



MINISTERIO
DE TRABAJO
Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO
DE EMPLEO ESTATAL
SEPE
SERVEI PÚBLIC
D'Ocupació Estatal



MINISTERIO
DE EDUCACIÓN, FORMACIÓN PROFESIONAL
Y DEPORTES



**Generalitat
de Catalunya**

SOC

Servei d'Ocupació de Catalunya



SPAIN

Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Protección de datos de carácter personal

- Introducción
- Principios generales de protección de datos de carácter personal
- Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal
- Resumen

Introducción

Introducción a los Requisitos Legales en Seguridad de la Información

- Cumplir con la legislación es el principal criterio para determinar los requisitos de seguridad y seleccionar salvaguardas.
- Principios esenciales de seguridad, como la protección de datos y la privacidad, son fundamentales según MAGERIT e ISO 27002.
- La Constitución Española de 1978 y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) establecen regulaciones para salvaguardar la intimidad y los derechos digitales de los ciudadanos.

Legislación de Protección de Datos en España

- La Directiva 95/46/CE y la LOPD garantizan la protección de datos y la libre circulación de los mismos en la Unión Europea.
- La LOPDGDD 3/2018, también conocida como Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, es una norma extensa y práctica en España.
- Estas leyes establecen requisitos específicos para empresas y organizaciones en el manejo y protección de datos personales.

Principios generales de protección de datos de carácter personal

Introducción

- La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) tiene como objetivo principal adaptar el ordenamiento jurídico español al Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
- También busca garantizar los derechos digitales de la ciudadanía, conforme a lo establecido en el artículo 18.1 de la Constitución Española.
- En resumen, la LOPDGDD se enfoca en adaptar las leyes españolas al RGPD y asegurar los derechos digitales de los ciudadanos según la Constitución.

Principios generales de protección de datos de carácter personal

Ámbito de aplicación y conceptos fundamentales

Introducción a la LOPDGDD

¿Qué es la LOPDGDD?

- Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.
- Adapta el Reglamento General de Protección de Datos (RGPD) al ordenamiento jurídico español.

¿Para qué sirve?

- Proteger los datos personales de los ciudadanos.
- Regular el tratamiento de los datos personales por parte de empresas y organizaciones.

¿Cuándo se aplica?

- Cuando se traten datos personales de personas físicas en el ámbito de la Unión Europea.
- Cuando el responsable del tratamiento tenga su residencia habitual en la Unión Europea.
- Cuando el tratamiento se ofrezca a personas que se encuentren en la Unión Europea.

Principios generales de protección de datos de carácter personal

Ámbito de aplicación y conceptos fundamentales

Conceptos fundamentales

¿Qué son datos de carácter personal?

- Cualquier información que pueda identificar a una persona física, directa o indirectamente.
- Ejemplos: nombre, DNI, dirección, teléfono, correo electrónico, etc.

¿Qué es un fichero?

- Conjunto de datos de carácter personal, sin importar la forma o modo de almacenamiento.

¿Quién es el afectado o interesado?

- Persona física titular de los datos que se están tratando.

¿Qué es el consentimiento?

- Manifestación de voluntad libre, inequívoca, específica e informada por la que el interesado acepta el tratamiento de sus datos.

Principios generales de protección de datos de carácter personal

Ámbito de aplicación y conceptos fundamentales

Conceptos fundamentales

¿Qué es el tratamiento de los datos?

- Cualquier operación realizada con datos personales, como la recogida, almacenamiento, uso, comunicación o cancelación.

¿Quién es el responsable del tratamiento?

- Persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento.

¿Quién es el encargado del tratamiento?

- Persona física o jurídica que trata los datos personales por cuenta del responsable.

Principios generales de protección de datos de carácter personal

Ámbito de aplicación y conceptos fundamentales

Conceptos fundamentales

¿Qué derechos tienen las personas?

- Acceso: A sus datos personales.
- Rectificación: A corregir sus datos personales si son inexactos o incompletos.
- Supresión: A que se eliminen sus datos personales.
- Limitación del tratamiento: A restringir el tratamiento de sus datos personales.
- Oposición: A que se traten sus datos personales.
- Portabilidad: A recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento.

