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
IRON HACK SPAIN

Auditoria en seguridad informática

IFCT0109 – Seguridad informática

MF0487_3 (90 horas)

Aplicación de la normativa de protección de datos de carácter personal

- Introducción
- Principios de protección de datos de carácter personal
- Normativa europea: Reglamento General de Protección de Datos (RGPD)
- Normativa nacional: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
- Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 994/2019 (RGPD y LOPDGDD)
- Guía para la realización de la auditoría bienal obligatoria de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Resumen

Introducción

Las tecnologías de la información han revolucionado la forma en que generamos, almacenamos y compartimos información, incluyendo datos personales sensibles a la privacidad de las personas.

Necesidad de proteger los datos personales:
Su protección es fundamental para garantizar la privacidad y el derecho a la autodeterminación informativa de los individuos.

Evolución de la normativa de protección de datos:
Las primeras normativas surgieron en un contexto tecnológico diferente al actual, requiriendo actualizaciones para adaptarse a los nuevos desafíos.

Desarrollo de un marco normativo europeo:
La Unión Europea ha desarrollado un marco normativo completo con el RGPD como norma fundamental, complementado por la Directiva sobre la privacidad en las comunicaciones electrónicas y otras normas y directrices.

Introducción

Importancia de la protección de datos:

Es crucial para:

- Proteger la privacidad de los individuos: garantizar que las personas controlen sus datos y que no se usen sin su consentimiento.
- Fomentar la confianza en la economía digital: crear un entorno digital seguro para transacciones e intercambio de información.
- Promover la innovación: estimular el desarrollo de nuevas tecnologías que respeten la privacidad y los derechos de los ciudadanos.

Análisis de la normativa vigente:
El capítulo analizará en detalle las diferentes normativas nacionales e internacionales, con especial atención al RGPD.

Derechos de los interesados:
Se abordarán los derechos que asisten a los titulares de los datos personales, como el derecho de acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad.

Principios de protección de datos de carácter personal

Introducción

En la era digital, la protección de los datos de carácter personal es un derecho fundamental que se configura como la capacidad de las personas para decidir sobre el uso de su información personal.

El conocimiento y control por parte de los individuos sobre el tratamiento de sus datos son esenciales para respetar los derechos fundamentales recogidos en la Constitución española, como la intimidad y las libertades públicas.

Marco normativo en España:

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) es la principal norma española en materia de protección de datos.

Esta ley adapta la normativa nacional al Reglamento General de Protección de Datos (RGPD), la norma de referencia a nivel europeo, y sustituye a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).

Principios de protección de datos de carácter personal

Conceptos principales de la protección de datos

- **Datos de carácter personal**: Cualquier información en texto, imagen o audio que permita la identificación de una persona.
- **Fichero**: Conjunto organizado de datos personales.
- **Tratamiento de datos**: Cualquier operación realizada con datos personales, como su recogida, almacenamiento, elaboración o cesión.
- **Responsable del fichero o tratamiento**: Persona física o jurídica que decide sobre la finalidad, el contenido y el uso de los datos.
- **Interesado o afectado**: Persona física cuyos datos son tratados.
- **Consentimiento del interesado**: Manifestación libre, inequívoca, específica e informada por la que el interesado acepta el tratamiento de sus datos.
- **Cesión o comunicación de datos**: Revelación de datos a personas distintas del interesado.
- **Datos relativos a la salud:** Información sobre el estado físico o psíquico de una persona.
- **Datos biométricos**: Características físicas, fisiológicas o conductuales que confirman una identidad única.
- **Transferencia internacional de datos**: Comunicación de datos a destinatarios fuera del Espacio Económico Europeo.
- **Elaboración de perfiles**: Utilización de datos para evaluar aspectos de una persona física, como su situación económica, salud o comportamiento.
- **Violaciones de seguridad**: Incidentes que supongan la pérdida, destrucción o alteración de datos personales, o el acceso no autorizado a los mismos.

