APUNTES 04

LEGISLACIÓN Y JURISPRUDENCIA EN MATERIA DE PROTECCIÓN DE DATOS

NORMATIVA DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

A lo largo de esta unidad van a desarrollar competencias sobre la protección de datos y la regulación existente en esta materia, principalmente serán:

1. Identificar regulación existente.
2. Aplicación de los principios relacionados con protección de datos.
3. Requisitos para la aplicación de la privacidad en el diseño.
4. Herramientas de cumplimiento normativo.
5. Análisis de riesgos de las actividades de procesamiento de las organizaciones.
6. Implantación de medidas para la reducción de riesgos identificados en la protección de datos.
7. Conocimiento el rol de delegado de protección de datos en una organización.

En esta unidad se van a desarrollar los siguientes contenidos:

1. Principios de protección de datos.
2. Novedades del RGPD de la Unión Europea.
3. Privacidad por Diseño y por Defecto.
4. Análisis de Impacto en Privacidad (PIA), y medidas de seguridad.
5. Delegado de Protección de Datos (DPO).

1.- PRINCIPIOS DE PROTECCIÓN DE DATOS.

Caso práctico

Durante los últimos meses, una gran empresa de telecomunicaciones en España, ha recibido la mayor multa de la historia en materia de protección de datos.

La dirección de ACME, viendo el antecedente, ha decidido minimizar los riesgos relacionados con la normativa de protección de datos, y hacer un análisis de los datos que trata la compañía, así como de las medidas de seguridad existentes, y de los requisitos de la regulación vigente cuyo cumplimiento evite o minimice posibles sanciones y daños reputacionales por incumplimiento.

Todas estas implicaciones y los procesos asociados se analizarán en los siguientes epígrafes.

- **Protección de datos, Conceptos Básicos.**

Los datos personales son cualquier información relativa a una persona física identificada o identificable.

Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona.

Ejemplos de datos personales:

- ➢ Nombre y apellidos
- ➢ Domicilio
- ➢ Dirección de correo electrónico, del tipo nombre.apellido@empresa.com
- ➢ Número de documento nacional de identidad
- ➢ Datos de localización (como la función de los datos de localización de un teléfono móvil) (*)
- ➢ Dirección de protocolo de internet (IP)
- ➢ Identificador de una cookie (*)
- ➢ Identificador de la publicidad del teléfono
- ➢ Datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona

Ejemplos de datos no considerados personales:

- ➢ Número de registro mercantil,
- ➢ Dirección de correo electrónico tipo info@empresa.com
- ➢ Datos anonimizados.

La Regulación General de Protección de Datos establece además, una categorización de datos especialmente sensibles. Estos datos son:

- ➢ Origen racial
- ➢ Ideología política.
- ➢ Religión o Creencias.
- ➢ Afiliación sindical.
- ➢ Datos relativos a la Salud.
- ➢ Datos relativos a la vida sexual u orientaciones sexuales.
- ➢ Datos genéticos y biométricos.

Por lo general, el tratamiento de estos datos esta prohibido, salvo en los siguientes escenarios:

- ➢ Con el consentimiento explicito del interesado, cuando el individuo consiente su tratamiento.
- ➢ Por obligación legal cuando existen peticiones judiciales.
- ➢ Por interés vital del interesado, por ejemplo en las urgencias de un hospital.
- ➢ Para fundaciones o asociaciones políticas, filosóficas y religiosas o sindicales.
- ➢ Datos manifiestamente públicos como por ejemplo la ideología de un líder político.
- ➢ Formulación / defensa de reclamaciones / tribunales.
- ➢ Interés público en el ámbito de la salud pública, investigación científica, histórica, etc...

- **Legislación vigente.**

El Reglamento General de Protección de Datos (RGPD) es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 24 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018.

La Ley Orgánica de Protección de Datos es la adaptación española del reglamento europeo. Fue aprobada el 5 de diciembre de 2018 como Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). Aunque en esencia es muy similar al RGPD Europeo, incluye artículos adicionales dentro de los epígrafes de Garantía de los Derechos Digitales, tales como el derecho de Desconexión Digital.

- **Principios de protección de datos.**

La protección de datos se basa principios rectores definidos en el artículo 5 de la RGPD, son los siguientes:

- Exactitud: los datos tratados deben ser exactos, y en caso de no serlo, estos deben ser actualizados. Este principio trata de establecer las directrices para mantener los datos actualizados y correctos, o se supriman o modifiquen en caso de que no lo sean.
- Confidencialidad: los responsables y encargados de tratamiento y por lo general, cualquier persona que intervenga en el proceso de gestión de datos, debe mantener el deber de confidencialidad.
- Consentimiento: el tratamiento de la información personal debe basarse en el consentimiento de su propietario y limitado al marco de una finalidad o finalidades comunicadas.
- Licitud, transparencia y lealtad: se deben utilizar los datos de manera legal y lícita, informando al propietario del motivo por el cual se van a tratar los datos y utilizándolos únicamente para los fines comunicados y consentidos por el propietario.
- Finalidad: los datos deben ser tratados para llevar a cabo finalidades específicas y no para cualquiera. En línea con los principios anteriores, estas finalidades deben ser identificadas, comunicadas y aprobadas por el propietario de los datos en caso necesario.
- Minimización de datos: utilizar la cantidad de datos mínima posible para cumplir con una finalidad.
- Limitación del plazo de conservación: los datos deben ser tratados y/o almacenados solo durante el tiempo por el tiempo necesario para garantizar la finalidad del tratamiento consentida.
- Seguridad: establecer las medidas técnicas y organizativas que permitan mantener su confidencialidad, integridad y disponibilidad.
- Responsabilidad activa: demostrar diligencia debida en el tratamiento de datos personales, para proteger y garantizar derechos y libertades de las personas físicas en base a un análisis de riesgos.