¿Cómo se pueden ejercer estos derechos?

- Mediante la presentación de una solicitud al responsable del tratamiento.

Principios generales de protección de datos de carácter personal

Ámbito de aplicación y conceptos fundamentales

Conceptos fundamentales

¿Cuándo no se aplica la LOPDGDD?

- Cuando el tratamiento de datos se realiza en el ámbito de una actividad personal o doméstica.
- Cuando el tratamiento de datos se realiza por parte de las autoridades competentes en materia de prevención, investigación, detección y enjuiciamiento de delitos.
- Cuando el tratamiento de datos se realiza con fines de seguridad nacional o defensa.

¿Qué derechos tienen los familiares de una persona fallecida?

- Acceder a los datos personales del fallecido.
- Rectificar o eliminar los datos personales del fallecido.
- Oponerse al tratamiento de los datos personales del fallecido.

¿Cómo se pueden ejercer estos derechos?

- Mediante la presentación de una solicitud al responsable del tratamiento por parte de los familiares o herederos del fallecido.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Calidad de los Datos

- El RGPD establece que los datos personales deben ser recogidos de manera estrictamente necesaria para la finalidad del tratamiento.
- Los datos deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que son tratados.
- Se deben mantener actualizados y exactos, cancelándolos si resultan inexactos o si dejan de ser necesarios.

Seguridad de los Datos

- El RGPD exige que se apliquen medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos.
- Estas medidas incluyen el cifrado de datos, garantizar la confidencialidad, integridad, disponibilidad y resiliencia, y la capacidad de restaurar la disponibilidad.
- El responsable del tratamiento debe asegurar que cualquier persona que acceda a los datos lo haga siguiendo sus instrucciones.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Obligaciones de Registro

- Las empresas deben mantener registros detallados de las actividades de tratamiento de datos.
- Esto incluye registros de las solicitudes de acceso de los interesados, violaciones de seguridad, obtención de consentimientos y evaluaciones de impacto de protección de datos.

Principios de Protección de Datos

- Los principios fundamentales de protección de datos se centran en la calidad y seguridad de la información.
- La calidad implica que los datos sean adecuados, pertinentes, exactos y actualizados.
- La seguridad requiere medidas técnicas y organizativas para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Cumplimiento del RGPD

- Cumplir con el RGPD no es suficiente; las empresas deben demostrar responsabilidad proactiva en la protección de datos.
- Esto implica mantener registros detallados de las actividades de tratamiento y cumplir con obligaciones de llevanza de registros.

Implicaciones de la LOPDGDD

- La LOPDGDD establece normativas específicas para adaptar el RGPD al ordenamiento jurídico español.
- Las obligaciones de calidad y seguridad de los datos son fundamentales para cumplir con la legislación vigente y proteger los derechos de los individuos.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Derechos de las personas

- La LOPDGDD y el RGPD (Reglamento General de Protección de Datos) garantizan una serie de derechos fundamentales para las personas físicas respecto a sus datos personales.
- Estos derechos incluyen la capacidad de controlar cómo se utilizan y gestionan sus datos por parte de las empresas y organizaciones.
- Es esencial que las empresas informen de manera clara y completa a los interesados sobre el uso que se dará a sus datos, así como sobre sus derechos en relación con ellos.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Derechos de las personas

Derechos Reconocidos

- Queja ante autoridades de control: Las personas tienen el derecho de presentar una queja ante las autoridades de control de protección de datos, como la Agencia Española de Protección de Datos (AEPD), si consideran que sus derechos no se están respetando.
- Retirada del consentimiento: Las personas pueden retirar en cualquier momento el consentimiento otorgado previamente para el tratamiento de sus datos personales.
- Acceso, rectificación o supresión de datos: Los individuos tienen derecho a acceder a sus datos personales, así como a solicitar su rectificación o supresión (derecho al olvido) por parte de las empresas u organizaciones que los posean.
- Conocimiento de tratamientos automatizados: Las personas tienen derecho a ser informadas sobre la existencia de cualquier tratamiento automatizado de sus datos personales, incluyendo la elaboración de perfiles.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Derechos de las personas

