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

CLASIFICACIÓN: **NIVEL "B"**

(Artículo 43.2 Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia)

PROCEDIMIENTOS DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

CÓDIGO	P/PDP	**APROBACIÓN**	Decreto nº 15875, de 27 de diciembre de 2022, del Presidente de la Diputación

CONTROL DOCUMENTAL

ELABORADO POR:	REVISADO POR:	APROBADO POR:
	Eusebio Moya López	Antoni Francesc Gaspar
Departamento de Protección de Datos y Seguridad de la Información	Jefe Departamento de Protección de Datos y Seguridad de la Información	Presidente Diputación de Valencia

HISTÓRICO DEL DOCUMENTO:

Fecha	Edición	Revisión	Cambios Realizados
27/12/2022	01	01	Aprobación inicial de la norma

FICHEROS: NORMATIVA PDP

LOCALIZACIÓN :

FECHA DE EMISIÓN: Diciembre 2022

INDICE

INTRODUCCIÓN

El artículo 43.2 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, establece que deberán elaborarse un conjunto de procedimientos técnicos de carácter obligatorio orientados a resolver las tareas, procesos de trabajo o modos de actuación considerados más relevantes atendiendo al perjuicio que causaría una actuación inadecuada de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información, o de protección de datos de carácter personal, o por venir impuestos por la legislación aplicable.

Dicho precepto recoge expresamente como integrados en su mandato los denominados *Procedimientos de Protección de Datos de Carácter Personal*, otorgando el artículo 39.1 la competencia para su aprobación al Presidente de la Diputación o Diputado/a en quien éste delegue.

Por Decreto nº 15875, de 27 de diciembre de 2022, el Presidente de la Diputación ha aprobado los presentes *Procedimientos de Protección de Datos de Carácter Personal.*

En el presente documento constan los procedimientos de trabajo relacionados con la protección de datos de carácter personal de la Diputación de Valencia. En consonancia con el artículo 4 del citado Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal, la presente normativa es de aplicación a todos los departamentos y unidades de la Diputación de Valencia, y resultará de obligado cumplimiento en el tratamiento de los datos personales llevados a cabo.

1. PROCEDIMIENTOS DE TRABAJO DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

P/PDP-001 PROCEDIMIENTO PARA LA CREACIÓN Y MODIFICACIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

OBJETIVOS Y ALCANCE

Garantizar una adecuada coordinación y comunicación entre las diferentes partes implicadas en la inscripción, modificación y supresión en el Registro de las Actividades de Tratamiento (en adelante, RAT) de la Diputación de Valencia, con el fin de garantizar que se da cumplimiento a las obligaciones establecidas en la normativa en materia de protección de datos.

Están afectados:

- todos aquellos tratamientos de datos de carácter personal de nueva creación en la Diputación de Valencia.
- aquellos tratamientos de datos ya inscritos en el RAT y que sufran modificaciones en la finalidad, en las categorías de datos que se tratan o en cualquier otra información que deba hacerse constar en el RAT.
- todos aquellos tratamientos de datos que dejen de efectuarse y que, en consecuencia, deben ser suprimidos del RAT.

Entidades de la Diputación de Valencia afectadas:

- **El Delegado de Protección de Datos**, encargado de supervisar las altas, modificaciones y supresiones de tratamientos en el RAT.

- **Cualquier área o servicio de la Corporación obligada a inscribir, modificar o suprimir una actividad de tratamiento de datos de carácter personal**. Estas Unidades, como centros gestores del tratamiento (CGT), serán responsables de mantener actualizada la información sobre actividades de tratamiento existentes o la intención de crear nuevas actividades que resulten de su competencia.

DESARROLLO

El CGT responsable en que se detecte la necesidad de crear, modificar o eliminar una actividad de tratamiento lo realizará a través del aplicativo interno de gestión del RAT.

El Delegado de Protección de Datos asesorará al CGT en cualquier cuestión que desee consultársele durante la creación, modificación o eliminación de una actividad de tratamiento en RAT.

El Delegado de Protección de Datos supervisará las acciones de alta, modificación o supresión llevadas a cabo en el RAT, pudiendo intervenir para recabar del CGT información adicional o interesar cualquier tipo de aclaración. De igual forma, el Delegado de Protección de Datos podrá comunicar al CGT la no conformidad de la actuación pretendida o practicada sobre el RAT.

La creación de una nueva actividad de tratamiento se realizará con un mínimo de **un mes de antelación** sobre la fecha en que esté previsto el comienzo del tratamiento. Esto permitirá disponer de ese margen de tiempo para adoptar las medidas necesarias para su regularización.

P/PDP-002 PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS ARSOPL

OBJETIVOS Y ALCANCE

Garantizar el ejercicio de los derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento por parte de los titulares de los datos de carácter personal. Este procedimiento será común para todos los departamentos y unidades de la Corporación y para cualquier tratamiento/fichero con datos de carácter personal, salvo en aquellos supuestos en que las leyes aplicables a determinados tratamientos/ficheros establezcan un procedimiento especial para la rectificación o supresión de los datos contenidos en los mismos, en cuyo caso se estará a lo dispuesto en aquéllas.

Están afectados:

- todos aquellos tratamientos de datos de carácter personal cuyo Responsable del Tratamiento sea la Diputación de Valencia.
- aquellos tratamientos de datos de carácter personal de los que la Diputación de Valencia sea Encargado del Tratamiento, y respecto de los cuales se haya pactado de forma expresa entre el Responsable del Tratamiento y la Diputación que ésta atenderá, por cuenta y orden del primero, los derechos ARSOPL.

Entidades de la Diputación de Valencia afectadas:

- **El CGT responsable del fichero/tratamiento de datos correspondiente**. Estas unidades serán responsables de atender los

derechos ARSOPL que ejerciten los titulares de los datos personales que tratan.

DESARROLLO

1º. Legitimación

El ejercicio de los derechos ARSOPL tiene carácter personalísimo, por lo que únicamente podrá solicitarse y llevarse a cabo por:

a) El afectado o interesado (el titular de los datos personales)
b) El representante legal o voluntario del afectado o interesado:

- **legal**. Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que imposibilite el ejercicio personal de los derechos.
- **voluntario**. Mediante expresa designación para el ejercicio del derecho.

En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, supresión, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la LOPDGDD.

En el caso de que el afectado haya fallecido, las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquél y, en su caso, su rectificación o supresión.

Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

En caso de fallecimiento de menores, estos derechos podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estos derechos también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2º. Solicitud

La solicitud de ejercicio de derechos ARSOPL podrá efectuarse a través de uno de los siguientes medios:

a) **Tramitación electrónica**. En la sede electrónica de la Diputación (www.sede.dival.es) se encuentra en el catálogo de trámites el denominado “Derechos Protección de datos”, dentro de la sección de “Atención al ciudadano”.

b) **Tramitación en soporte papel**. Utilizando la solicitud tipo habilitada para ello, la instancia general o cualquier otro escrito que presente el interesado.

c) **Tramitación por otros medios electrónicos o telemáticos**. Mediante correo electrónico, mecanismos facilitados en portales web o entornos similares en Internet.

La tramitación a través de alguno de los medios de los apartados a) o c) deberá reunir las condiciones y garantías establecidas en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, y resto de normativa sobre administración electrónica que sea de aplicación. Estos medios dispondrán de sistemas que permitan el establecimiento de medidas de seguridad de acuerdo con lo establecido en Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3º. Requisitos

Deberá **acreditarse la legitimidad** para el ejercicio de los derechos ARSOPL de acuerdo con las siguientes especificaciones:

• las solicitudes tramitadas conforme al apartado a) del punto 2º. La acreditación se ajustará a lo dispuesto en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, así como a las normas que para dichos procedimientos se establecen en la sede electrónica. La acreditación en la actuación por medio de representante se realizará de acuerdo con lo dispuesto en el artículo 32 del citado Real Decreto 203/2021.

• las solicitudes tramitadas conforme al apartado b) del punto 2º. La acreditación se llevará a cabo:

- mediante la aportación de fotocopia del DNI, pasaporte u otro documento válido que lo identifique, cuando se solicite por el propio interesado.
- cuando se actúe mediante representante, además de lo anterior, mediante la aportación de los mismos documentos anteriores pertenecientes al representante legal o voluntario, y de los documentos que acrediten la representación.

• las solicitudes tramitadas conforme al apartado c) del punto 2º. La acreditación se llevará a cabo mediante la validación del interesado (login) en el portal web, entorno de Internet, etc, con las credenciales que se hayan establecido para el acceso personalizado o las asociadas a la cuenta de correo electrónico utilizada. La acreditación se ajustará a lo dispuesto en el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. La acreditación en la actuación por medio de representante se realizará de acuerdo con lo dispuesto en el artículo 32 del citado Real Decreto 203/2021.

La solicitud **deberá contener**, como mínimo:

a. Nombre y apellidos del interesado y, en su caso, de la persona que lo represente.
b. Petición en que se concreta la solicitud (acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento).
c. Dirección a efectos de notificaciones, fecha y firma del solicitante.
d. Documentos acreditativos de la petición que se formula, en su caso.
e. Cuando se actúe mediante representante, la aportación de los documentos que acrediten la representación.

Además de lo anterior, si se trata del **derecho de acceso**, se indicará:

- El tipo de datos respecto a los que se solicita el acceso (concretos, totales, de un fichero específico...)
- El sistema de consulta por el que se opta (copia, en pantalla, formato telemático, etc.)

Si se pretende el **derecho de rectificación o supresión**:

- Los datos afectados, corrección o supresión que se pretende y, en su caso, documentación justificativa.

En el caso del ejercicio del **derecho de oposición**:

- En el supuesto de no ser necesario el consentimiento, indicación de los motivos fundados y legítimos que justifiquen la oposición.

En los supuestos tramitados conforme al apartado c) del punto 2º, podrán obviarse los requisitos citados para la solicitud cuando se ponga a disposición del interesado, tras su validación, el acceso al conjunto de sus datos y la posibilidad de ejercitar *in situ* la modificación o cancelación de los mismos.

En el caso del ejercicio del **derecho a la portabilidad**:

- En el supuesto de solicitar que los datos se transmitan directamente a otro responsable, indicación de los datos de contacto del responsable destinatario de los datos.

En el caso del ejercicio del **derecho a la limitación del tratamiento:**

• Los datos respecto a los que se solicita la limitación y, de ser posible, información sobre la condición necesaria para obtener la limitación del tratamiento (impugnación de la exactitud de los datos personales; ilicitud del tratamiento y oposición a la supresión; ausencia de necesidad para los fines del tratamiento, pero necesidad para la formulación, ejercicio o defensa de reclamaciones; limitación del tratamiento mientras se verifica la oposición solicitada).

4º. Procedimiento

Una vez recibida la solicitud, se comprobará que reúne todos los requisitos citados en los puntos anteriores. Si se careciera de alguno de ellos, se requerirá al solicitante para que subsane la solicitud conforme a lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (**LPACAP)** o, en su caso, Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. La no subsanación en el plazo legal comportará el archivo de la solicitud.

Si la solicitud cumple todos los requisitos:

➢ ***solicitud de acceso.*** Deberá resolverse la solicitud.

La resolución expresa podrá:

- Comunicar la inexistencia de datos personales del afectado.

- Denegar el acceso al afectado, en virtud de las causas previstas legalmente, justificando tal denegación.
- Otorgar el acceso, acompañando la información preceptiva.

➢ ***solicitudes de rectificación y supresión.*** Deberá resolverse la solicitud.

La resolución expresa podrá:

- Comunicar la inexistencia de datos personales del afectado.
- Denegar la rectificación o supresión al afectado, en virtud de las causas previstas legalmente, justificando tal denegación.
- Otorgar la rectificación o supresión.

➢ ***solicitud de oposición.*** Deberá resolverse la solicitud.

La resolución expresa podrá:

- Comunicar la inexistencia de datos personales del afectado.
- Denegar la exclusión del tratamiento, en virtud de las causas previstas legalmente, justificando tal denegación.
- Acceder a la petición, excluyendo del tratamiento los datos personales del solicitante.

➢ ***solicitud de portabilidad.*** Deberá resolverse la solicitud.

La resolución expresa podrá:

- Comunicar la inexistencia de datos personales del afectado.

- Denegar la portabilidad de los datos personales, en virtud de las causas previstas legalmente, justificando tal denegación.
- Acceder a la petición, remitiendo al solicitante los datos personales que le incumban, que hubiera facilitado a la Diputación de Valencia, en un formato estructurado, de uso común y lectura mecánica; o en su caso, transmitiéndolos a otro responsable del tratamiento, cuando el interesado así lo desee y sea técnicamente posible.

➢ ***solicitud de limitación del tratamiento.*** Deberá resolverse la solicitud.

La resolución expresa podrá:

- Comunicar la inexistencia de datos personales del afectado.
- Denegar la limitación del tratamiento de los datos personales, en virtud de las causas previstas legalmente, justificando tal denegación.
- Acceder a la petición, en cuyo caso, los datos objeto de limitación únicamente podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

5º . Plazos de respuesta

El plazo máximo de resolución de las solicitudes es de **un mes desde la recepción de aquéllas**.