1.1.- REGULACIÓN GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA.

- **Disposiciones Generales de la Regulación General de Protección de Datos.**

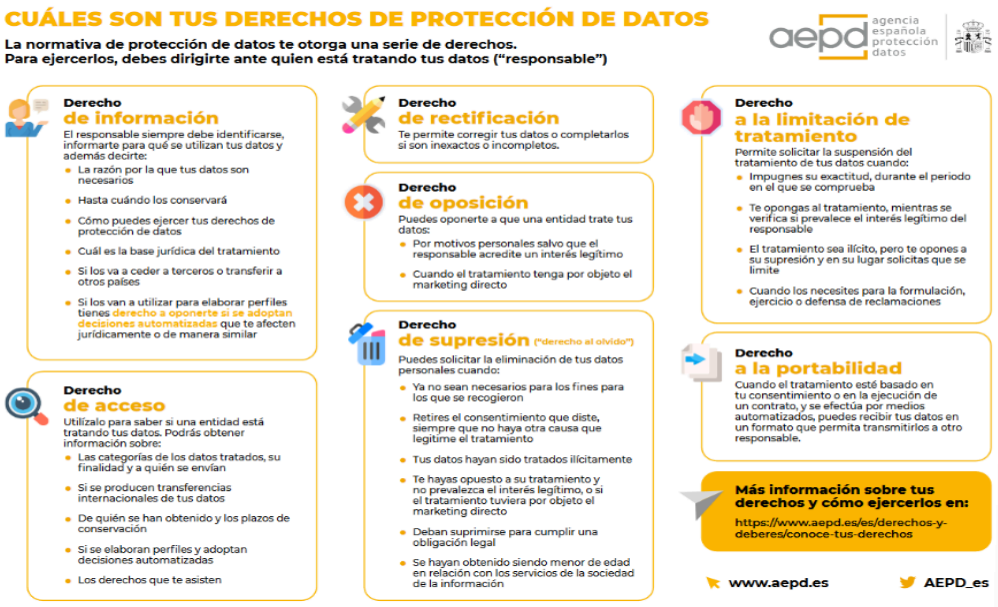
El objetivo de la Regulación General de Protección de Datos (RGPD) es la protección de las personas físicas con respecto a sus datos personales y a la libre circulación de los mismos.
La RGPD aplica a todo tratamiento de datos personales ya sean automatizados o no, en el territorio europeo o bien en otros territorios si es que se están tratando datos de ciudadanos europeos.
El tratamiento de datos consiste en la ejecución de cualquier operación sobre datos, de manera manual o automatizada, como la recogida, registro, modificación, consulta, uso, comunicación o difusión, conservación, supresión o destrucción.
La regulación establece que los datos de carácter personal solo se podrán tratar bajo los siguientes escenarios:

- ➢ El propietario de la información da su consentimiento para el tratamiento de sus datos con uno o varios fines específicos.
- ➢ El tratamiento se ejecuta en base a una obligación legal.
- ➢ El tratamiento es necesario para la ejecución de un contrato firmado entre propietario y responsable de los datos.
- ➢ El tratamiento es necesario para proteger la vida del interesado o de otra persona física.
- ➢ El tratamiento es necesario para alguna actividad de interés público.
- ➢ el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

Obtención del consentimiento para el tratamiento de datos:
Los responsables de tratamiento de datos estarán obligadas a obtener el consentimiento de los propietarios de la información para gestionar sus datos, y deben informar de qué modo los procesan y para que finalidad. Los responsables de tratamiento deben demostrar que han obtenido el consentimiento para la gestión de la información. La solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo para los propietarios de la información. Éstos podrán retirar su consentimiento en cualquier momento, siendo la dificultad de este proceso similar a la de otorgarlo.

- **Derechos del interesado en la Regulación General de Protección de Datos**

La siguiente infografía muestra los derechos de los propietarios de los datos con respecto a su información:



- **Figuras en el tratamiento de información**

A continuación se presentan las diferentes figuras que intervienen en el proceso de tratamiento de datos:

Propietario de los datos / Interesado: Individuo sobre el que versan los datos que se están tratando, impactado por la limitación de sus derechos y libertades en caso de que no sea respetada la regulación, y sus datos no sean tratados de manera diligente o existan fugas. Ejemplo: Juan Flores

Responsable del tratamiento de datos o controlador: Persona física o Jurídica que maneja la información del interesado a través de uno o varios medios con uno o varios fines determinados. Ejemplo: Juan Flores firmando una hipoteca con Caja Rural de Teruel.

Encargado de tratamiento o procesador: Persona física o Jurídica que trata los datos personales en nombre del responsable de tratamiento, siempre bajo el marco de un contrato. Ejemplo: Gestoría Tecnotramit realiza la gestión del proceso de registro de la propiedad en nombre de Caja Rural de Teruel, siendo Juan Flores el que ha contratado este servicio.