Derechos Reconocidos

- Oposición a ciertos tratamientos: Los individuos pueden oponerse al tratamiento de sus datos para ciertos fines, como el marketing directo, o decisiones basadas únicamente en un tratamiento automatizado.
- Información sobre la conservación de datos: Las personas tienen derecho a conocer cuánto tiempo se conservarán sus datos personales.
- Contacto con delegados de protección de datos: Las empresas deben proporcionar a los individuos los datos de contacto de los delegados de protección de datos designados para atender consultas y reclamaciones sobre el tratamiento de datos.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Derechos de las personas

Representación por Organizaciones Sin Ánimo de Lucro

Las personas tienen la posibilidad de ejercer sus derechos a través de organizaciones sin ánimo de lucro, que pueden actuar en su nombre y presentar reclamaciones colectivas en caso de incumplimiento de la normativa de protección de datos.

Consentimiento Explícito

El consentimiento para el tratamiento de datos debe ser explícito y no predefinido por defecto. Esto significa que las personas deben otorgar su consentimiento de manera clara y específica para cada operación de tratamiento de datos.

Retiro del Consentimiento

Las personas tienen el derecho a retirar su consentimiento en cualquier momento de forma sencilla y sin que esto les suponga ninguna dificultad.

Principios generales de protección de datos de carácter personal

Principios de protección y derechos de las personas

Derechos de las personas

Detalle de los Derechos

- Derecho de Acceso: Obtención gratuita de información sobre la existencia y tratamiento de los datos personales.
- Derecho de Rectificación: Modificación de datos inexactos o incompletos en un plazo de 10 días.
- Derecho de Supresión (Derecho al Olvido): Eliminación de datos por revocación del consentimiento o por ser inadecuados o excesivos.
- Derecho de Oposición: Impedir el tratamiento de datos para ciertos fines, como la publicidad o las decisiones automatizadas.
- Derecho de Limitación del Tratamiento: Suspensión del tratamiento en determinadas circunstancias.
- Derecho a la Portabilidad: Solicitar que los datos sean transferidos a otro responsable de tratamiento.

Principios generales de protección de datos de carácter personal

Comunicación y acceso por terceros

- La LOPDGDD establece directrices claras para la comunicación y cesión de datos personales a terceros.
- El consentimiento del interesado es fundamental para la comunicación de sus datos, pero existen excepciones definidas por ley. Estas excepciones incluyen situaciones donde la comunicación es necesaria para el cumplimiento de obligaciones legales o para la prestación de servicios esenciales.
- Los responsables del tratamiento deben asegurarse de que cualquier tercero que acceda a los datos cumpla con las normativas de protección de datos.
- Los encargados del tratamiento deben tener contratos escritos que especifiquen claramente sus responsabilidades y obligaciones para garantizar el cumplimiento normativo.
- El consentimiento otorgado por el interesado debe ser claro, voluntario y específico, y puede ser revocado en cualquier momento.
- Estas medidas aseguran que los derechos de los interesados sean protegidos y que el tratamiento de datos se realice de manera justa y transparente.

Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal

Infracciones

El régimen sancionador se recoge en el título IX de la LOPDGDD (artículo 70-78). Se fija que los responsables de ficheros, del tratamiento y encargados del tratamiento, estarán sujetos al régimen sancionador según las infracciones sean leves, graves o muy graves.

Infracciones Consideradas Leves

- Incumplimiento del principio de transparencia de la información.
- Exigencia de pago de un canon por facilitar información al afectado.
- No atender solicitudes de ejercicio de derechos de los interesados.
- No informar al afectado sobre destinatarios de sus datos.
- Falta de formalización de acuerdos entre responsables del tratamiento.
- No poner a disposición de los afectados aspectos del acuerdo.
- Notificación incompleta o tardía.
- Incumplimiento de la obligación de documentar violaciones de seguridad.
- No publicar datos de contacto del delegado de protección de datos.

Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal

Infracciones

El régimen sancionador se recoge en el título IX de la LOPDGDD (artículo 70-78). Se fija que los responsables de ficheros, del tratamiento y encargados del tratamiento, estarán sujetos al régimen sancionador según las infracciones sean leves, graves o muy graves.

Infracciones Graves

- Tratamiento de datos de un menor sin consentimiento.
- No atender reiteradamente los derechos del interesado.
- Falta de medidas técnicas adecuadas para cumplir la ley y garantizar el fin específico del tratamiento, así como la seguridad.
- Encargar tratamiento a un tercero sin contrato formal.
- Ausencia de registro de actividades.
- Falta de cooperación con autoridades de control.
- Uso de sello o certificación no otorgado por entidad certificadora.

Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal

Infracciones

El régimen sancionador se recoge en el título IX de la LOPDGDD (artículo 70-78). Se fija que los responsables de ficheros, del tratamiento y encargados del tratamiento, estarán sujetos al régimen sancionador según las infracciones sean leves, graves o muy graves.

Infracciones muy Graves

- Incumplimiento de los requisitos de validez del consentimiento.
- Uso de datos para fines incompatibles con su recogida.
- Tratamiento de datos penales o de seguridad sin autorización.
- Omisión de informar al afectado sobre el tratamiento de sus datos.
- Violación del deber de confidencialidad.
- Exigencia de pago al interesado.
- Transferencia internacional a países sin garantías del reglamento.
- Obstaculizar el acceso del personal de la autoridad de protección de datos.

Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal

Sanciones y criterios de graduación

La LOPDGDD establece tres tramos para sanciones económicas, con criterios para determinar la cuantía.

- Infracciones leves: hasta 40.000 €
- Infracciones graves: de 40.001 € a 300.000 €
- Infracciones muy graves: desde 300.001 € hasta 20.000.000 €

Criterios para graduar sanciones:

- Continuidad de la infracción.
- Relación de la actividad del infractor con el tratamiento de datos.
- Posibilidad de inducción de la infracción por parte del afectado.
- Fusión con una empresa infractora.
- Impacto en los derechos de los menores.
- Existencia de un delegado de protección de datos.
- Otros datos relevantes que determinen la ilegalidad.

Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal

Titularidad de los ficheros

Ficheros de Titularidad Pública.

Son aquellos bajo responsabilidad de entidades estatales o regionales con funciones constitucionales o vinculadas al ejercicio de potestades de derecho público. Esto incluye órganos constitucionales, instituciones autonómicas, administraciones públicas territoriales, así como entidades vinculadas o dependientes de estas. La finalidad de estos ficheros es el ejercicio de potestades de derecho público.

Ficheros de Titularidad Privada.

En contraste, estos ficheros son responsabilidad de personas, empresas o entidades de derecho privado. La titularidad de su capital o la fuente de sus recursos económicos son independientes de su responsabilidad sobre estos ficheros. También, se incluyen los ficheros bajo la responsabilidad de corporaciones de derecho público, siempre que no estén directamente vinculados al ejercicio de potestades de derecho público definidas por su normativa específica.

Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización

Introducción

Identificación y clasificación de datos personales según el RGPD

Esencial conocer los datos personales almacenados y tratados por la empresa para cumplir con el Reglamento General de Protección de Datos (RGPD).

El RGPD clasifica los datos personales en tres categorías: datos de carácter especial, datos relativos a condenas y el resto de los datos personales.

A diferencia de la Ley Orgánica de Protección de Datos (LOPD) de 1999, el RGPD no especifica medidas de seguridad para cada tipo de dato, sino que requiere que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas.

El artículo 25 del RGPD establece que el responsable del tratamiento debe garantizar que el tratamiento de datos se realice solo con fines específicos, mientras que el artículo 32 requiere que el encargado del tratamiento aplique medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización

Introducción

Responsabilidades del encargado del tratamiento y medidas de seguridad

Además, el encargado del tratamiento es responsable de implementar medidas de seguridad para proteger los datos.

