Guía básica en protección de datos de carácter personal

Diputació de València | Protecció de Dades i Seguretat de la Informació

Diputació de València | Protecció de Dades i Seguretat de la Informació

Índice

Introducción

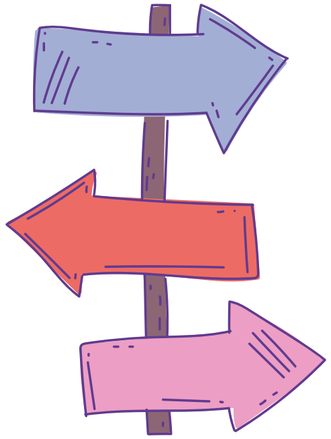
En esta **guía, con un carácter sucinto, claro y sencillo,** se abordan las **cuestiones elementales** que, el personal de la Diputación, debiera conocer en relación a la **aplicación de la legislación en protección de datos de carácter personal.**

Esta guía se divide en **3 grandes bloques**, que tratan la siguiente temática:

I. En el primer bloque, se indican las **principales normas reguladoras, el objeto y alcance** de las mismas. Así como, se señalan los **conceptos básicos** en protección de datos, en cuanto a qué se define como dato de carácter personal, tipología de datos personales y, además, se presentan las diferentes figuras involucradas en la protección de datos a nivel de la Diputación.

II. En el segundo bloque, se relacionan y se desgranan, sin exhaustividad, **las obligaciones relevantes que, la Diputación, debe cumplir.**

III. Por último, el tercer bloque señala aquellos **aspectos más relevantes que, el personal de la Diputación, debe tener en cuenta en el tratamiento, informático o en papel, de datos personales**.



Bloque I

Cuestiones generales

1. Normativa de protección de datos

1. Derecho fundamental. Protección de datos de personas físicas.

La protección de datos concernientes a personas físicas es un **derecho fundamental.**

El **tratamiento automatizado (informático) o no automatizado (papel) de datos de personas físicas (no jurídicas) debe ser protegido** por las entidades, públicas o privadas, responsables o encargadas de dicho tratamiento.

La legislación contempla un conjunto de principios y normas encaminadas a **garantizar los derechos de las personas sobre el control de su información personal** (= derechos de acceso, rectificación, supresión, limitación, oposición, portabilidad) y sobre la confidencialidad, integridad y disponibilidad de ésta, a conferir, mediante la adopción de **medidas de seguridad**, técnicas y organizativas, por parte de la entidad, responsable o encargada del tratamiento de los datos de carácter personal.

La Diputación al tratar datos de de personas físicas está sujeta a las obligaciones y responsabilidades de esta normativa.

2. Principales normas reguladoras.

Generales

- 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 o **RGPD**).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (**LOPDGDD**).

Específicas de la Diputación

- **Reglamento** por el cual se regula la política de seguridad y de la protección de datos de carácter personal en esta corporación [BOPV Nº127 5/7/2022].

- **Normativa** de Protección de Datos de Carácter Personal [Decreto nº 15874, de 27 de diciembre de 2022, del Presidente de la Diputación].

- **Procedimientos** de protección de datos de carácter personal [Decreto nº 15875, de 27 de diciembre de 2022, del Presidente de la Diputación].

2. ¿Qué se define como dato personal?

1. Definición.

Dato de carácter personal es **toda información concerniente a una persona física** (no jurídica), **identificada o identificable.**

Ejemplos

Nombre y apellidos; D.N.I./Pasaporte; Firma; Domicilio; Correo electrónico; Teléfono.; Edad; Sexo; Nacionalidad, Imagen/Voz; Datos bancarios; Titulación.

2. Tipología de datos.

- **Datos identificativos** [entre otros, Nombre y Apellidos; DNI/NIE/Pasaporte; N.º S.S.; Dirección; Teléfono; Imagen; Voz; Marca Física; Firma; Huella digital; Firma electrónica].
- **Datos de infracciones o sanciones administrativas y datos de naturaleza penal**.
- **Datos de características personales** [ente otros, Estado civil; Edad; Sexo; Fecha de nacimiento; Nacionalidad]
- **Datos de circunstancias sociales** [ente otros, Aficiones y estilo de vida; Pertinencia a clubes, asociaciones; Licencias, permisos, autorizaciones].
- **Datos académicos y profesionales** [entre otros, Titulaciones; Experiencia profesional; Pertenencia a colegios o asociaciones profesionales]
- **Datos detalle de empleo** [ente otros, Cuerpo/Escala; Categoría/grado; Historial trabajador]
- **Datos de información comercial** [entre otros, Actividades y negocios; Licencias comerciales;]
- **Datos económico-financieros y de seguros** [entre otros, Datos bancarios; Rentas; Inversiones, Bienes patrimoniales; Créditos; Pensiones; Nómina; Deducciones impositivas/impuestas; Seguros; Hipotecas; Subsidios]
- **Datos de transacciones** [Bienes y servicios suministrados por el afectado; Bienes y servicios recibidos por el afectado; Transacciones financieras; Compensaciones/indemnizaciones]