- **Códigos de conducta y certificación**

Las asociaciones sectoriales o cualquier organización que agrupe entidades de sectores homogéneos, podrán elaborar códigos de conducta a los que adscribirse que describan el modo en el que están cumpliendo el presente reglamento. Estos códigos de conducta incluirán elementos como:

1. El tratamiento leal y transparente de la información.
2. Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos.
3. El modo de recogida de datos personales.
4. La seudonimización de datos personales.
5. La información proporcionada al público y a los interesados.
6. El ejercicio de los derechos de los interesados.
7. La información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño.
8. Las medidas y procedimientos para garantizar la seguridad del tratamiento de la información.
9. La notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;
10. La transferencia de datos personales a terceros países u organizaciones internacionales.
11. Los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento.

Para saber más: los códigos de conducta son notificados a la AEPD que debe validarlos y aprobarlos, siendo estos publicados y consultables en la web de la AEPD. Códigos de conducta en AEPD

- **Registro de actividades de tratamiento**

Uno de los requisitos del RGPD es el mantenimiento de un registro de actividades de tratamiento de la información que almacena la organización. Este registro, debe ser puesto en manos de un auditor de la AEPD en caso de que así lo requiera como información mínima que evidencie el cumplimiento del reglamento.
El RGPD y la LOPDGDD exigen que el registro contenga como mínimo la siguiente información:

- ➢ El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
- ➢ Las finalidades de tratamiento.
- ➢ Una descripción de las categorías de interesados y de las categorías de datos personales.
- ➢ Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- ➢ Las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional.
- ➢ Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- ➢ Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

El contenido del Registro de Actividades de Tratamiento constituye una información mínima exigible, éste, podría formar parte de los catálogos de procesos que ya existiesen en la entidad, incluyendo toda la información que el responsable considere necesaria para proteger los derechos y libertades de las personas físicas y poder demostrar cumplimiento atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los posibles orígenes de los riesgos que dicho tratamiento pudiera suponer para los interesados.
El registro podría incluir aspectos que faciliten la aplicación efectiva de la responsabilidad proactiva como: análisis de riesgos para los derechos y libertades realizados, la descripción sistemática del tratamiento, los sistemas de información sobre los que se apoya, la descripción de la identidad de los encargados del tratamiento, las garantías previstas para llevar a cabo transferencias internacionales de datos, información de contacto de las personas o los departamentos de la organización que se encuentran implicados en las operaciones de tratamiento, etc.
En el caso de dar acceso al contenido del Registro de Actividades de Tratamiento, y con relación a una posible descripción general de las medidas técnicas y organizativas de seguridad, debe evitarse desvelar cualquier información que pudiera ser perjudicial para la organización, para los tratamientos de datos personales y que comprometiese la propia seguridad.

- **Medidas de seguridad en el tratamiento de datos.**

El artículo 32 del RGPD impone a los responsables de un tratamiento la obligación de definir e implantar las medidas de seguridad adecuadas para garantizar el nivel de seguridad apropiado en función del estado de la técnica, los costes de aplicación y, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos asociados al mismo.
A diferencia de la LOPD existente previamente en España, en la cual se definían explícitamente las medidas de seguridad a implementar, con el RGPD, el responsable debe evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. En dicha evaluación del riesgo deben tenerse en cuenta los riesgos que atenten contra los derechos y libertades de los interesados.
Con el objetivo de seleccionar las medidas para gestionar el riesgo para los derechos y libertades, pueden utilizarse estándares de seguridad ya existentes en el mercado como la norma ISO 27000 o cualquier otra, como las que se pueden consultar en el apartado de normas nacionales e internacionales en la unidad 5. Por su parte, las Administraciones Públicas deberán utilizar el Esquema Nacional de Seguridad para seleccionar las medidas que deban implantarse para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos.
Con carácter general el estándar utilizado implicará:

- ➢ La realización de un inventario de activos partiendo de la descripción sistemática del tratamiento.
- ➢ La identificación de los riesgos, para los derechos y libertades de los interesados, asociados a los activos que consten en el inventario de activos.
- ➢ La evaluación del riesgo para los derechos y libertades de los interesados.
- ➢ La gestión de riesgos para los derechos y libertades de los interesados a lo largo del ciclo de vida del tratamiento.

RGPD ni LOPD-GDD establecen medidas de seguridad obligatorias, no obstante, las medidas a adoptar deben estar basadas en un análisis de riesgos de cada tratamiento de datos que vayáis a realizar, porque no todas las actividades de tratamiento implican los mismos riesgos y tienen el potencial de causar los mismos daños y perjuicios a los titulares de los datos. A continuación se proponen una serie de medidas de seguridad a modo de ejemplo, que permiten aumentar el nivel de seguridad en el tratamiento de la información:
Medidas de seguridad técnicas propuestas:

- ➢ Instalación de antivirus, sistemas Endpoint Detection and Response (EDR), sistemas Data Rights Management(DRM), sistemas Data Leakage Prevention (DLP).
- ➢ Sistemas de seguridad de red como firewalls.
- ➢ Protección del correo electrónico, como protocolos contra el phishing.
- ➢ Gestión de actualizaciones para solucionar vulnerabilidades.
- ➢ Cifrado de ficheros, discos duros y memorias USB.
- ➢ Sistemas de copias de seguridad copias de seguridad.
- ➢ Sistemas de cifrado, ofuscación, aleatorización de datos.

- ➢ Software de borrado seguro y destrucción de archivos segura.
- ➢ Sistemas de gestión centralizada de controles de acceso y contraseñas.
- ➢ Gestión de usuarios, roles y privilegios basados en una política de privilegios mínimos y zero trust.