Principios de protección de datos de carácter personal

Aspectos relevantes de la LOPDGDD:

- Derogación del concepto de "Fuentes de acceso público": La LOPDGDD elimina este concepto, aunque puede seguir siendo interpretado en otras leyes.
- Ampliación de los derechos de los interesados: La ley reconoce nuevos derechos, como el derecho a la portabilidad de los datos, el derecho a la limitación del tratamiento y el derecho a la oposición al tratamiento.
- Mayor transparencia y responsabilidad: Las empresas y organizaciones deben ser más transparentes en el tratamiento de los datos personales y deben rendir cuentas ante las autoridades de control.
- Refuerzo de las medidas de seguridad: Se establecen medidas de seguridad más exigentes para proteger los datos personales frente a accesos no autorizados, pérdida o destrucción.

Principios de protección de datos de carácter personal

Principios básicos

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), junto con el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), establecen una serie de principios que rigen el tratamiento de estos datos.

Licitud, lealtad y transparencia:

- Los datos deben ser tratados de forma lícita, leal y transparente.
- La organización debe informar al interesado sobre la finalidad del tratamiento, las consecuencias y los posibles riesgos.

Ejemplo: Una empresa no puede usar la cuenta bancaria de un cliente sin su consentimiento.

Limitación de la finalidad:

- Los datos deben ser tratados para una o varias finalidades específicas, explícitas y legítimas.
- No se pueden tratar posteriormente de forma incompatible con esas finalidades.

Ejemplo: Un centro de salud puede usar datos médicos para un estudio científico, siempre que se garantice la anonimización de los usuarios.

Principios de protección de datos de carácter personal

Principios básicos

Minimización de los datos:

- Los datos deben ser adecuados, pertinentes y limitados a lo necesario para la finalidad del tratamiento.
- No se deben tratar datos innecesarios o redundantes.

Ejemplo: Un servicio de notificaciones por correo electrónico solo necesita la dirección de e-mail del usuario.

Exactitud:

- Los datos deben ser exactos y actualizados.
- El responsable del tratamiento debe tomar medidas razonables para garantizar la exactitud de los datos.

Ejemplo: Una compañía telefónica debe mantener actualizados los datos de sus clientes para evitar errores en el servicio.

Limitación del plazo de conservación:

- Los datos deben ser eliminados o destruidos una vez cumplida la finalidad del tratamiento.
- Se pueden establecer plazos para la revisión o eliminación de los datos.
- Hay excepciones, como la defensa de reclamaciones o fines científicos, históricos o estadísticos.

Ejemplo: La Ley de Autonomía del Paciente establece un plazo de 5 años para la conservación de historiales clínicos.

Reglamento General de Protección de Datos (RGPD)

Introducción

El Reglamento Europeo de Protección de Datos (RGPD), nacido en 2018, responde a la necesidad de regular el uso de los datos personales de los ciudadanos de la Unión Europea. Supone un avance significativo respecto a la normativa anterior, como la Directiva 95/46/CE, endureciendo el control sobre los datos y empoderando a los ciudadanos.

Puntos clave del RGPD:

Transparencia:

- Las organizaciones deben informar claramente a los usuarios sobre la finalidad de la recopilación de datos y demostrar que solo se usan para esos fines.
- Se busca una mayor transparencia en el tratamiento de los datos personales.

Consentimiento:

- Se elimina el "consentimiento tácito". Los usuarios tienen derecho a retirar su consentimiento y a que se elimine su información personal.
- Se fortalece el control del individuo sobre sus datos.

Reglamento General de Protección de Datos (RGPD)

Puntos clave del RGPD:

Seguridad de los datos:

- Cada organización es responsable de la seguridad de los datos que utiliza o almacena.
- Se establecen obligaciones para la detección y comunicación de brechas de seguridad.
- Se exige a las organizaciones ser proactivas en la protección de la información.

Privacidad desde el diseño y por defecto:

- Todo proyecto debe evaluar desde el inicio los riesgos para la privacidad de los datos.
- Se deben implementar medidas para eliminar o mitigar esos riesgos.
- Se busca integrar la protección de datos desde las primeras fases de cualquier proyecto.

Delegado de Protección de Datos:

- Se establece la figura del Data Protection Officer (DPO) para empresas que traten datos a gran escala o administraciones públicas.
- El DPO es responsable de identificar riesgos y buscar soluciones para la protección de datos.