El plazo de un mes podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. La Diputación de Valencia informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

Si la Diputación de Valencia no da curso a la solicitud del interesado, le informará de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar las acciones administrativas y judiciales que estime oportunas.

6º. Satisfacción de los derechos

Las solicitudes que resulten estimadas conllevarán la satisfacción de los derechos interesados en los plazos señalados en el punto 5º. Para ello, se actuará del modo siguiente:

- ***derecho de acceso.*** El derecho se satisface poniendo en conocimiento del interesado si sus datos de carácter personal están siendo objeto de tratamiento y, en tal caso, concediendo el acceso a sus datos personales y, en su caso, a la siguiente información: la finalidad del tratamiento que, en su caso, se esté realizando, las categorías de datos personales de que se trate, los destinatarios o categorías de destinatarios a los que se comunicaron o serán comunicados los datos,

el plazo previsto de conservación o los criterios para determinarlo, la existencia del derecho a solicitar la rectificación, supresión, oposición o limitación del tratamiento de sus datos, el derecho a presentar una reclamación ante una autoridad de control, la información sobre el origen de los datos cuando no se hayan obtenido del propio interesado, la existencia de decisiones automatizadas, las garantías en caso de que se transfieran datos a un tercer país u organización internacional.

La Diputación de Valencia facilitará una copia de los datos personales objeto de tratamiento. El derecho a obtener copia no debe afectar negativamente a los derechos y libertades de otros.

La información que se proporcione al interesado debe darse en forma legible e inteligible.

El derecho de acceso se entenderá otorgado si la Diputación de Valencia facilita al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por la Diputación de Valencia del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho. No obstante, el interesado podrá solicitar de la Diputación de Valencia la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto (finalidad del tratamiento, categorías de datos, destinatarios, etc.).

Cuando el interesado haya presentado la solicitud por medios electrónicos, la información se facilitará por medios electrónicos, cuando

sea posible, a menos que el interesado solicite que se facilite de otro modo. **Se puede considerar repetitivo el ejercicio del derecho de acceso cuando el interesado lo solicite en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello. En caso de repetición, la Diputación de Valencia podrá cobrar un canon razonable en función de los costes administrativos afrontados o negarse a actuar respecto de la solicitud. La Diputación de Valencia soportará la carga de demostrar el carácter repetitivo de dicha solicitud.**

➢ ***derechos de rectificación y supresión.*** El derecho de rectificación se satisface practicando la modificación de los datos que resulten ser inexactos o incompletos. El derecho de supresión se satisface suprimiendo los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo[3].

➢ ***derecho de oposición.*** El derecho de oposición se satisface excluyendo del tratamiento los datos de carácter personal afectados.

➢ ***derecho a la portabilidad.*** El derecho de portabilidad se satisface facilitando al interesado los datos personales que le incumban en un formato estructurado, de uso común y lectura mecánica o, en su caso, transmitiendo los datos a otro responsable del tratamiento seleccionado por el interesado, cuando sea técnicamente posible.

[3] ***el bloqueo de los datos*** *consiste en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión de los datos.*

➢ ***derecho a la limitación del tratamiento.*** El derecho a la limitación del tratamiento se satisface limitando el tratamiento de los datos personales afectados, con excepción de su conservación, a aquel que hubiera consentido el interesado o al necesario para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. Todo interesado que haya obtenido la limitación del tratamiento debe ser informado por la Diputación de Valencia antes del levantamiento de dicha limitación.

Se comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. La Diputación de Valencia informará al interesado acerca de dichos destinatarios, si este así lo solicita.

7º. Reclamaciones y recursos

El procedimiento para el ejercicio de los derechos ARSOPL es un procedimiento especial. Las normas del procedimiento administrativo común contenidas en la **LPACAP** son de aplicación subsidiaria. Ello supone:

• Las resoluciones (expresas o presuntas) sobre solicitudes de derechos ARSOPL agotan la vía administrativa ante la Diputación, y el interesado puede interponer la reclamación ante la autoridad de control competente en materia de protección de datos**,** sin perjuicio de que interponga cualquier otro recurso que estime procedente.

• A los actos de trámite o las resoluciones que desestimen una solicitud sin entrar en el fondo de la petición (falta de subsanación en plazo, carencia de legitimación, etc) les será de aplicación el régimen general sobre recursos de la **LPACAP**.

8º. Constancia

Deberá dejarse constancia de todas las actuaciones llevadas a cabo en relación con el ejercicio de los derechos ARSOPL, con independencia de las características del fichero o tratamiento de los datos (automatizado, en papel, mixto), de los cauces utilizados para el ejercicio y de los resultados.

9º. Especialidades en el tratamiento de datos personales mediante dispositivos de captación de imágenes y sonidos

Por su propia naturaleza, en el tratamiento de datos personales a través de dispositivos de captación de imágenes y sonidos **únicamente cabe ejercitar los derechos de acceso, supresión y limitación**.

Cuando se soliciten dichos derechos se procederá de acuerdo a las siguientes especialidades:

- ***derecho de acceso.*** A la documentación que acompañe la solicitud de acceso deberá adjuntarse una imagen reciente del interesado, en la que se identifique perfectamente a éste.
  La facilitación del derecho de acceso no supondrá proporcionar al interesado el visionado de las grabaciones, pues ello podría comportar la vulneración de los derechos de terceros. El personal que resulte autorizado por la normativa interna de protección de datos será quien

visualice las correspondientes imágenes captadas y, en su caso, realizará un informe describiendo con detalle aquellas imágenes en las que pueda identificarse al afectado, trasladándose dicho informe al interesado. Únicamente en aquellos casos en que el estado de la tecnología lo permita, sin implicar grandes esfuerzos y recursos, y las circunstancias de las imágenes captadas no afecten a derechos de terceros, podrá facilitarse puntualmente el acceso visual a las grabaciones.

➢ ***derecho a la limitación del tratamiento.*** El derecho a la limitación será ejercitable en el único sentido de conservar los archivos más allá del plazo de conservación, cuando el tratamiento de datos sea ilícito y el interesado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso, o cuando la Diputación ya no necesite los datos para los fines del tratamiento pero el interesado sí los necesite para la formulación, ejercicio o defensa de reclamaciones.

➢ ***derecho de supresión.*** No procederá acceder a la solicitud de supresión de imágenes y/o sonidos que se encuentren en situación de bloqueo por las razones indicadas en la normativa interna de protección de datos.

P/PDP-003 PROCEDIMIENTO PARA GARANTIZAR LA EXACTITUD Y ACTUALIDAD DE LOS DATOS PERSONALES

OBJETIVOS Y ALCANCE

Garantizar que los datos de carácter personal sean exactos y puestos al día, de forma que respondan de modo veraz a la situación actual de sus titulares y a la vigencia de su tratamiento. Se pretende establecer mecanismos que permitan a la Diputación cumplir con el deber de mantener "de oficio" la exactitud, actualidad y pertinencia de tratamiento respecto de los datos de carácter personal de los que resulte "Responsable del Tratamiento", así como de aquellos otros que en calidad de "Encargado del Tratamiento" comporte la obligación de mantener la exactitud, actualidad y vigencia de sus datos.