Medidas de seguridad organizativas propuestas:

- ➢ Planes de seguridad de la información y de tratamiento de datos.
- ➢ Definición de un cuerpo normativo de seguridad que incluya políticas y procedimientos.
- ➢ Protocolos para el control de documentos y registros.
- ➢ Política para el manejo y tratamiento de información confidencial.
- ➢ Inclusión de cláusula de seguridad y confidencialidad para proveedores.
- ➢ Política de controles de acceso.
- ➢ Designación de un Responsable de Seguridad de la Información.
- ➢ Designación de un Delegado de Protección de Datos.
- ➢ Realización periódica de auditorías de seguridad y de protección de datos.

- **Las brechas de Seguridad**

Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.
Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.
El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.
El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo. El plazo para notificar a la autoridad de control es de 72 horas desde que la organización tiene constancia de la brecha.
Si además entraña un alto riesgo deberá comunicarse sin dilación indebida a los afectados a través del medio que se suela utilizar para comunicarse con ellos, con un lenguaje claro y sencillo. Esto permitirá que los afectados puedan reaccionar cuanto antes y tomar las medidas oportunas, porque en dicha comunicación se les deberá explicar claramente lo sucedido y las medidas recomendadas para que puedan minimizar o eliminar las consecuencias negativas que pueda tener la brecha sobre ellos.
En el ámbito privado, los responsables del tratamiento afectados por una brecha de datos personales deberán notificar a la AEPD:

- ➢ Cuando su único establecimiento esté localizado en España.
- ➢ Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
- ➢ Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.
- ➢ Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

La notificación a la autoridad de control de una brecha que afecta a datos personales forma parte de la responsabilidad proactiva establecida en el RGPD, y el hecho de notificarla no implica necesariamente la apertura de un procedimiento administrativo. De hecho, notificar en tiempo y forma es una evidencia de la diligencia de la organización, mientas que no cumplir con esa obligación si está tipificado como infracción.
Sin embargo, en aquellos casos en los que el responsable considere que no existieran riesgos para los derechos y libertades de las personas físicas el responsable tiene la obligación de documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas, dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el artículo 33 del RGPD.

Para saber más: la agencia española de protección de datos ha publicado una guía para la notificación de brechas de datos personales. Guía para la notificación de brechas de datos

- **Transferencias internacionales de datos.**

Una transferencia internacional de datos se produce cuando los datos personales que son tratados por un responsable o un encargado del tratamiento en el Espacio Económico Europeo (países de la Unión Europea, Islandia, Liechtenstein y Noruega) son enviados a un tercer país u organización internacional, fuera de dicho territorio.
El objetivo de la regulación es garantizar, que una vez que los datos salgan del territorio europeo, se sigan dando los elementos necesarios para garantizar el derecho fundamental a la protección de datos personales de las personas físicas cuyos datos personales son objeto de tratamiento.

Una transferencia internacional de datos fuera del Espacio Económico Europeo (EEE), es decir, los países de la Unión Europea e Islandia, Liechtenstein y Noruega, solo puede llevarse a cabo cuando el tercer país u organización internacional tiene un nivel adecuado o se dan otras garantías adecuadas en materia de protección de datos personales.
Por lo general, todas las transferencias internacionales, deben ser notificadas y aprobadas por la agencia española de protección de datos, no obstante, los responsables y encargados del tratamiento podrán realizar transferencias internacionales de datos sin necesidad de autorización siempre que el tratamiento de datos observe lo dispuesto en el RGPD y en los siguientes supuestos:

Transferencias basadas en una decisión de adecuación:
Cuando las entidades receptoras de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional que hayan sido declarados de nivel de protección adecuado por la Comisión Europea. Hasta la fecha los países y territorios están declarados como adecuados son: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Japón, Reino Unido y República de Corea.

Mediante la aportación de garantías adecuadas:
A falta de decisión de adecuación si se ofrecen garantías adecuadas, que podrán ser aportadas a través de:

- ➢ Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
- ➢ Normas corporativas vinculantes.
- ➢ Cláusulas tipo de protección de datos adoptadas por la Comisión.
- ➢ Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión.
- ➢ Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.
- ➢ Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.

Excepciones para situaciones específicas

A falta de decisión de adecuación y de garantías adecuadas únicamente se podrán realizar si se cumple alguna de las condiciones siguientes:

- La persona interesada haya dado explícitamente su consentimiento, después de haber sido informada de los posibles riesgos.
- La transferencia sea necesaria para la ejecución de un contrato entre la persona interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona interesada.
- La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica.
- La transferencia sea necesaria por razones importantes de interés público.
- La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones.
- La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento.
- La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Una transferencia internacional, necesitará aprobación explicita de la Agencia Española de Protección de Datos, cuando el ofrecimiento de garantías adecuadas se realice mediante:

- Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o sub encargado, que no hayan sido adoptadas por la Comisión Europea o por la Agencia Española de Protección de Datos y aprobadas por la Comisión Europea.
- Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para las personas interesadas

- **La agencia española de protección de datos.**

Logo de la agencia española de protección de datos
Agencia española de protección de datos . Agencia española de protección de datos (CC BY-NC-SA)
La Agencia Española de Protección de Datos (AEPD) está encargada de velar por el cumplimiento de la normativa de protección de datos y controlar su aplicación, a nivel estatal, no obstante, para los ámbitos geográficos de Andalucía, Cataluña y País Vasco, existen agencias autonómicas de protección de datos con potestad de actuación en ámbito local y con funciones similares a las de la AEPD.