Reglamento General de Protección de Datos (RGPD)

Puntos clave del RGPD:

Protección de datos de menores:

- Se exige el consentimiento parental para procesar datos de menores de 16 años en servicios online.
- Los países miembros pueden modificar la edad de consentimiento, pero no puede ser inferior a 13 años.

Certificaciones:

- Se contemplan certificaciones de cumplimiento de estándares de protección de datos.
- Estas certificaciones pueden ser otorgadas por autoridades de protección de datos, el Comité Europeo o entidades privadas acreditadas.

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

Introducción:

La protección de datos personales en España se configura como un derecho fundamental. La normativa vigente en este ámbito comprende tanto el Reglamento General de Protección de Datos (RGPD) de la Unión Europea como las leyes nacionales. En este análisis, nos centraremos en dos instrumentos clave: el Código Penal y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).

Protección de datos en el Código Penal:

El artículo 197 del Código Penal tipifica como delito el apoderamiento, uso o modificación sin consentimiento de datos personales. Las penas van de uno a cuatro años de prisión y multa de doce a veinticuatro meses.

Conductas tipificadas como delito:

- Apoderamiento de datos personales sin consentimiento.
- Utilización de datos personales sin consentimiento.
- Modificación de datos personales sin consentimiento.
- Acceso no autorizado a sistemas informáticos con datos personales.
- Revelación, difusión o cesión de datos personales obtenidos de forma ilegítima.

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

Protección de datos en el Código Penal:

El artículo 197 del Código Penal tipifica como delito el apoderamiento, uso o modificación sin consentimiento de datos personales. Las penas van de uno a cuatro años de prisión y multa de doce a veinticuatro meses.

Agravantes del delito:

- Si el delito lo comete un responsable del fichero de datos.
- Si los datos revelan información sensible (ideología, religión, salud, etc.).
- Si la víctima es un menor de edad o una persona incapaz.
- Si el delito se comete con fines lucrativos.
- Si el delito se comete dentro de una organización criminal.

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

Protección de datos en la Ley Orgánica 3/2018:

La LOPDGDD desarrolla el marco legal para la protección de datos personales en España, adaptando la normativa nacional al RGPD.

Entre sus puntos clave se encuentran:

- Derechos de los interesados: acceso, rectificación, supresión, limitación del tratamiento, oposición al tratamiento y portabilidad de los datos.
- Obligaciones de los responsables del tratamiento: transparencia, licitud del tratamiento, minimización de datos, exactitud, seguridad y medidas técnicas y organizativas para la protección de los datos.
- Figura del Delegado de Protección de Datos (DPD): obligatorio para empresas que traten datos a gran escala o datos sensibles.

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

Leyes de protección de datos en España: análisis comparativo

Evolución normativa:

- Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD) (1992): Primera ley de protección de datos en España.
- Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) (1999): Sustituye a la LORTAD, adaptándola a la Directiva 95/46/CE del Parlamento Europeo.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD): Implementa el RGPD en España y deroga la LOPD.

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

Leyes de protección de datos en España: análisis comparativo

Principios comunes:

- Tratamiento de datos personales: Debe ser lícito, leal y transparente.
- Calidad de los datos: Deben ser exactos, actualizados y adecuados a su finalidad.
- Información y consentimiento: El interesado debe ser informado sobre el tratamiento de sus datos y debe dar su consentimiento.
- Datos especialmente protegidos: Se establecen medidas especiales para proteger datos sensibles como los de salud.
- Deber de secreto: Los responsables del tratamiento de datos deben mantener la confidencialidad.
- Seguridad de los datos: Se deben implementar medidas técnicas y organizativas para proteger los datos.
- Cesión de datos: La cesión de datos a terceros debe ser lícita y el interesado debe ser informado.