El RGPD basa su concepto de seguridad en el análisis de riesgos, lo que implica que las medidas de seguridad deben ser proporcionales al riesgo identificado.

Esto significa que se deben implementar diferentes medidas de seguridad según el resultado del análisis de riesgos.

La Agencia Española de Protección de Datos (AEPD) proporciona la plataforma web [FACILITA](#) para ayudar en la determinación del análisis de riesgos.

Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización

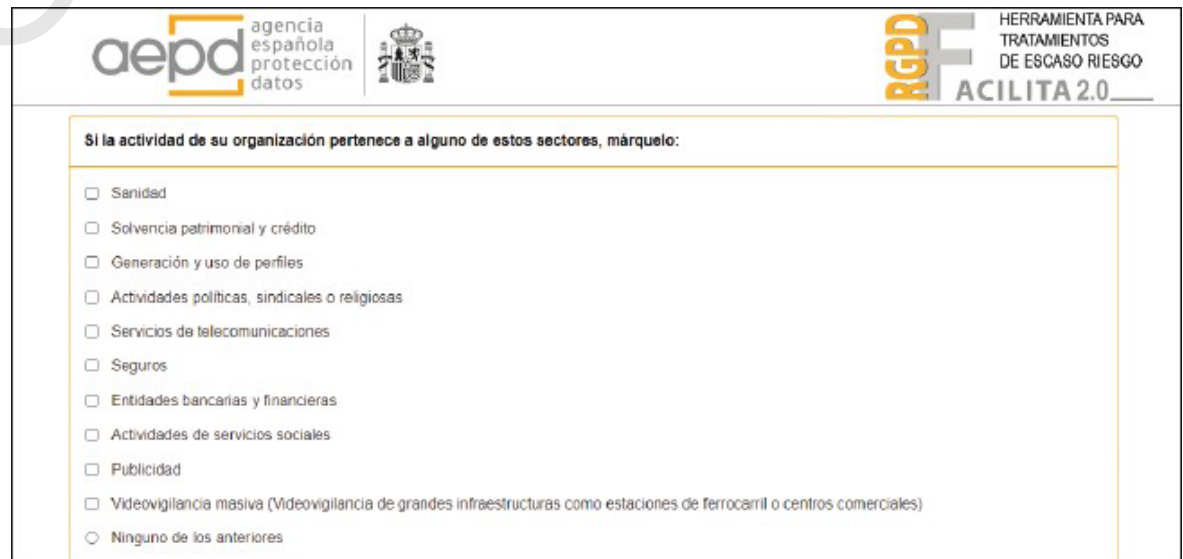
Introducción

Herramienta FACILITA de la AEPD y consideraciones finales

FACILITA es una herramienta proporcionada por la AEPD que ayuda a determinar si es necesario realizar un análisis de riesgos en función del tipo de datos personales y la finalidad del tratamiento.

Es importante tener en cuenta que, según la Ley de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), no es necesario realizar un registro de ficheros ni un documento de seguridad.

Es crucial comprender y clasificar correctamente los datos personales de acuerdo con las normativas vigentes para garantizar el cumplimiento legal y la protección de la privacidad de los individuos.



The screenshot shows the header of the FACILITA 2.0 tool. On the left is the AEPD logo (Agencia Española de Protección de Datos). In the center is the Spanish coat of arms. On the right is the text 'HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO FACILITA 2.0'. Below the header, there is a section titled 'Si la actividad de su organización pertenece a alguno de estos sectores, márquelo:'. This section contains a list of sectors with checkboxes: Sanidad, Solvencia patrimonial y crédito, Generación y uso de perfiles, Actividades políticas, sindicales o religiosas, Servicios de telecomunicaciones, Seguros, Entidades bancarias y financieras, Actividades de servicios sociales, Publicidad, Videovigilancia masiva (Videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales), and Ninguno de los anteriores.