Las funciones principales que llevan a cabo estas agencias, son las siguientes:

- Controlar la aplicación del Reglamento General de Protección de Datos y el resto de la normativa de protección de datos, así como proceder a que se aplique.
- Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento.
- Asesorar al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los
derechos y libertades de las personas físicas con respecto al tratamiento.
- Promover la sensibilización de las personas responsables y encargadas del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento.
- Facilitar información a cualquier interesado en relación con el ejercicio de sus derechos.
- Tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación, e investigar, en la medida oportuna, el motivo de la reclamación.
- Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento.
- Alentar la elaboración de códigos de conducta, dictaminar y aprobar los códigos de conducta presentados, que den suficientes garantías con arreglo al cumplimiento del RGPD.
- Fomentar creación de mecanismos de certificación de protección de datos y de sellos y marcas de protección datos.
- Llevar registros internos de las infracciones del presente Reglamento.
- Llevar a cabo investigaciones en forma de auditorías de protección de datos.
- Sancionar a toda persona responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir o hayan infringido lo dispuesto en la normativa de protección de datos.
- Tutelar los derechos y garantías de las personas abonadas y usuarias en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente (spam).
- Recibir las notificaciones de las eventuales quiebras de seguridad que se produzcan en los sistemas de los proveedores de servicios de comunicaciones electrónicas y que puedan afectar a datos personales.
- Cooperación con diversos organismos internacionales y con los órganos de la Unión Europea en materia de protección de datos.

- **Sanciones por incumplimiento de la legislación en protección de datos.**

En este epígrafe se detallará el régimen sancionador por incumplimiento de protección de datos.
En este sentido, se debe diferenciar la cuantía de las multas según lo definido en el RGPD que las que están especificadas en la nueva LOPD-GDD. El reglamento europeo es más abstracto en cuanto a la especificidad de los incumplimientos y la graduación de su cuantía, mientras que la LOPD-GDD lo especifica de manera más pormenorizada.
La cuantía de las sanciones por protección de datos que tanto el RGPD como la LOPDGDD imponen, se valora según los derechos personales afectados, los beneficios obtenidos, la posible reincidencia, la intencionalidad y cualquier circunstancia que sea relevante para determinar la culpabilidad.
Así, las sanciones que establece el RGPD son:

- Para infracciones graves: multa de hasta 10 millones de euros (o el 2% de la facturación anual, aplicando la cuantía que resulte más alta).
- Para infracciones muy graves: multa de hasta 20 millones de euros (o el 4% de la facturación anual, aplicando la cuantía que resulte más alta).

En caso de la LOPD-GDD española, las infracciones por protección de datos se dividen en leves, graves y muy graves.

Las sanciones para infracciones leves suponen una multa de hasta 40.000 €. Son consideradas infracciones leves:

- Incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información que exigen los artículos 13 y 14 del RGPD.
- Pedir un pago al interesado para poder acceder a la información que exigen los artículos 13 y 14 del RGPD o para atender las solicitudes de ejercicio de derechos contempladas en los artículos 15 a 22 del citado Reglamento.
- No atender las solicitudes de los ejercicios de los derechos que se establecen en los artículos 15 a 22 del RGPD.
- No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o portabilidad de los datos cuando no se requiera la identificación del afectado.
- No cumplir con la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento que exige el artículo 19 del RGPD.
- No cumplir con la obligación de informar al afectado de los destinatarios a los que se haya comunicado la rectificación, supresión o limitación del tratamiento.
- No cumplir con la supresión de datos referidos a una persona fallecida cuando así lo exige el artículo 3 de la LOPDGDD.
- Incumplimiento de las obligaciones de los responsables y encargados del tratamiento.
- Que el registro de actividades de tratamiento no contenga toda la información que exige el artículo 30 del RGPD.
- Informar tarde o de forma incompleta a la AEPD de una brecha de seguridad.

- ➢ Dar información inexacta a la AEPD en los supuestos en los que el responsable del tratamiento debe elevar una consulta previa, de acuerdo al artículo 36 del RGPD.
- ➢ No publicar los datos de contacto del delegado de protección de datos o comunicarlos a la AEPD.
- ➢ Incumplimiento de las obligaciones de los organismos de certificación de informar a la AEPD de la expedición, renovación o retirada de una certificación.
- ➢ Incumplimiento de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a la AEPD de las medidas que resulten oportunas en caso de infracción del código.

Las sanciones para incumplimientos Graves suponen una multa de 40.001 € a 300.000 €. Se pueden considerar como graves:

- ➢ Tratar datos de menores de edad sin recabar su consentimiento, cuando tenga edad para ello, o de sus padres o tutores.
- ➢ No acreditar esfuerzos razonables para verificar la validez del consentimiento del menor o de sus padres o tutores.
- ➢ No atender de forma reiterada u obstaculizar la solicitud de los derechos de acceso, rectificación, supresión, limitación del tratamiento o portabilidad de los datos en los tratamientos en los que no se requiere la identificación del afectado.
- ➢ No adoptar las medidas técnicas y organizativas apropiadas para aplicar la protección de datos desde el diseño.
- ➢ No adoptar las medidas técnicas y organizativas que garanticen el tratamiento de los datos personales necesarios para cada uno de los fines específicos del tratamiento.
- ➢ No adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos.
- ➢ Brechas de seguridad ocurridas por no haber adoptado las medidas adecuadas de seguridad.
- ➢ No designar un representante del responsable o encargado del tratamiento no establecido en territorio de la UE, de acuerdo al artículo 27 del RGPD.
- ➢ No atender las solicitudes de las agencias de protección de datos.
- ➢ Contratar un encargado del tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas necesarias, de acuerdo al Capítulo IV del RGPD.
- ➢ Encargar el tratamiento de datos a un tercero sin el debido contrato.
- ➢ Contratación por parte del encargado del tratamiento de otros encargados sin contar con la autorización del responsable.
- ➢ Infracción de lo dispuesto en el artículo 28.10 del RGPD respeto a la determinación de los fines y los medios de tratamiento por parte del encargado.
- ➢ No disponer del registro de actividades.
- ➢ No cooperar con la AEPD u otras autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de la LOPDGDD.
- ➢ El tratamiento de datos personales sin cumplir con lo recogido en el artículo 28 de la LOPDGDD.
- ➢ Incumplir el deber de informar de las violaciones de seguridad por parte del encargado del tratamiento al responsable.
- ➢ No informar de las violaciones de seguridad a la AEPD, según el artículo 33 del RGPD.
- ➢ No informar al afectado de una violación de seguridad de datos personales.
- ➢ Llevar a cabo el tratamiento de datos sin realizar una evaluación de impacto cuando esta es exigible.
- ➢ Tratar datos personales sin haber realizado consulta previa a la AEPD cuando esta sea obligatoria.
- ➢ No designar a un delegado de protección de datos cuando sea obligatorio.
- ➢ No permitir que el delegado de protección de datos pueda cumplir con sus funciones.
- ➢ Utilizar sellos o certificaciones en materia de protección de datos que no hayan sido otorgados por una entidad de certificación acreditada o estén expirados.
- ➢ Incumplimientos de los organismos de certificación.

Las sanciones muy graves implican una multa de entre 300.001 € a 20.000.000 €, son consideradas infracciones muy graves, las siguientes:

- ➢ Tratamiento de datos personales que vulneren las garantías y principios establecidos en el artículo 5 del RGPD.
- ➢ Trata datos personales sin la legitimación establecida en el artículo 6 del RGPD.
- ➢ No cumplir con los requisitos exigidos en el artículo 7 del RGPD para la validez del consentimiento.
- ➢ Utilizar los datos personales recogidos con una finalidad diferente para la que se dio el consentimiento.
- ➢ Trata datos personales de las categorías recogidas en el artículo 9 del RGPD sin que concurra alguna de las circunstancias previstas de dicho artículo y del artículo 9 de la LOPDGDD.
- ➢ Tratar datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos del artículo 10 del RGPD y el artículo 10 de la LOPDGDD.

1.2.- PRIVACIDAD POR DISEÑO Y POR DEFECTO.

La privacidad desde el diseño y por defecto se trata de establecer un proceso a través del cual se consideren los riesgos en privacidad de un proceso o un sistema de tal manera que durante su construcción se apliquen las medidas técnicas y organizativas necesarias para garantizar la privacidad de la información de carácter personal antes de su tratamiento.
Este paradigma implica un cambio en la manera en el que se desarrollan estos procesos, en los cuales, típicamente se realizaba un diseño funcional para posteriormente, se agregaran las medidas de seguridad, una vez desarrollado.
Este proceso esta regulado en el RGPD en el artículo 25:
"Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."
El concepto de privacidad desde el diseño y por defecto se basa en siete principios fundamentales:

1. Proactivo, no reactivo; preventivo, no correctivo: La privacidad por diseño, (por sus siglas en ingles "PbD") implica anticiparse a los eventos que afecten a la privacidad antes de que sucedan. Cualquier sistema, proceso o infraestructura que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños.

2. La privacidad como configuración predeterminada: La configuración por defecto deberá quedar establecida desde el diseño a aquel nivel que resulte lo más respetuoso posible en términos de privacidad. En el caso de que el sujeto no tome ninguna acción de configuración, su privacidad debe estar garantizada y mantenerse intacta, pues está integrada en el sistema y configurada por defecto. Como ejemplo práctico de este principio se pueden determinar los siguientes elementos:

2.1. Fijar criterios de recogida limitados a la finalidad que persigue el tratamiento.

2.2. Limitar el uso de los datos personales a la(s) finalidades para la(s) que fueron recogidos y asegurarse de que existe una base legitimadora del tratamiento.

2.3. Restringir los accesos a los datos personales a las partes implicadas en los tratamientos atendiendo al principio de “need to know” y según la función que realicen mediante la creación de perfiles de acceso diferenciados.

2.4. Definir plazos estrictos de conservación y establecer mecanismos operativos que garanticen su cumplimiento.

2.5. Crear barreras tecnológicas y procedimentales que impidan la vinculación de no autorizada de fuentes de datos independientes.

3. Privacidad incorporada en la fase de diseño: La privacidad debe formar parte de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No debe consistir en una serie de medidas de seguridad que se añade a algo preexistente , sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña.

4. Funcionalidad total, pensamiento “todos ganan”: Tradicionalmente se ha entendido se gana en privacidad a costa de perder otras funcionalidades, presentando dicotomías como privacidad vs usabilidad, privacidad vs funcionalidad. El objetivo ha de ser buscar el balance óptimo en una búsqueda tipo “gana-gana”, con una mentalidad abierta a nuevas soluciones para conseguir sistemas plenamente funcionales, eficaces y eficientes también a nivel de privacidad.

5. Privacidad en todo el ciclo de vida: La privacidad nace en el diseño, debe existir a lo largo de todo el ciclo de vida completo de los datos. Mientras que la seguridad de la información impone confidencialidad, integridad, disponibilidad y resiliencia de los sistemas, la privacidad implica la desvinculación, la transparencia y la capacidad de intervención y control en el tratamiento por parte del sujeto del dato.