3. Datos de categoría especial.

Se trata de aquellos que pertenecen a la **esfera o halo más íntimo de la persona.** Se consideran más **sensibles** y, es por esto que, merecen especial protección.

- Datos relativos a la salud, física o psíquica.
- Opiniones políticas.
- Convicción religiosa o filosófica.
- Afiliación sindical.
- Origen étnico o racial.
- Datos genéticos.
- Datos biométricos dirigidos a identificar de manera unívoca a una persona física (ej. huella dactilar, reconocimiento facial).
- Vida u orientación sexual.

3. ¿Quién es quién en protección de datos?

1. Interesado o Interesada

Persona física, titular de los datos personales.

En el ámbito de la Diputación, se tratan datos de varios colectivos o grupos de personas físicas, titulares de datos personales (Ej. ciudadanos, cargos y empleados públicos, proveedores, candidatos o aspirantes en oferta pública de empleo).

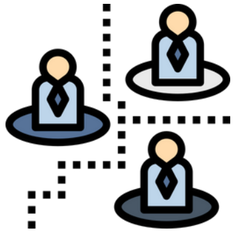
2. Responsable del Tratamiento (RT)

Persona física o jurídica, autoridad pública, servicio u organismo que **determina los fines y medios del tratamiento que se realiza.**

En nuestro ámbito, la condición de RT se atribuye a la persona jurídico-pública, Diputación provincial de Valencia. No se atribuye a cargo o empleado público, de forma individual y/o nominativa.

La Diputación es el sujeto obligado y es el que responde ante la autoridad de control, Agencia Española de Protección de Datos.

No obstante, los CGT asumen las obligaciones de cumplir con la normativa interna en proteccion de datos.



3. Centro Gestor del Tratamiento (CGT)

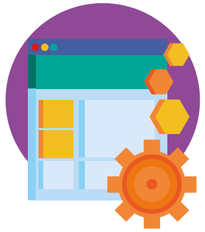
Unidad administrativa de la Diputación **responsable del fichero o tratamiento** de datos correspondiente.

Su determinación se basará en la **vinculación que dichas unidades tengan con la actividad de tratamiento:**

a) Presta el servicio o tiene la competencia para cuyo fin se tratan los datos.
b) Decide sobre la creación, finalidad y/o tipo de datos o el uso de estos.
c) Principal o mayor usuaria de los datos.

4. Usuario o Usuaria

Cargo, empleada o empleado público de la Diputación **que**, en el desempeño de las funciones y tareas, accede o **trata datos de carácter personal,** a nivel informático y/o en papel.



5. Encargado del Tratamiento (ET)

Persona física o jurídica, autoridad, servicio u organismo que **trata los datos por cuenta del Responsable del tratamiento (Diputación).**

En el ámbito de la Diputación, la condición de ET se atribuye a los terceros, adjudicatarios, contratistas o concesionarios, cuyo prestación de servicio comporte un acceso o tratamiento de datos de carácter personal, de los que es responsable del tratamiento la Diputación. (Ej. Empresa suministro software).

A su vez, la Diputación es ET respecto de los Ayuntamientos (Ej. Gestión y recaudación de tributos locales).

6. Delegado o Delegada de Protección de Datos (DPD)

Persona física o jurídica, pública o privada, de **obligado nombramiento** y designación en la Administración pública.

La figura del DPD puede ser designada a nivel **interno**, como es el caso de la Diputación. O, en su caso. designar a una persona, física o jurídica, **externa**.

El DPD es una figura que actúa con independencia y responde al más alto nivel jerárquico.

Las principales funciones del DPD son la de **supervisar y asesorar en el cumplimiento de la normativa.** A su vez, se ocupa de la interlocución con la autoridad de control, Agencia Española de Proteccion de Datos, así como con los titulares de datos.

Puedes contactar con nuestro DPD: **pdp@dival.es**.