Están afectados:

- todos aquellos tratamientos de datos de carácter personal cuyo "Responsable del Tratamiento" sea la Diputación de Valencia.
- aquellos tratamientos de datos de carácter personal de los que la Diputación de Valencia sea "Encargado del Tratamiento", y cuya prestación comporte la obligación de mantener la exactitud, actualidad y vigencia de sus datos.

Entidades de la Diputación de Valencia afectadas:

- **Cualquier área o servicio de la Corporación que lleve a cabo el tratamiento con datos de carácter personal**. Estas unidades serán responsables de asegurar la exactitud, actualidad y vigencia de los datos personales.

DESARROLLO

La diversidad en el origen, modos de obtención, tipología, transformación, comunicación y fines de los datos de carácter personal, entre otros,

condicionan las actuaciones para alcanzar el objetivo de asegurar la exactitud, actualidad y vigencia de los datos. Por ello, las directrices siguientes deberán adecuarse por cada área afectada a la realidad del fichero o tratamiento del que resulte responsable.

• Siempre que resulte factible -atendiendo al esfuerzo, recursos implicados y la posibilidad legal- deberá procederse de forma periódica y sistemática a trasladar a los afectados la información que de ellos se dispone con el propósito de que puedan manifestar la exactitud de la misma y practicar, en su caso, las modificaciones pertinentes. Cuando los datos provengan de terceros, por venir obligados a facilitarlos, se les incluirá como destinatarios. Se procurará que estos procesos se realicen, como mínimo, una vez al año.

• Cuando el origen de los datos sean fuentes de acceso público, se establecerán rutinas que constaten periódicamente la vigencia y, en su caso, exactitud de dichas fuentes. En este punto, ha de tenerse en cuenta que ha desaparecido, en la actual normativa de protección de datos, la referencia a las “fuentes accesibles al público” como causa de legitimación del tratamiento sin necesidad de consentimiento. En la actualidad, incluso en estos casos, deberá concurrir alguna de las causas legitimadoras establecidas en la normativa de protección de datos.

• Cuando los datos provengan de otras administraciones públicas se intentará, dentro del marco legal, formalizar acuerdos que faciliten la actualización y vigencia de la información, canalizándose preferentemente mediante soluciones tecnológicas de interoperabilidad.

• Deberán ser revisados periódicamente los datos de carácter personal que cada unidad publique o difunda en Internet, en los sitios web y otros canales

electrónicos o telemáticos, con independencia de que la titularidad de estos entornos corresponda o no a la Diputación de Valencia. Se prestará especial atención a la vigencia de estos datos en dichos entornos, eliminando aquellos que hayan cumplido el objeto de su publicidad; para ello, el **responsable de la información** determinará el marco temporal de vigencia previamente a la publicación o difusión de los datos.

• Cuando se comuniquen datos personales a terceros en virtud de una relación de prestación de servicios (encargado del tratamiento), se asegurarán los mecanismos para que dichos datos sean objeto de las acciones de actualización y vigencia. En cualquier caso, se evitará que en supuestos de redundancia unos mismos datos ofrezcan diferente información.

P/PDP-004 PROCEDIMIENTO PARA GARANTIZAR LA NORMALIZACIÓN INFORMATIVA EN SEDE ELECTRÓNICA, SITIOS WEB O ESPACIOS EN INTERNET

OBJETIVOS Y ALCANCE

Asegurar el cumplimiento del artículo 17 del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, que establece la obligación de que, tanto la Sede Electrónica de la Diputación de Valencia como cualquier espacio en Internet o tecnologías similares de cuyos contenidos sea responsable la Corporación, contenga una referencia al Registro de Actividades de Tratamiento, las políticas y normativas internas sobre protección de datos de carácter personal y, en particular, de los derechos que asisten a los titulares de los datos.

Están afectados:

- la Sede Electrónica de la Diputación de Valencia y cualquier espacio en Internet o tecnologías similares de cuyos contenidos sea responsable la Corporación.

Entidades de la Diputación de Valencia afectadas:

- **El Servicio de Informática de la Corporación**. Este servicio será responsable de asegurar el cumplimiento respecto de la Sede Electrónica, el portal web corporativo y cualquier espacio en Internet o tecnologías similares cuya administración directa lleve.

- **Cualquier área o servicio de la Corporación que administre directamente cualquier espacio en Internet o tecnologías similares**. Estas unidades serán responsables de asegurar el cumplimiento respecto de dichos espacios.

DESARROLLO

• En el supuesto de la Sede Electrónica, el portal web corporativo y cualquier espacio en Internet o tecnologías similares cuya administración directa lleve el **Servicio de Informática**, el citado Servicio implementará y mantendrá actualizada las pertinentes referencias de las políticas y normativas internas sobre protección de datos de carácter personal y, en particular, de los derechos que asisten a los titulares de los datos, utilizando para ello las plantillas y referencias documentales puestas a disposición por el Departamento de Protección de Datos y Seguridad de la Información.

• En el resto de supuestos, será el **responsable del área o servicio** que administre directamente estos espacios el que implementará y mantendrá actualizada las pertinentes referencias de las políticas y normativas internas sobre protección de datos de carácter personal y, en particular, de los derechos que asisten a los titulares de los datos, utilizando para ello las plantillas y referencias documentales puestas a disposición por el Departamento de Protección de Datos y Seguridad de la Información.

Está prohibido poner en servicio cualquiera de los espacios tecnológicos referidos sin que contenga los requisitos mencionados.

P/PDP-005 PROCEDIMIENTO PARA LA GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

OBJETIVOS Y ALCANCE

Se describe el procedimiento operativo a seguir para la gestión y notificación, en su caso, a la AEPD y a los afectados, de las brechas de seguridad que afecten a datos personales, es decir, cuando implique destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales, y que permita a la organización responder de forma rápida, ordenada y eficaz al evento, minimizando las consecuencias del mismo sobre la propia organización y terceras partes implicadas. Afecta a todos aquellos eventos que acontezcan en la Diputación de Valencia o por cuenta de un encargado del tratamiento, en los que pudieran verse afectadas la confidencialidad, integridad o disponibilidad de datos personales.

Quedan afectados por este procedimiento:

- Todos aquellos datos personales cuya confidencialidad, integridad o disponibilidad pudieran verse afectados por el evento de seguridad.