6. Visibilidad y transparencia: El proceso de privacidad por defecto en una organización, debe ser demostrable, verificando que el tratamiento es acorde a la información dada. El principio de transparencia en el tratamiento de datos implica la capacidad de demostrar la diligencia y la responsabilidad proactiva ante la Autoridad de Control (AEPD) y como medida de confianza ante los sujetos cuyos datos son tratados, principalmente, los clientes de una organización.

7. Respeto por la privacidad de los usuarios: se debe mantener un enfoque centrado en el usuario respetando los intereses legítimos del tratamiento de la información. El objetivo final del proceso es garantizar la privacidad de los propietarios de la información. El usuario debe tener un papel activo en la gestión de sus propios datos y su inacción no debe suponer un nivel inferior en la privacidad de sus datos. La configuración de privacidad por defecto debe ofrecer el máximo nivel de protección.

Tradicionalmente la protección de los procesos y sistemas de información se ha basado en el despliegue de medidas de seguridad cuya finalidad se basaba en la cobertura de las principales propiedades de seguridad de la información: confidencialidad, integridad y disponibilidad. La minimización de riesgos en privacidad implica una serie de objetivos nuevos distintos pero complementarios a los de la seguridad, que cumplen con los principios establecidos en la RGDP, estos son:
Desvinculación: Este objetivo de privacidad minimiza el riesgo de un uso no autorizado de los datos personales y la creación de perfiles mediante la interconexión de información perteneciente a diferentes conjuntos de datos, estableciendo garantías sobre los principios de limitación de la finalidad, la minimización de datos y la limitación del plazo de conservación.
Transparencia: Este objetivo de la privacidad pretende que el contexto del tratamiento quede perfectamente delimitado y que la información sobre las finalidades y las condiciones legales, técnicas y organizativas aplicables esté disponible antes, durante

y después del tratamiento a todas las partes implicadas, tanto para el responsable como para el sujeto cuyos datos son tratados, minimizando así los riesgos que pueden afectar a los principios de lealtad y transparencia.
Control: Este objetivo se basa en la implementación de procedimientos para el ejercicio de derechos en materia de protección de datos, la presentación de reclamaciones o la revocación de los consentimientos prestados por parte de los interesados, así como mecanismos para garantizar, por parte del responsable, la evaluación del cumplimiento y la efectividad de las obligaciones que le son fijadas por la normativa, lo que contribuye a respetar los principios de exactitud y responsabilidad proactiva marcados por el RGPD.

Para que la privacidad quede integrada como parte del diseño del sistema debe seguirse una aproximación sistemática y metodológica, trasladando los requisitos de la fase de análisis a su desarrollo en la fase de implementación. Para ello, existen ciertas estrategias de manejo de información que dan soporte en el cumplimiento de los objetivos recién mencionados. Las estrategias de privacidad se materializan, a más bajo nivel, en patrones de diseño de soluciones reutilizables de privacidad que son aplicables para resolver problemas comunes y repetibles de privacidad que se presentan de forma reiterada en el desarrollo de productos y sistemas. Se han identificado ocho estrategias de diseño de la privacidad que se conocen como 'minimizar', 'ocultar', 'separar', 'abstraer', 'informar', 'controlar', 'cumplir' y 'demostrar'.

Minimizar: El objetivo que persigue esta estrategia es recoger y tratar la mínima cantidad de datos posible, de modo que, evitando el procesamiento de datos que no sean necesarios para las finalidades perseguidas en el tratamiento, se limitan los posibles impactos en la privacidad.

Ocultar: Esta estrategia se centra en limitar la exposición de los datos, estableciendo las medidas necesarias para garantizar la protección de los objetivos de confidencialidad y desvinculación.

Separar: El objetivo que persigue esta estrategia es evitar, que durante el procesamiento de diferentes datos personales pertenecientes a un mismo individuo en una misma entidad, y utilizados en tratamientos independientes, se pueda llegar a realizar un perfilado completo del sujeto. Para ello, es necesario mantener contextos de tratamiento independientes que dificulten la correlación de grupos de datos que deberían estar desligados.

Abstraer: La idea que subyace bajo el uso de esta estrategia es limitar al máximo el detalle de los datos personales que son tratados. A diferencia de la estrategia 'minimizar' que realiza una selección previa de los datos recogidos, esta estrategia se centra en el grado de detalle con el que los datos son tratados y en su agregación.

Informar: Este objetivo persigue que los interesados estén plenamente informados del procesamiento de sus datos en tiempo y forma. Siempre que se realice un tratamiento, los sujetos cuyos datos son tratados deberían conocer qué información es la que se procesa, con qué propósito y a qué terceras partes es comunicada.

Controlar: Se trata de proporcionar a los interesados control en relación a la recogida, tratamiento, usos y comunicaciones realizadas sobre sus datos personales mediante la implementación de mecanismos que permitan el ejercicio de los derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación al tratamiento así como la prestación y retirada del consentimiento o la modificación de las opciones de privacidad en aplicaciones y servicios.

Cumplir: Esta estrategia asegura que los tratamientos de datos personales son compatibles y respetan los requisitos y obligaciones legales impuestos por la normativa. Esta estrategia se basa en la definición de un marco de privacidad y una estructura de gobernanza que incluya una política de protección de datos apoyada desde la alta dirección, así como los roles y responsabilidades que velen por su cumplimiento.