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

Leyes de protección de datos en España: análisis comparativo

Avances en la LOPDGDD:

- Ampliación de los derechos de los interesados: Se incluyen nuevos derechos como el derecho a la portabilidad de los datos, el derecho a la limitación del tratamiento y el derecho a la oposición al tratamiento.
- Mayor transparencia y responsabilidad: Las empresas y organizaciones deben ser más transparentes en el tratamiento de los datos personales y deben rendir cuentas ante las autoridades de control.
- Refuerzo de las medidas de seguridad: Se establecen medidas de seguridad más exigentes para proteger los datos personales frente a accesos no autorizados, pérdida o destrucción.

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

Introducción:

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) establece la obligación para las empresas y organizaciones de identificar y registrar los ficheros con datos de carácter personal que utilizan. Este proceso es fundamental para garantizar la protección de la privacidad de los ciudadanos en la era digital.

¿Qué son los datos de carácter personal?

Cualquier información que pueda identificar a una persona física, como su nombre, dirección, teléfono, número de identificación, datos de salud, etc.

¿Por qué es importante identificar y registrar los ficheros con datos personales?

- Cumplimiento legal: Permite a las organizaciones cumplir con las obligaciones de la LOPDGDD.
- Protección de la privacidad: Minimiza el riesgo de pérdida, robo o uso indebido de datos personales.
- Mejora la transparencia: Permite a los ciudadanos conocer qué datos se están recopilando sobre ellos y cómo se están utilizando.
- Facilita el ejercicio de los derechos ARCO-POL: Permite a los ciudadanos acceder, rectificar, cancelar, oponerse, limitar el tratamiento o portar sus datos personales.

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

Proceso de implantación de la LOPDGDD (FASES)

1.- Identificación de los ficheros:

- Todos los ficheros que contengan datos de carácter personal, incluyendo aquellos en formato electrónico, físico o mixto.

Ejemplos: fichas de clientes, nóminas de empleados, bases de datos de marketing, etc.

2.- Nivel de seguridad:

- Dependiendo del tipo de datos que contenga el fichero, se aplicarán diferentes medidas de seguridad.
- Niveles de seguridad: bajo, medio y alto.

3.- Delegado de Protección de Datos:

- Figura obligatoria para empresas que traten datos a gran escala o datos sensibles.
- Funciones: velar por el cumplimiento de la normativa, gestionar los riesgos y solucionar problemas relacionados con la protección de datos.

4.- Documento de seguridad:

- Describe las medidas de seguridad técnicas y organizativas para proteger los datos.
- Debe ser actualizado regularmente.

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

Proceso de implantación de la LOPDGDD (FASES)

5.- Formación:

- Impartir formación en materia de protección de datos a todos los empleados.
- Formación específica para el Delegado de Protección de Datos.

6.- Información a los interesados:

- Informar a los ciudadanos sobre la existencia de un fichero con sus datos, la finalidad del tratamiento y sus derechos ARCO-POL.

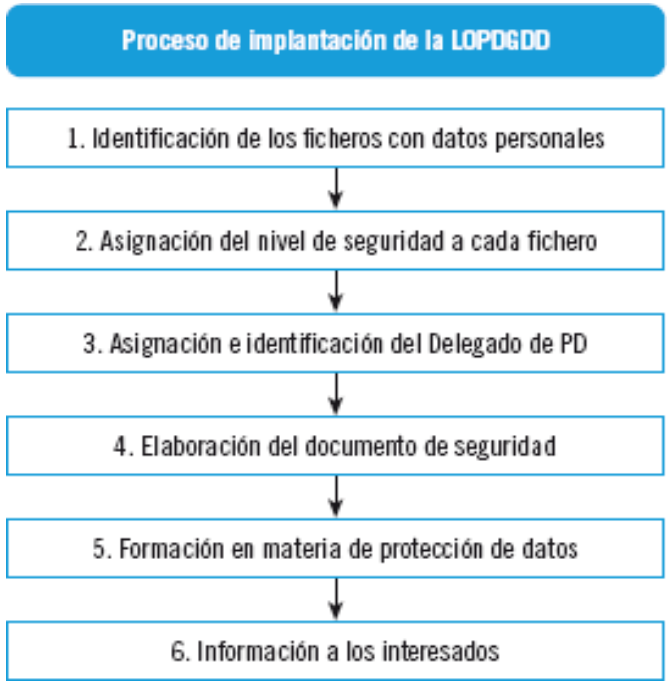
7.- Auditorías:

- Obligatorias para empresas con datos de nivel de protección medio o alto.
- Frecuencia mínima: cada dos años.
- Objetivo: detectar y corregir deficiencias en la protección de datos.