Bloque II

Obligaciones relevantes de la Diputación, en calidad de responsable del tratamiento de datos de carácter personal

1. Registro de Actividades de Tratamiento

1. Es el **inventario de las actividades de tratamiento de datos de carácter personal**, que se efectúan, en calidad de responsable o encargado, por parte de los diferentes órganos o unidades administrativas de la Diputación, en el desempeño de las funciones o competencias atribuidas. En el R.A.T. constan, entre otros: (i) la finalidad o uso de los datos (ii) la base jurídica de licitud (iii) tipología de datos (iv) categoría de interesados (v) plazos de conservación (vi) cesionarios o destinatarios de los datos (vii) datos de contacto del Delegado de Proteccion de Datos.

2. La Diputación tiene un **Registro de Actividades del Tratamiento (R.A.T.)**:

- En calidad de **RESPONSABLE:** inventario de actividades de tratamiento de datos personales, de las cuales decide por sí, la Diputación, el uso, los fines y los medios del tratamiento.

- En calidad de **ENCARGADO:** actividades de tratamiento que efectúa por cuenta de otra entidad pública. Ej. gestión tributaria por cuenta de los Ayuntamientos.

3. La Diputación debe poner a disposición del público por medios electrónicos, el R.A.T., en calidad de responsable y de encargado del tratamiento. La Diputación tiene **publicado** los R.A.T. en:

www.dival.es/es/content/registro-actividades-de-tratamiento

Diputació de València | Protecció de Dades i Seguretat de la Informació

2. Deber de informar del tratamiento datos

1. ¿ En qué consiste?

La Diputación debe **informar** a los interesados [personas físicas titulares de datos] **acerca del tratamiento de los datos personales.**

El interesado tiene el **derecho a ser informado** de forma previa, concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

2. Canales o medios de recogida, donde deberemos informar al interesado:

3. ¿De qué debemos informar?

- Datos identificando Responsable de tratamiento (Diputación) y el contacto con el Delegado de Protección de Datos (**pdp@dival.es**).
- Fines y base jurídica del tratamiento.
- Plazo de conservación o, criterios utilizados para determinar este plazo.
- En su caso, destinatarios o categorías de destinatarios.
- En su caso, transferencias internacionales.
- Derechos de los interesados.
- Derecho a presentar reclamación ante la Agencia Española de Protección de Datos.

4. ¿Cómo informar?

En función del canal de recogida de datos, deberemos adoptar el modo de informar más adecuado. Aunque tengamos limitaciones, en todo caso, siempre deberá transmitirse una información, de carácter básico y luego completar toda la información en otro espacio. Así, se admite la información por capas:

1ª Capa: Información básica.

- Identidad del responsable del tratamiento (= Diputación de Valencia).
- Descripción sencilla de los fines del tratamiento.
- Referencia al ejercicio de derechos en protección de datos.

2ª Capa: Información completa.

Se incluye toda la información preceptiva indicada en el apartado anterior. A estos efectos, se trata, por ejemplo, de informar en el reverso de un impreso; locución telefónica; indicar una dirección web (Política Privacidad); un código QR; cartel zona videovigilada.

Puedes consultar el **Repositorio documental de protección de datos** de la Diputación aquí: **www.dival.es/intranet/node/42701**

3. Encargos de tratamiento de datos personales

1. ¿Quién es el Encargado del Tratamiento (ET)?

Persona física o jurídica, autoridad, servicio u organismo que **trata los datos por cuenta del Responsable del tratamiento (Diputación).**

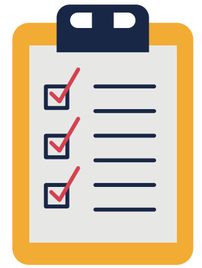
En el ámbito de la Diputación, la condición de ET se atribuye a los terceros, adjudicatarios, contratistas o concesionarios, cuyo prestación de servicio comporte un acceso o tratamiento de datos de carácter personal, de los que es responsable del tratamiento la Diputación. (Ej. Empresa suministro software).

A su vez, la Diputación es ET respecto de los Ayuntamientos (Ej. Gestión y recaudación de tributos locales).

2. ¿Cómo se articulan los encargos de tratamiento? En **actos jurídicos o contratos** (en su caso, acuerdos o convenios) entre la Diputación y el tercero, ET. En materia de contratación, a través de los **Pliegos** (PCPA y/o PPT).

3. ¿Qué se contempla en el encargo de tratamiento?

- Objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados.
- Las personas autorizadas para tratar los datos personales están sujetas al **deber de confidencialidad**.
- Tomará todas las **medidas de seguridad** necesarias para la protección de los datos. En concreto, serán conforme al Esquema Nacional de Seguridad (ENS).
- **Asistir** a la Diputación, en su caso, en la obligación de responder solicitudes de ejercicio de derecho en protección de datos.
- A elección de la Diputación, **suprimirá o devolverá todos los datos** personales una vez finalice la prestación de los servicios de tratamiento.
- Permitirá y contribuirá a la realización de **auditorías,** incluidas **inspecciones,** por parte de la Diputación o tercero contratado a estos efectos.
- Debe transmitirse **idénticas obligaciones y responsabilidades** a los terceros, en su caso, **subcontratados.**



4. ¿Qué más se contempla en un encargo de tratamiento? De acuerdo con la legislación de contratación del sector público, el licitador deberá aportar una **declaración responsable** en el que indique **dónde están ubicados los servidores** y los servicios asociados a éstos, utilizados, en su caso, para albergar los datos personales.

Téngase en cuenta que datos relativos a **censos electorales, de población, fiscales o tributarios, y de usuarios del servicio de salud** no pueden albergarse en países fuera del Espacio Económico Europeo o que no tengan decisión de adecuación de la Comisión Europea.

Puedes consultar el **Repositorio documental de protección de datos** de la Diputación aquí:

www.dival.es/intranet/node/42701

4. Adopción de medidas de seguridad

1. Esquema Nacional de Seguridad

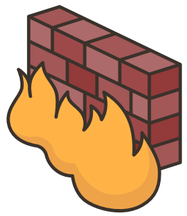
La protección de los datos de carácter personal, tratados por la Diputación, será conforme a las **medidas de seguridad** previstas por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (**ENS**).

2. Medidas de protección

Aparte de medidas de carácter organizativo y operacional, la Diputación **debe adoptar medidas técnicas de seguridad para la protección**:

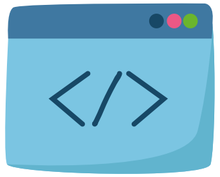
De las instalaciones e infraestructuras (Ej. Llevar una relación de personas autorizadas y un sistema de control de acceso que verifique la identidad y, en su caso, la autorización).

De los equipos (Ej. Bloqueo automático del equipo informático ante un tiempo de inactividad).



De las comunicaciones (Ej. Instalación de un cortafuegos que separe la red interna del exterior. Todo el tráfico de comunicaciones con el exterior estará sometido a los cortafuegos).

De la información (Ej. Realizar copias de respaldo que permitan recuperar datos perdidos accidentalmente o a causa de un ciberataque).



De las aplicaciones informáticas (Ej. Durante las pruebas de desarrollo o producción de la aplicación se tratará de no usar datos reales, sino datos ficticios).

De los soportes de información (Ej. Borrado o destrucción segura de los soportes extraíbles (electrónicos y no electrónicos) que vayan a ser reutilizados).

5. Análisis de Riesgos y Evaluaciones de Impacto en Protección de Datos

1. Análisis de Riesgos

Todas las actividades de tratamiento de datos personales **implican un riesgo** para las personas cuyos datos son tratados y, en particular, para sus **derechos y libertades.**

En función de los riesgos detectados, se deberán adoptar las **medidas de seguridad** oportunas para evitar o mitigar estos.

2. Evaluaciones de Impacto en Protección de Datos (EIPD)

La Diputación deberá realizar una EIPD cuando sea probable que un tipo de tratamiento de datos personales entrañe un **ALTO RIESGO para los derechos y libertades de las personas físicas.**

Ejemplos de supuestos en los que se debiera llevar a cabo una EIPD, previamente a efectuar el tratamiento de los datos de las personas:

- Utilización de reconocimiento facial para controlar el acceso a las instalaciones.

- Implantación de un Sistema interno de información para garantizar la protección de las personas que informen sobre infracciones normativas, en cumplimiento de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Diputació de València | Protecció de Dades i Seguretat de la Informació

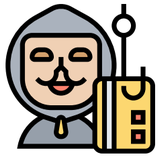
6. Incidente en la seguridad de datos personales

1. ¿Qué se considera incidente en protección de datos?

El **«incidente»,** en este contexto, es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos personales, a nivel informático o en papel.

Se considera **«violación de seguridad»** todas aquellas violaciones o 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. Afecta a la confidencialidad, integridad o disponibilidad de los datos personales.