Entidades de la Diputación de Valencia que podrían verse afectadas:

- El **área o servicio de la Corporación que detecte el incidente o que se vea afectado** por el mismo.
- El **Servicio de Informática** de la Corporación.
- El **Departamento de Protección de Datos y Seguridad de la Información.**
- El **Delegado de Protección de Datos.**
- **En su caso, responsables, encargados, titulares de los datos y otras figuras** que se determinen.

DESARROLLO

El procedimiento de actuación incluye las siguientes fases:

1º. Detección, comunicación, identificación y clasificación

1.A Detección y comunicación

La detección de eventos de seguridad de datos personales puede producirse a través de fuentes externas o internas:

• **Fuentes externas:** Proveedores de servicios informáticos, proveedores de servicios de telecomunicaciones, proveedores de servicios de seguridad, entidades públicas: Instituto Nacional de Ciberseguridad (INCIBE), Centro Criptológico Nacional (CCN), CSIRT-CV (Centro de Alerta y respuesta de incidentes de seguridad de la CV), Fuerzas y cuerpos de seguridad del estado, etc.

• **Fuentes internas:** Los usuarios de los sistemas de información de la Diputación o los propios sistemas internos de monitorización: antivirus, analizadores de logs, monitorización de servidores o tráficos de red, etc.

Con independencia de la persona que detecte el evento, será comunicado inmediatamente al Responsable designado al efecto, el cual valorará si se considera un evento de seguridad que se tenga que reportar como tal.

Los datos mínimos del evento a cumplimentar por escrito serán:
• Fecha y hora de la detección.
• Persona que lo ha detectado.
• Naturaleza del evento de seguridad de los datos personales.
• Descripción breve.
• Sistema afectado.

La comunicación de los hechos se realizará preferentemente a través del sistema automatizado de notificación de incidencias existente en cada momento en la Corporación, habilitándose un ítem específico.

1.B Identificación y registro

El análisis de las fuentes de información antes mencionadas permitirá determinar si se está ante un incidente de seguridad o no, así como su naturaleza, clase, tipo, si dicho incidente ha afectado a datos de carácter personal y por tanto constituye una "brecha de seguridad de los datos de carácter personal" descrita en la normativa de protección de datos, y el nivel de riesgo al que se enfrenta la organización.

Se deberá mantener un registro documental de los incidentes de seguridad, incluyendo el tipo de incidente, descripción del mismo, gravedad, estado y medidas adoptadas para su resolución.

1.C Análisis y clasificación

Una vez registrado el incidente de seguridad y recopilada la información disponible en primera instancia, el responsable designado al efecto realizará una primera clasificación: incidente de seguridad o brecha de seguridad.

- **Incidente de seguridad:** cualquier evento que afecte o impacte en las dimensiones de la seguridad (Confidencialidad, Integridad, Disponibilidad, Trazabilidad o Autenticidad) debe ser considerado al menos como un incidente de seguridad de datos personales siempre que afecte a un sistema de información que contenga dichos datos personales, aunque el impacto sea muy reducido y los inconvenientes puedan ser subsanados rápidamente.

- **Brecha de seguridad:** consideraremos que un incidente de seguridad es una *Brecha de seguridad* cuando ocasione la destrucción, pérdida o

alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

En caso de que se trate de una brecha de seguridad, es imprescindible evaluar el nivel de perjuicio que puede causar a los derechos y libertades de los afectados, determinando con el mayor grado de precisión posible el nivel de severidad de las consecuencias para los individuos. Es asimismo imprescindible determinar si se trata de una brecha de confidencialidad, integridad o disponibilidad, categoría y número de afectados, categoría y número de registros de datos, etc.

En ambos casos (incidente o brecha), se comunicará inmediatamente al Delegado de protección de Datos, el cual hará un seguimiento a los efectos de cumplimentar, en su caso, el deber de notificación en plazo a la autoridad de control y, si fuera necesario, a los titulares de los datos personales afectados.

2º. Respuesta al incidente

2.A Contención

Durante el proceso de respuesta, en una primera fase se intentará contener el incidente. Una parte esencial de la contención es la toma de decisiones rápidas como puede ser cerrar un sistema, aislarlo de la red, deshabilitar ciertas funciones, etc.

2.B Solución

Tras la aplicación de las medidas de contención, se tomarán las medidas correctoras o de erradicación necesarias y se verificará el correcto funcionamiento de éstas, confirmando su idoneidad para la eliminación del incidente.

Se debe considerar también si las medidas aplicadas son de carácter temporal o si forman parte de una solución definitiva, y el sistema y/o la información afectada ha vuelto de nuevo de modo efectivo a su estado original.

2.C Recuperación

Solucionado el incidente o la brecha de seguridad y verificada la eficacia de las medidas adoptadas, se entrará en la fase de recuperación, que tiene como objetivo el restablecimiento del servicio en su totalidad, confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa.

2.D Evidencias

Se deberán recabar todas las evidencias disponibles con la información generada por los sistemas involucrados en el incidente o brecha de seguridad.

2.E Comunicación

La comunicación es fundamental durante todo el ciclo de vida del proceso de respuesta, y debe hacerse de una manera continua de modo que se tenga visibilidad clara tanto del incidente como de las acciones tomadas para

afrontarlo. Es especialmente importante cuando el incidente trasciende el perímetro de la Diputación y toma relevancia pública.

Los responsables de gestionar el incidente o brecha de seguridad mantendrán permanentemente informado de todas las actuaciones al Delegado de Protección de Datos.

2.F Informe de resolución

La elaboración del informe de resolución tiene como objetivo servir como base de conocimiento. Este se debe presentar en forma de línea temporal, de modo que facilite el seguimiento de las diferentes acciones, y debería incluir al menos información relativa a los siguientes apartados:

- Alcance e impacto del incidente.
- Controles preventivos existentes.
- Acciones de respuesta tomadas sobre las diferentes alternativas consideradas para la resolución de la brecha.
- Acciones tomadas para la prevención de futuras brechas.
- Impacto en la resolución del incidente de las acciones de respuesta tomadas.
- Acciones definidas para el seguimiento.

Se deberá dar traslado del informe de resolución al Delegado de protección de datos. Con independencia del informe de resolución implementado por los responsables de gestión del incidente de seguridad, el Delegado de protección de datos emitirá un informe propio en el que reflejará sus conclusiones sobre todos los hechos y actuaciones llevadas a cabo, en especial sobre las posibles causas del incidente, el impacto sobre los derechos y libertades de los

afectados y sobre la Corporación, la gestión del incidente y la identificación de los posibles responsables en su caso. El Delegado elevará su informe a la Presidencia de la Corporación y lo incorporará a su Informe/Memoria anual correspondiente.

