que los ciberdelincuentes podrían acceder a ellos.



COPIA DE SEGURIDAD Y BORRADO SEGURO

Ante un incidente **una copia de seguridad puede marcar la diferencia** entre recuperarse o sufrir consecuencias críticas para el negocio. Cuando la información deja de ser útil para la empresa será necesario destruirla de forma segura, de tal manera que no vuelva a ser accesible.



ALMACENAMIENTO LOCAL, RED O NUBE

Pros y contras de cada tipo de almacenamiento:

- Local:** es de rápido acceso, siempre estará accesible a no ser que se produzca un fallo en el equipo.
- Red:** almacenamiento en un equipo de la red interna de la empresa que requiere de permisos para poder gestionar la información. En caso de que exista esta opción será la que debemos utilizar. De este modo, toda la información estará centralizada y se podrán aplicar las medidas de seguridad de forma más eficiente.
- Nube:** siempre estará accesible si se cuenta con Internet y los permisos adecuados. Por el contrario, existe la problemática de almacenar información confidencial fuera de la empresa, por lo que habrá que utilizar herramientas de cifrado para protegerla.

La **Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales** o LOPDGDD es aplicable a empresas, sociedades, comunidades y autónomos que realicen algún tipo de tratamiento de datos personales. Llevar a cabo un tratamiento incorrecto sobre los datos personales que gestiona la empresa puede suponer graves consecuencias para esta.

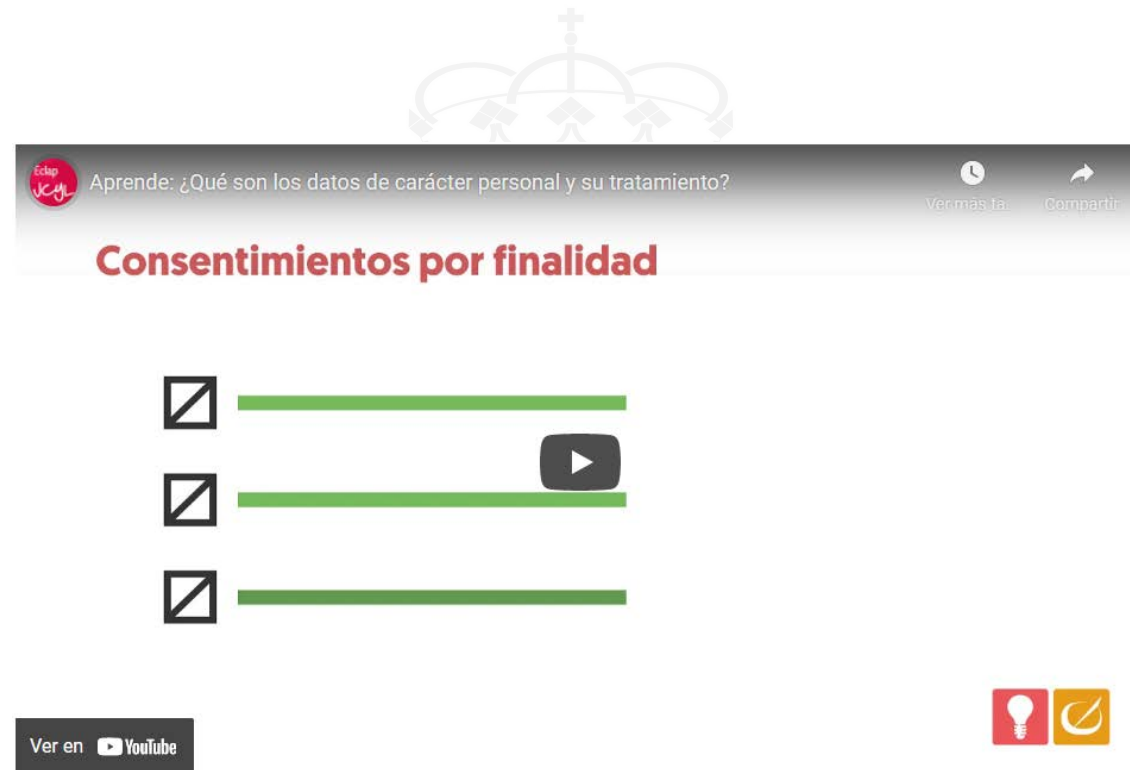
Fuente:
INCIBE

VIDEOS SOBRE DATOS DE CARÁCTER PERSONAL Y TRATAMIENTO DE LOS MISMOS



Diputación
de Salamanca

VIDEO DE ECLAPJCYL SOBRE DATOS DE CARÁCTER PERSONAL Y TRATAMIENTO DE LOS MISMOS



VIDEO DE LA ECLAPJCYL SOBRE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS





Diputación
de Salamanca

VIDEOS DE LA AEPD SOBRE DERECHOS DE PROTECCIÓN DE DATOS



Diputación
de Salamanca

VIDEOS SOBRE PROTECCIÓN DE DATOS PERSONALES POR LAS AAPP



VIDEO DE INCIBE DE CONCIENCIACION EN EL PUESTO DE TRABAJO