La identificación y registro de los ficheros con datos personales es un proceso fundamental para la protección de la privacidad en el ámbito empresarial. La LOPDGDD establece un marco legal para este proceso, con diferentes fases y requisitos que las organizaciones deben cumplir. La implementación adecuada de la LOPDGDD no solo permite cumplir con la ley, sino que también mejora la transparencia, la seguridad y la confianza de los ciudadanos.

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

Fase	Descripción
1. Identificación de los ficheros	Localizar todos los ficheros que contienen datos personales.
2. Nivel de seguridad	Definir las medidas de seguridad para cada fichero.
3. Delegado de Protección de Datos	Designar un responsable de la protección de datos.
4. Documento de seguridad	Documentar las medidas de seguridad.
5. Formación	Capacitar a los empleados en materia de protección de datos.
6. Información a los interesados	Informar a los ciudadanos sobre sus derechos.
7. Auditorías	Realizar auditorías para verificar el cumplimiento de la normativa.



Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 994/2019 (RGPD y LOPDGDD)

Medidas de seguridad en el RGPD:

El RGPD exige a las empresas y organizaciones que implementen medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales. Estas medidas deben ser proporcionales al riesgo que supone el tratamiento de los datos.

Tipos de medidas de seguridad:

- Seudonimización y cifrado de datos: Convertir los datos en un formato que no permita la identificación directa de las personas.
- Capacidad de garantizar los derechos ARCO-POL: Implementar medidas para que los ciudadanos puedan ejercer sus derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad.
- Capacidad de restaurar la disponibilidad y el acceso a los datos: Contar con planes de recuperación ante desastres y copias de seguridad.
- Verificación, evaluación y valoración de las medidas de seguridad: Realizar auditorías periódicas para evaluar la eficacia de las medidas de seguridad.

Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 994/2019 (RGPD y LOPDGDD)

Medidas de seguridad en el RGPD:

Enfoque de riesgo:

El RGPD introduce un enfoque de riesgo para la evaluación de las medidas de seguridad. Las empresas y organizaciones deben tener en cuenta:

- Los costes de aplicación y la tecnología disponible.
- La naturaleza, alcance, contexto y fines del tratamiento.
- Los riesgos para los derechos y libertades de los usuarios.
- Los riesgos derivados del tratamiento de los datos.

Adhesión a códigos de conducta y mecanismos de regulación:

El RGPD establece la posibilidad de adherirse a códigos de conducta o mecanismos de regulación para cumplir con los estándares de seguridad.

Registro de actividades de tratamiento:

El responsable del tratamiento debe mantener un registro de las actividades de tratamiento que realiza, incluyendo las medidas técnicas y organizativas utilizadas.

Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 994/2019 (RGPD y LOPDGDD)

Medidas de seguridad en el RGPD:

Medidas de seguridad específicas en la LOPDGDD:

La LOPDGDD amplía las medidas de seguridad del RGPD con dos puntos específicos:

- Medidas de seguridad en el sector público: Se establece el cumplimiento del Esquema Nacional de Seguridad (ENS) para las entidades públicas.
- Tratamiento de datos en caso de incidentes de seguridad: Las autoridades competentes pueden tratar datos personales para dar respuesta a un incidente de seguridad, adoptando las medidas de seguridad adecuadas.

Guía para la realización de la auditoría bienal ¿obligatoria? de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Introducción:

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) no establece la obligación de realizar auditorías bienales de forma explícita. Sin embargo, no cumplir con el deber de implantar medidas de seguridad adecuadas para proteger los datos personales puede conllevar sanciones.

La ley Orgánica 15/1999 de Protección de Datos de Carácter Personal sí obligaba a la realización de una auditoría bienal.

¿Por qué realizar una auditoría bienal?