3º. Proceso de notificación

Independientemente de las notificaciones internas que se deban producir para gestionar un incidente de seguridad, la Diputación de Valencia deberá notificar a:

3.A La autoridad de control en protección de datos

En caso de brecha de la seguridad de los datos personales, la Diputación de Valencia deberá notificar a la autoridad de control competente sin dilación indebida y, de ser posible, 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. El plazo de 72 horas empieza a calcularse desde el instante en que se tenga constancia de que el incidente de seguridad ha afectado a datos personales, incluyendo las horas trascurridas durante fines de semana y días festivos.

Se establecerá la metodología y se facilitarán las herramientas necesarias para poder valorar la procedencia de la comunicación de la brecha a la autoridad de control.

En caso de que se determine la procedencia de notificar a la autoridad, la notificación se realizará a través del formulario destinado a tal efecto en la

Sede Electrónica de la Agencia Española de Protección de Datos (AEPD): "Notificación de brechas de seguridad de los datos personales (art. 33 RGPD)" o por el señalado por la autoridad de control autonómica, en su caso.

En la notificación, se proporcionará la siguiente información:

· Datos identificativos y de contacto de la entidad / Responsable del tratamiento.
· Datos identificativos y de contacto del Encargado del tratamiento, en caso de que estuviera implicado en la brecha.
· Datos identificativos y de contacto del Delegado de Protección de Datos.
· Datos de la notificación: indicar si se trata de una nueva brecha de datos personales o de la modificación de una notificación hecha con anterioridad.
·Información sobre el tratamiento: desde cuándo se viene realizando; nº aproximado de personas físicas sobre las que se tratan datos; ámbito geográfico.
· Información sobre la brecha y sus consecuencias: accidental/intencionado; origen del incidente; cómo ha ocurrido la brecha; dimensiones afectadas; en caso de brecha de confidencialidad, si los datos estaban protegidos; en caso de brecha de disponibilidad, si se ha recuperado la disponibilidad de los datos personales; en caso de brecha de integridad, si los datos han sido alterados y usados de forma ilegal; posibles consecuencias sobre las personas físicas y grado de afectación; constancia de que se hayan materializado las consecuencias identificadas; resumen de la brecha.
· Tipos de datos afectados.

· Perfil de las personas afectadas (menores, miembros de colectivos vulnerables, otros perfiles) y número de personas afectadas.
· Implicaciones transfronterizas.
· Medidas de seguridad adoptadas antes de la brecha.
· Acciones tomadas tras el incidente
· Comunicación a los afectados
· Documentación adjunta
· Indicación de si se trata de una notificación completa o inicial.

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

Antes del plazo máximo de 30 días hábiles desde la notificación inicial, se deberá completar toda la información mediante una “modificación” de la notificación anterior, incluida la decisión tomada sobre la comunicación de la brecha de datos personales a los afectados.

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.

A modo de contingencia, en caso de no estar disponible el servicio electrónico de la AEPD, se deberá contactar con la Agencia, en el número de teléfono u otra vía de contacto establecida en su portal web, y acordar el canal alternativo por el que realizar la notificación.

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

Las notificaciones de brechas de seguridad ante la autoridad de control serán llevadas a cabo por el Delegado de protección de datos.

3.B Los afectados

Cuando sea probable que la brecha de seguridad de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, se comunicará al afectado sin dilación indebida.

Se establecerá la metodología y se facilitarán las herramientas necesarias para poder valorar la procedencia de la comunicación de la brecha a los interesados.

Asimismo, la brecha deberá ser comunicada a los afectados a solicitud de la autoridad de control competente.

La comunicación será realizada en un lenguaje claro y sencillo, y deberá contener, como mínimo, la siguiente información:

• Datos de contacto del Delegado de Protección de Datos.
• 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.
• 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 se deberá realizar, preferentemente, de forma directa al afectado, ya sea por teléfono, correo electrónico, correo postal, o a través de cualquier otro medio dirigido al afectado que se considere adecuado.

Las notificaciones a los afectados serán llevadas a cabo por el área o departamento responsable de los datos implicados, en coordinación con el Servicio de Informática.

4º. Seguimiento y cierre

Esta fase tiene por objetivo solventar posibles deficiencias en la gestión de incidentes o incorporar mejoras que permitan una mejor respuesta en las siguientes ejecuciones. Debe de servir por tanto para:

• Depurar errores o actualizar información que se haya evidenciado obsoleta.
• Detectar nuevos mecanismos de control que puedan ser necesarios o mejorar los ya existentes, y modificar en su caso las medidas técnicas y organizativas definidas en la fase de preparación.
• Revisar la eficacia del proceso de gestión de incidentes.
• Analizar la información que todavía esté pendiente de procesar y que pueda aportar mejoras.

• Comunicar los resultados del proceso y realizar una valoración final del incidente que se añada al informe de resolución para su cierre.

P/PDP-006 PROCEDIMIENTO DE ANÁLISIS DE RIESGOS

OBJETIVOS Y ALCANCE

Analizar los riesgos de los tratamientos de datos que lleva a cabo la Diputación de Valencia, con el fin de establecer medidas de seguridad adecuadas para garantizar los derechos y libertades de las personas físicas cuyos datos personales son tratados por la Diputación.

Están afectados:

- Todos aquellos tratamientos de datos de carácter personal cuyo "Responsable del Tratamiento" o "Encargado del tratamiento" sea la Diputación de Valencia.

Entidades de la Diputación de Valencia afectadas:

- El **Centro Gestor del tratamiento de datos (CGT)**.
- El **Servicio de Informática**.
- El **Departamento de Protección de Datos.**

DESARROLLO

1º. Descripción de las operaciones de actividades de tratamiento

Se deberá efectuar una descripción de los tratamientos sujetos al análisis de riesgos, lo que permitirá obtener un conocimiento del ciclo de vida de los datos, de las actividades realizadas y de cualquier elemento que interviene en las mismas. Las actividades de tratamiento se podrán agrupar por procesos comunes expuestos a riesgos similares.

La descripción de los tratamientos y las actividades que comportan debe ser cumplimentada por el CGT correspondiente, pudiendo implicar a más de un CGT. La descripción del entorno tecnológico en el que se desarrollan las actividades de tratamiento debe ser cumplimentada, en su caso, por el Servicio de Informática.

2º. Gestión de riesgos

La adecuada gestión de riesgos requiere un proceso de identificación, evaluación y tratamiento de los riesgos a los que está expuesto cada actividad de tratamiento o cada proceso común expuesto a riesgos similares.

Una vez identificados los riesgos inherentes a la actividad de tratamiento de partida, se aplicarán medidas de seguridad y control que reduzcan su nivel de exposición. Para cada uno de los riesgos identificados, se deberán establecer tantas medidas de seguridad como sean necesarias para garantizar un nivel de seguridad y control adecuado que reduzca la exposición al riesgo.