Ejemplos



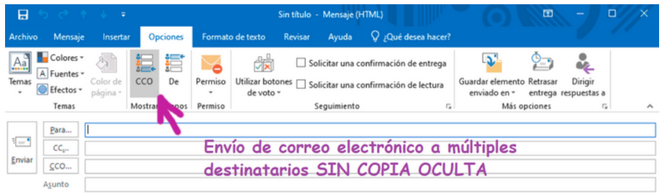
Ciberincidente por Suplantación de identidad (Phising)

Ciberincidente por infección de virus informático

Ciberincidente por dispositivo cifrado /secuestro de datos (Ej. Ransomware)

Bloqueo o acceso no autorizado a sistema informático

Deshacerse de documentos confidenciales o con datos personales sin previa destrucción



Incendio o inundación de archivo

2. ¿Qué debemos hacer cuando sufrimos o tenemos constancia de un incidente?

proactivanet

Comunicarlo de forma inmediata al **Servicio de Informática,** a través del sistema automatizado de notificación de incidencias: **www.incidencias.dival.es/** Este valorará si se considera un evento de seguridad a reportar.

Información a comunicar: fecha y hora de detección; persona que ha detectado; descripción breve del suceso; sistema, aplicación, archivo afectados.

En todo caso, sea un incidente o brecha de seguridad, que afecte a datos personales, se comunicará, inmediatamente, al Delegado de Protección de Datos **pdp@dival.es**

3. ¿Qué debe hacer la Diputación?

Independientemente de las notificaciones internas que se deban producir para gestionar un incidente de seguridad, en caso de brecha o violación, la **Diputación**, bajo el asesoramiento del **Delegado de Protección de Datos,** deberá:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

1. Notificar a la Agencia Española de Protección de Datos (AEPD), cuando:

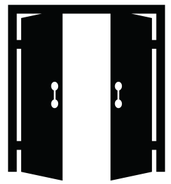
- Riesgo para los derechos y las libertades de las personas.
- 72 horas después de haber tenido constancia de la brecha o violación. Es por esto que debe comunicarse con máxima diligencia al Responsable y DPD.

2. Comunicar a los **Afectados**, cuando:

- Alto riesgo para sus derechos y libertades.
- Sin dilación indebida.

7. Derechos en protección de datos

Acceso



La persona titular de los datos puede solicitar a la Diputación **saber información acerca del tratamiento,** ente otros: qué categorías o tipos de datos se tratan; finalidad del tratamiento; destinatarios; de dónde se han obtenido los datos. Debe distinguirse de otros derechos de acceso (ej.): en calidad interesado en procedimiento administrativo; acceso información pública; acceso en calidad de Edil; a historia clínica.

Rectificación

La persona titular de los datos puede solicitar a la Diputación la **corrección de sus datos o se completen,** si son **inexactos o incompletos**.

Oposición

La persona titular de los datos puede solicitar a la Diputación la **oposición al tratamiento de sus datos** por motivos relacionados con su situación particular.

Supresión

La persona titular de los datos puede puede solicitar a la Diputación la **eliminación o borrado de sus datos** cuando: ya no son necesarios; retirada del consentimiento; tratamiento ilícito; por obligación legal.

Portabilidad

La persona titular de los datos puede solicitar **recibir sus datos** en un formato estructurado, de uso común y lectura mecánica, para transmitirlos a otra entidad.

Este derecho **NO es de aplicación** en los tratamientos de datos hechos por la **Administración pública.**

Limitación

La persona titular de los datos puede solicitar a la Diputación la **suspensión del tratamiento** de sus datos o limitar el uso de estos.

No ser objeto de decisiones automatizadas

No ser objeto de **decisiones automatizadas,** como la elaboración de perfiles, **que produzcan efectos jurídicos**.

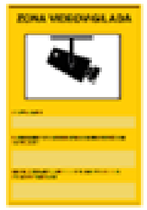
Cuestiones comunes a los derechos

- Pueden ejercerse también por representante legal o voluntario.
- La Diputación debe dar respuesta en el plazo de **1 mes.**
- Ante cualquier solicitud de este tipo póngase en conocimiento del Delegado de Protección de Datos **pdp@dival.es**

8. Videovigilancia

Obligaciones relativas al tratamiento de imágenes de personas físicas mediante **sistema de videovigilancia** de la Diputación.

La Diputación únicamente **utiliza** el sistema de videovigilancia **para preservar la seguridad de personas, bienes e instalaciones.**



1. Deber de información.- Se debe informar a los interesados mediante la colocación de distintivos informativos en lugares suficientemente visibles de las zonas videovigiladas. A su vez, se informará en documento adicional, en espacio on-line o código QR.