- Detectar y corregir deficiencias en la seguridad de los datos: Las auditorías permiten identificar áreas de mejora y tomar medidas para proteger los datos personales de forma eficaz.
- Demostrar el cumplimiento de la normativa: La realización de auditorías bienales demuestra el compromiso de la organización con la protección de datos y facilita la respuesta ante una inspección de la Agencia Española de Protección de Datos (AEPD).
- Mejorar la confianza de los clientes, empleados y partners: Las empresas que demuestran un buen gobierno en materia de protección de datos generan mayor confianza entre sus stakeholders.

Guía para la realización de la auditoría bienal ¿obligatoria? de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

¿Cuándo realizar la auditoría?

- Recomendación: Cada dos años o cuando se produzcan cambios relevantes en el sistema o en las políticas de seguridad de la empresa.
- Obligación: En caso de modificaciones sustanciales del sistema de información, antes de que transcurran dos años.

Pasos para realizar la auditoría:

- Determinación del alcance:
  - Identificar los ficheros con datos de carácter personal.
  - Definir los tratamientos realizados, los sistemas de tratamiento, los procedimientos de protección de datos, etc.
- Planificación de recursos: Determinar los recursos necesarios: fuentes de información, ubicación de los ficheros, instalaciones, equipos, etc.
- Obtención de datos: Recopilar la información a evaluar mediante diferentes técnicas y herramientas (ver tabla).

Guía para la realización de la auditoría bienal ¿obligatoria? de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Pasos para realizar la auditoría:

- Métodos de obtención de datos:

Método	Descripción
Relación de ficheros	Estructura y contenido de los ficheros con datos personales.
Políticas de seguridad	Información sobre las políticas y procedimientos de seguridad de la organización.
Documento de seguridad y auditorías	Revisión del documento de seguridad y de las auditorías anteriores.
Diseño físico y lógico	Revisión del diseño de los sistemas de información (ubicación, dispositivos, redes, etc.).
Relación de usuarios	Lista de usuarios con sus accesos autorizados y funciones.
Inventario de soportes	Registro de los soportes con datos personales y sus entradas y salidas.
Entrevistas	Entrevistas a usuarios, responsables de seguridad, etc.

Guía para la realización de la auditoría bienal ¿obligatoria? de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

Pasos para realizar la auditoría:

- Evaluación de las pruebas:
  - Comprobar si se cumplen los requisitos de la LOPDGDD y su reglamento de desarrollo.
  - Detectar posibles deficiencias en la seguridad de los datos personales.
- Medidas correctivas:
  - En caso de detectar deficiencias, establecer medidas para recuperar un nivel de seguridad adecuado.
  - Modificar el documento de seguridad incluyendo los cambios y medidas implantadas.

Resumen

Importancia de la protección de datos:

- La protección de datos de carácter personal es un derecho fundamental que permite a las personas controlar el uso de su información personal.
- Esta protección está regulada por una serie de normativas, tanto nacionales como europeas, de obligatorio cumplimiento para las organizaciones.

Marco legislativo en España:

- La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) es la normativa vigente en España.
- La LOPDGDD adapta el Reglamento General de Protección de Datos (RGPD) europeo al contexto español.
- Su objetivo es proteger a las personas físicas en el tratamiento de sus datos y garantizar sus derechos digitales.

Razones para la reforma:

- La evolución de las tecnologías de la información y las nuevas formas de negocio exigían una actualización de la normativa.
- La LOPDGDD busca cubrir los vacíos legales de la LOPD anterior e incluir nuevas obligaciones para las organizaciones.

Resumen

Cumplimiento del RGPD:

- El RGPD es de obligado cumplimiento para todos los estados miembros de la Unión Europea.
- Permite a los estados miembros adaptar la normativa a su marco legislativo, siempre que no contradigan el reglamento.

Medidas de protección de datos:

- Las organizaciones deben establecer medidas de protección de datos de forma proactiva, basadas en un análisis de riesgos.
- El RGPD define los puntos clave para realizar este análisis.

Documento de seguridad:

- Tras la implantación de las medidas de protección, las organizaciones deben elaborar un documento de seguridad.
- Este documento describe las medidas y procedimientos utilizados para proteger los datos.
- Permite justificar la actuación de la organización ante las autoridades y realizar auditorías internas.