La Diputación de Valencia establecerá la metodología y facilitará las herramientas necesarias para poder efectuar el análisis de riesgos.

Los riesgos identificados y las medidas de control definidas deberán documentarse, con el objetivo de evidenciar la evaluación de riesgos realizada y tener una base de trabajo ante futuras revisiones del análisis derivadas de cambios en las actividades de tratamiento.

Por último, dado que los riesgos son variables y pueden cambiar ante variaciones en las actividades de tratamiento, se debe garantizar una adecuada gestión de riesgos mediante la monitorización continua de los riesgos y la evaluación periódica de la efectividad de las medidas de control definidas para reducir el nivel de exposición al riesgo. Por tanto, se revisará el análisis de riesgos realizado ante cualquier cambio significativo en las actividades de tratamiento que pueda derivar en la aparición de nuevos riesgos.

La evaluación de los riesgos asociados a los tratamientos de datos personales deberá ser complementada con las disposiciones internas relativas a la evaluación de riesgos de los sistemas de información.

El Departamento de Protección de Datos y Seguridad de la Información prestará asesoramiento en las actividades destinadas a la evaluación de riesgos de los tratamientos de datos personales.

P/PDP-007 PROCEDIMIENTO PARA LA EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS (EIPD)

OBJETIVOS Y ALCANCE

Identificar en qué supuestos es necesario llevar a cabo una Evaluación de Impacto de Protección de Datos y, en su caso, las consideraciones a tener en cuenta para que dicha Evaluación se lleve a cabo satisfactoriamente.

Están afectados:

- Todos los tratamientos de datos de carácter personal cuyo "Responsable del Tratamiento" sea la Diputación de Valencia, en particular aquellos que utilizan nuevas tecnologías, y que por su naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas físicas.

Entidades de la Diputación de Valencia afectadas:

- El **Centro Gestor del tratamiento de datos (CGT)**
- El **Servicio de Informática**, en su caso
- El **Delegado de Protección de Datos**
- El **Departamento de protección de Datos y Seguridad de la información**

DESARROLLO

El **Departamento de Protección de Datos y Seguridad de la Información** establecerá la metodología y facilitará las herramientas necesarias para poder llevar a cabo el análisis de necesidad y, en su caso, la EIPD.

El **Delegado de Protección de Datos** ofrecerá el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la EIPD y supervisará su aplicación.

Cada **CGT** es responsable de llevar a cabo el análisis de necesidad de realizar la EIPD, ejecutar la EIPD en caso de resultar necesario y poner en conocimiento del Delegado de protección de datos el resultado de las anteriores.

El **Servicio de Informática** llevará a cabo el análisis de los elementos tecnológicos del tratamiento que incidan en la valoración del impacto.

1º. Análisis de la necesidad de realizar EIPD

La normativa en materia de protección de datos exige llevar a cabo una Evaluación de Impacto en la Protección de Datos (en adelante, EIPD) para todo aquel nuevo tratamiento que probablemente entrañe, por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas. **Las EIPD deberán llevarse a cabo antes de poner en marcha el tratamiento.**

Para analizar si una actividad de tratamiento requiere de EIPD de forma previa a poner en marcha dicho tratamiento, se tendrán en cuenta la finalidad del

tratamiento, las categorías y el volumen de datos que se recoge, la duración y extensión geográfica del tratamiento, así como las operaciones de tratamiento de las que serán objeto, especialmente si se trata de tratamientos automatizados como la elaboración de perfiles.

Naturaleza del tratamiento: Se deben valorar las características más básicas del tratamiento y ver si estas pueden implicar un alto riesgo.

Alcance del tratamiento: Se deben valorar los efectos o consecuencias del tratamiento, identificando hasta qué punto puede llegar y si éste puede suponer un alto riesgo.

Contexto del tratamiento: Se debe valorar el conjunto de circunstancias bajo las cuales se realizarán las actividades de tratamiento, con el objetivo de verificar si pueden suponer un alto riesgo.

Finalidades del tratamiento: Se deben identificar cada una de las finalidades del tratamiento y analizar si estas derivan en un alto riesgo.

En cualquier caso, será obligatorio realizar una EIPD cuando concurra alguna de las siguientes causas:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- Tratamiento a gran escala de categorías especiales de datos y datos relativos a condenas e infracciones penales.

- Observación sistemática a gran escala de una zona de acceso público.

Asimismo, se tendrán en cuenta las posibles listas de tratamientos que requieren EIPD que la Agencia Española de Protección de Datos pueda publicar una lista de tratamientos, así como otras para las actividades de tratamiento en las que no sería necesario.

El CGT que desee llevar el cabo el tratamiento procederá previamente a la realización del análisis de necesidad mediante las utilidades habilitadas para tal fin por el Departamento de Protección de Datos y Seguridad de la Información. El análisis de necesidad y su resultado será comunicado al Delegado de protección de datos.

El resultado del análisis de necesidad determinará la obligación o no de ejecutar una EIPD.

2º. Realización de la EIPD

En caso de que el resultado del análisis de necesidad determine la obligación de realizar una EIPD.

La EIPD deberá contener, como mínimo:

- Una descripción sistemática de la actividad de tratamiento prevista.
- Una evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
- Una evaluación de los riesgos.
- Las medidas de seguridad previstas para mitigar los riesgos y garantizar la protección de los datos personales.

El CGT correspondiente procederá a la realización de la EIPD mediante las utilidades habilitadas para tal fin por el Departamento de Protección de Datos y Seguridad de la Información.

Si fuera necesario evaluar aspectos o partes del tratamiento de datos que fueran competencia o de conocimiento de otras unidades distintas al CGT, el CGT indicará cuáles son los citados aspectos o partes del tratamiento y la unidad interna afectada, a la cual se le dará traslado para la evaluación específica. En especial, se dará traslado al Servicio de Informática siempre que existan aspectos o elementos de carácter tecnológico que deban ser objeto de la evaluación.

La EIPD y su resultado serán comunicados al Delegado de protección de datos.

3º. Consulta previa a la autoridad de control

Si tras haber realizado la EIPD, el resultado de la misma determina que el tratamiento entraña un alto riesgo para los derechos y libertades de los interesados si el responsable no toma medidas para para mitigarlo, será necesario elevar consulta a la Autoridad de Control competente antes llevarlo a cabo.

La consulta **será realizada por el Delegado de protección de datos** y deberá incluir lo siguiente:

- Las responsabilidades respectivas del responsable del tratamiento, los corresponsables y los encargados del tratamiento implicados en el tratamiento.
- Los fines y medios del tratamiento.