2. Supresión.- Las imágenes deben suprimirse en el plazo máximo de **un mes desde su captación**. Excepción: grabación delito o infracción administrativa.

3. Prohibiciones. - Captar imágenes en la vía pública (expto. Fuerzas y Cuerpos de Seguridad); terrenos y viviendas privadas colindantes o de cualquier otro espacio ajeno; baños, vestuarios o lugares análogos.

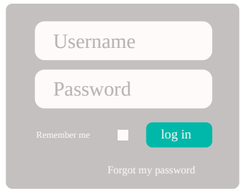
4. Contratación de un tercero.- La Diputación debe elegir una empresa de seguridad privada y/o instaladora de estos sistemas, que ofrezca las garantías suficientes. Se formalizará un contrato de encargo de tratamiento de datos.

5. Acceso a las imágenes.- A las imágenes grabadas accederán sólo las personas autorizadas. Se deben adoptar medidas de seguridad que impidan el acceso a las imágenes por parte de personal no autorizado.

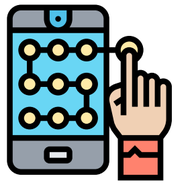
Bloque III

Buenas prácticas en el tratamiento de los datos por parte de las personas usuarias del sistema de información

1. Buenas prácticas en el tratamiento automatizado (informático) de datos personales

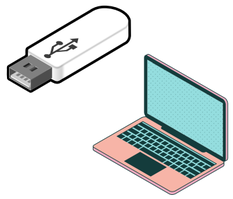


Protege tus **contraseñas** corporativas de acceso a los sistemas de información, como si se tratase del PIN de tu tarjeta de crédito o claves de acceso a tu teléfono móvil.



No utilices las **contraseñas de tú ámbito privado o doméstico** como claves de acceso al sistema de información de la Diputación.

Asegúrate de proteger tu equipo cuando abandonas tu entorno de trabajo, mediante el **bloqueo de acceso**. No alteres la configuración, física o lógica, de los equipos informáticos o de telefonía, ni instales software no autorizado.



Cifrar los dispositivos en los que obraran datos personales o información de carácter confidencial de la Diputación.

Almacena los archivos o ficheros informáticos en los **espacios habilitados en el servidor informático**, para poder ser protegidos frente a terceros y efectuar las copias de seguridad.

Utilizar el **correo electrónico** e Internet como **instrumentos de trabajo**, únicamente para la ejecución de las funciones o tareas asignadas.

No acceder a correo electrónico, abrir los archivos adjuntos o acceder a dirección de Internet, **sospechoso de ser dañino o perjudicial**.

Comunicar de manera inmediata al Servicio de Informática y Delegado de protección de datos **pdp@dival.es cualquier incidencia** que afecte a la seguridad de los datos.

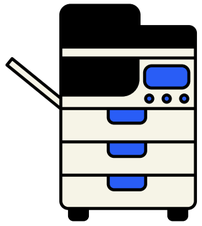
2. Buenas prácticas en el tratamiento no automatizado (papel) de datos personales

Guardar todos los soportes o documentos que contengan información de carácter personal **en un lugar seguro**, cuando éstos no sean usados, particularmente, fuera de la jornada laboral.

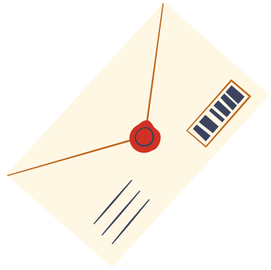
Mantener debidamente **custodiadas las llaves de acceso** a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contenga soportes o documentos en papel con datos de carácter personal.

Documentos no visibles en los escritorios, mostradores u otro mobiliario. Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.

No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información.



No dejar en fotocopiadoras, faxes o impresoras papeles con datos de carácter personal. Asegurarse de que **no quedan documentos impresos** que contengan datos personales, **en la bandeja de salida de la fotocopiadora**, impresora o faxes.



Si se envían a terceros ajenos a la organización alguna **información sensible**, que pueda contener categorías especiales de datos, se debe realizar, en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de **correo certificado** o a través de una forma de correo ordinario **que permita su completa confidencialidad**.

Comunicar de manera inmediata al Delegado de protección de datos **pdp@dival.es cualquier incidencia** que afecte a la seguridad de los datos.

Diputació de València

Protecció de Dades i Seguretat de la Informació