aepd agencia española protección datos		HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO FACILITA 2.0	
Si la actividad de su organización pertenece a alguno de estos sectores, márquelo:			
<input type="checkbox"/>	Sanidad		
<input type="checkbox"/>	Solvencia patrimonial y crédito		
<input type="checkbox"/>	Generación y uso de perfiles		
<input type="checkbox"/>	Actividades políticas, sindicales o religiosas		
<input type="checkbox"/>	Servicios de telecomunicaciones		
<input type="checkbox"/>	Seguros		
<input type="checkbox"/>	Entidades bancarias y financieras		
<input type="checkbox"/>	Actividades de servicios sociales		
<input type="checkbox"/>	Publicidad		
<input type="checkbox"/>	Videovigilancia masiva (Videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales)		
<input type="radio"/>	Ninguno de los anteriores		

Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización

Datos de carácter especial

Tratamiento de datos de carácter especial

Datos de categorías especiales según el RGPD (artículo 9) incluyen información sobre origen étnico, opiniones políticas, convicciones religiosas, afiliación sindical, datos biométricos para identificación única, datos de salud, vida u orientación sexual.

El RGPD y la LOPDGDD prohíben el tratamiento de estos datos, salvo en cuatro circunstancias: consentimiento del interesado, necesidad para derecho laboral y protección social, protección del interesado o razones de interés en salud pública.

El consentimiento del interesado es una base legal para el tratamiento de estos datos, pero también se permite su tratamiento en casos específicos como necesidades laborales, protección del interesado y razones de interés en salud pública.

Datos personales relativos a condenas e infracciones penales

Según el artículo 10 del RGPD, el tratamiento de datos personales relacionados con condenas e infracciones penales solo puede llevarse a cabo bajo la supervisión de las autoridades públicas.

Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización

Medidas de salvaguarda a implementar

Las medidas de seguridad según el RGPD se basan en un análisis de riesgos para proteger los derechos y libertades de los interesados.

El artículo 32 del RGPD enumera medidas técnicas y organizativas apropiadas, incluyendo la seudonimización y cifrado de datos, garantía de confidencialidad, integridad y disponibilidad de sistemas, capacidad de restauración de datos y evaluación continua de medidas implementadas.

Detalles de las medidas de seguridad según el RGPD

La seudonimización y cifrado de datos se aplican especialmente a tratamientos de datos sensibles, como los de menores o personas vulnerables.

Garantizar la confidencialidad, integridad y disponibilidad de sistemas implica monitoreo constante y políticas internas de protección.

La capacidad de restauración rápida de datos es esencial, requiriendo políticas de backup efectivas.

La evaluación continua de medidas técnicas garantiza la seguridad del tratamiento de datos a lo largo del tiempo.

Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

En la LOPD de 1999, artículo 88, se requería un documento de seguridad con medidas técnicas y organizativas para el tratamiento de datos, obligatorio para el personal con acceso a sistemas de información.

En la actual LOPDGDD 3/2018, no se exige dicho documento ni su inscripción.

Las medidas de seguridad deben ser suficientes y demostrables para garantizar la seguridad de los datos tratados.

Es responsabilidad del encargado del tratamiento determinar y aplicar medidas que aseguren la integridad, disponibilidad y confidencialidad de los datos.

Resumen

Es fundamental que los sistemas de seguridad cumplan con la legislación vigente, especialmente en lo que respecta a la protección de datos personales, como lo establece la LOPDGDD y el RGPD europeo.

La LOPDGDD define conceptos clave como fichero, afectado o titular de los datos, y responsable del fichero, quien determina la finalidad y tratamiento de los datos.

Establece principios de seguridad para los titulares de datos, como calidad de los datos, derecho de información, acceso, rectificación, cancelación, oposición, consulta, indemnización y derecho a impugnación de valoraciones.

Categoriza las infracciones y establece sanciones económicas según su gravedad.

El cumplimiento de la LOPDGDD comienza con la notificación a la AEPD y la solicitud de inscripción del fichero, proporcionando información detallada sobre su naturaleza.

El RGPD categoriza los ficheros según las medidas de seguridad necesarias, desde básicas hasta altas, y requiere un documento de seguridad que evoluciona con la implementación de medidas de protección.