- Las medidas y garantías establecidas para proteger los derechos y libertades de los interesados.
- Los datos de contacto del Delegado de Protección de Datos.
- La evaluación de impacto.
- Cualquier otra información a solicitud de la Autoridad de Control.

La comunicación se llevará a cabo a través del canal habilitado al efecto por la Agencia Española de Protección de Datos en su Sede Electrónica: “Consulta previa al inicio de tratamientos de riesgo alto (art. 36 RGPD)”.

Si la autoridad de control considera que el tratamiento previsto podría infringir el RGPD, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, debe asesorar en un plazo de ocho semanas desde la solicitud de la consulta. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación.

En tanto la autoridad de control no se haya manifestado, no podrá llevarse a cabo el tratamiento de datos en cuestión.

P/PDP-008 PROCEDIMIENTO DE DILIGENCIA EN LA CONTRATACIÓN DE ENCARGADOS DE TRATAMIENTO

OBJETIVOS Y ALCANCE

Verificar el cumplimiento de la legislación en materia de protección de datos por parte de los prestadores de servicios con acceso a datos personales de la

Diputación de Valencia. La Corporación elegirá, únicamente, encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la normativa de protección de datos y se garantice la protección de los derechos de los interesados.

Están afectados:

- Todos aquellos tratamientos de datos de carácter personal que lleven a cabo los prestadores de servicios por cuenta de la Diputación de Valencia (encargados del tratamiento).

Entidades de la Diputación de Valencia afectadas:

- Cada **unidad administrativa responsable de las prestaciones de servicios** con acceso a datos personales.
- El **Departamento de Protección de Datos y Seguridad de la Información**.

DESARROLLO

Cada unidad administrativa responsable de prestaciones de servicios remitirá a los prestadores de servicios que tengan acceso a datos personales un formulario con diversas cuestiones de obligada respuesta, con el fin de valorar el grado de cumplimiento en relación con la normativa de protección de datos. Asimismo, se requerirán evidencias de cumplimiento. Las cuestiones versarán sobre el grado de adecuación del encargado del tratamiento a la normativa de protección de datos, entre ellas:

-Elaboración de Registro de Actividades del Tratamiento
-Nombramiento de Delegado de Protección de Datos
-Cumplimiento del deber de información
-Realización de Análisis de Riesgos
-Adecuación de las Políticas web
-Información en relación con las transferencias internacionales de datos y garantías
-Información sobre subcontratación
-Formación al personal en materia de protección de datos
-Suscripción de normas de uso TIC y compromisos de confidencialidad por parte de las personas trabajadoras
-Medidas de seguridad implementadas
-Certificaciones de seguridad
-Realización de auditorías
-Incidentes o brechas de seguridad sufridas
-Procedimientos de respuesta frente a incidentes y brechas de seguridad

Los formularios de valoración serán facilitados por el Departamento de Protección de Datos y Seguridad de la Información y, una vez cumplimentados, serán puestos a disposición del Delegado de protección de datos, quien valorará, conforme al cuestionario y las evidencias remitidas, si dan cumplimiento a la normativa de protección de datos.

En caso de que algún prestador no ofrezca garantías suficientes, se deberá valorar si se puede subsanar y/o prestar una medida compensatoria o alternativa, estableciendo un plazo al efecto. En otro caso, se valorará la contratación con dicho proveedor por parte de la Diputación de Valencia.

P/PDP-009 PROCEDIMIENTO INFORMATIVO SOBRE VULNERACIÓN DE NORMATIVA DE PROTECCIÓN DE DATOS

OBJETIVOS Y ALCANCE

Regular un mecanismo o instrumento de transparencia y recopilación de información utilizado a nivel interno por el Delegado de Protección de Datos con las siguientes finalidades:

• Hacer saber a los posibles implicados que se ha apreciado alguna acción que pudiera ser constitutiva de infringir la normativa legal o interna en materia de protección de datos personales.

• Poder incorporar mayor información que pudiese ser relevante para que el Delegado valore jurídicamente el alcance exacto de la posible vulneración.

• Informar en todo momento a los implicados de las actuaciones que el Delegado pueda emprender en el marco de sus competencias.

Están afectados:

- Todos los tratamientos de datos de carácter personal a los que resulte de aplicación el Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia y que, por tanto, se encuentren bajo la supervisión del Delegado de protección de datos.

Entidades de la Diputación de Valencia afectadas:

- Personal y unidades administrativas que traten datos personales y estén sujetos a la aplicación de la normativa legal e interna en la materia.
- El **Delegado de protección de datos**.

DESARROLLO

El Delegado podrá iniciar el procedimiento informativo en el curso de cualquiera de sus actuaciones cuando lo considere necesario para el cumplimiento de los objetivos de transparencia y recopilación de información.

Fases. El procedimiento informativo está conformado por dos fases:

• **Fase I**. Se traslada a los implicados información mínima como: antecedentes de hecho, normativa aplicable, posibles vulneraciones apreciadas y posibles responsables (si ya se contemplan responsables). Según el papel o protagonismo que desempeñe en el procedimiento concreto, algún implicado puede recibir sólo parte de la citada información. Se incorpora también la información que, en su caso, puedan aportar los interesados.

Se entiende por implicados a aquellas personas, unidades administrativas o entidades que pueden ser protagonistas en una posible vulneración normativa: responsables directos e indirectos de la vulneración, titulares de los datos afectados, unidades gestoras o terceros que han participado en cualquier fase del tratamiento de datos involucrado, testigos o informadores en general que pueden aportar información relevante.

• **Fase II**. Se traslada a los implicados la información relativa a los posibles responsables (si ya se contemplan responsables), la información aportada por otros implicados, en su caso, y las conclusiones del Delegado tras la valoración del conjunto de información que conforma el procedimiento. Según el papel o protagonismo que desempeñe en el procedimiento concreto, algún implicado puede recibir sólo parte de la información.

Plazos. Con carácter general, el plazo para aportar información por parte de los implicados será de diez días hábiles desde que se les comunica la Fase I. Excepcionalmente podría ampliarse este plazo en diez días hábiles más si el Delegado lo considera oportuno atendiendo a la complejidad de la información a aportar por los implicados, a la propia naturaleza de los soportes, fuentes o depositarios de la información o a la dificultad de concretar o identificar a responsables. El procedimiento informativo se cierra o concluye con la comunicación de la Fase II. El plazo máximo para concluir el procedimiento informativo será de seis meses.

El Delegado puede dejar en suspenso el transcurso de los citados plazos si de las informaciones y averiguaciones aportadas se infiere la posible existencia de otros implicados, y considera oportuno incorporarlos al procedimiento informativo. En este supuesto, los plazos se reanudarán cuando las actuaciones con los nuevos implicados se equiparen con las llevadas a cabo con el resto de implicados.