Demostrar: El objetivo de esta estrategia es que el responsable del tratamiento pueda demostrar, tanto a los interesados como a las autoridades de supervisión, el cumplimiento de la política de protección de datos que esté aplicando, así como del resto de requisitos y obligaciones legales impuestos por el Reglamento.

Por último, como parte de las herramientas que pueden dar soporte en privacidad, se encuentran las tecnologías de privacidad mejorada o PETS (Privacy Enhancing Technologies) que se utilizan para implementar los patrones de diseño de la privacidad con una tecnología concreta. Las Privacy Enhancing Technologies o PETs son un conjunto de soluciones TIC que reducen los riesgos que afectan a la privacidad, implementando las estrategias y patrones definidos anteriormente. A continuación se proponen dos agrupaciones de PETs de tipología de herramientas utilizadas para la mejora en la privacidad:
Protección de la privacidad:

- Herramientas para seudonimizar: Permiten efectuar transacciones sin solicitar información personal.
- Productos y servicios para anonimizar: Proporcionan el acceso a servicios sin requerir la identificación del sujeto de datos.
- Herramientas de cifrado: Protegen los documentos y transacciones de ser visualizados por terceras partes.
- Filtros y bloqueadores: Evitan emails y contenido web no deseado
- Supresores de seguimiento: Eliminan las trazas electrónicas de la actividad digital del usuario.

Gestión de la privacidad:

- Herramientas de información: Crean y verifican las políticas de privacidad.
- Herramientas administrativas: Gestionan la identidad y los permisos del usuario

1.3.- ANÁLISIS DE IMPACTO EN PRIVACIDAD (PIA), Y MEDIDAS DE SEGURIDAD.

El RGPD habla del análisis de impacto en privacidad como una obligación regulada en el artículo 35 de la norma, en su transposición a la legislación española se habla de este proceso como Evaluación de Impacto en Protección de Datos.

Una Evaluación de Impacto en Protección de Datos (EIPD) es una actividad realizada para identificar los riesgos a los que están expuestos los datos personales que mantiene una organización en función de las actividades de tratamiento que se realizan, además, permite definir medidas de minimización de riesgos hasta reducirlos a un nivel aceptable para la organización. Este proceso debe ser ejecutado previo al tratamiento de la información en los casos en los que exista un riesgo alto para los derechos y libertades de los propietarios de la información.

A diferencia de una evaluación de riesgos en seguridad de la información que se centra en aspectos de riesgo para la organización, la evaluación de impacto de protección de dato, busca determinar el nivel de riesgo que un determinado tratamiento supone para los derechos y libertades de las personas, identificando amenazas y probabilidades y evaluando el impacto que esto tendría sobre la vida de los propietarios de la información.

El reglamento establece cuando es necesario llevar a cabo un análisis de impacto en privacidad, siendo obligatorio en las siguientes situaciones:

- Alto riesgo: Cuando el tratamiento vaya a entrañar un alto riesgo debido al uso de nuevas tecnologías, o por su naturaleza, alcance, contexto o fines.
- Evaluación sistemática: cuando se lleva a cabo una evaluación exhaustiva y sistemática de aspectos personales y se soporta en un proceso automatizado, como la elaboración de perfiles, y que además supone la toma de decisiones que afecten a los interesados.
- Tratamiento a gran escala de datos especialmente protegidos: Si se efectúa un tratamiento a gran escala de las categorías especialmente sensibles de datos del artículo 9, apartado 1 del RGPD, de los datos personales relativos a condenas e infracciones penales o de datos relativos a menores.
- Cuando se vayan a llevar a cabo actividades de observación sistemática a gran escala, en función a:
  - El número de interesados afectados, bien en términos absolutos, bien como proporción de una determinada población.
  - El volumen de datos y la variedad de datos tratados.
  - La duración o permanencia de la actividad de tratamiento.
  - La extensión geográfica de la actividad de tratamiento.

Para saber más: la agencia española de protección de datos ha desarrollado una guía para la evaluación de impacto y el análisis de riesgo en privacidad. Es consultable en el siguiente enlace: Guía para la evaluación de impacto y análisis de riesgos en privacidad

La evaluación de impacto de la protección de datos (EIPD) debe ser realizada en base a una metodología que tenga en cuenta los requerimientos establecidos por el RGPD. Los análisis de impacto deben incluir al menos lo siguientes contenidos:

- Una descripción sistemática de la actividad de tratamiento previstas.
- Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.
- Una evaluación de los riesgos.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Asimismo, también deben tenerse en cuenta los siguientes aspectos:

- Con respecto al contexto, se deben tener en cuenta dos elementos:
  - El ciclo de vida de los datos, elaborando una descripción del mismo y del flujo de datos durante el tratamiento, identificando los datos tratados, intervinientes, terceros, sistemas implicados y cualquier elemento relevante que participe en la actividad de tratamiento.
  - Analizar la idoneidad, necesidad y proporcionalidad del tratamiento, en base a:
    - Idoneidad: determinar si el tratamiento es adecuado para el fin que persigue. El tratamiento da respuesta a determinadas carencias, demandas, exigencias, obligaciones u oportunidades objetivas y puede conseguir los objetivos propuestos con la eficacia suficiente.
    - Necesidad: determinar si la finalidad perseguida no puede alcanzarse de otro modo menos lesivo o invasivo, es decir, no existe un tratamiento alternativo que sea igualmente eficaz para el logro de la finalidad perseguida.
    - Proporcionalidad: La gravedad del riesgo para los derechos y libertades del tratamiento, y su intromisión en la privacidad, ha de ser adecuada al objetivo perseguido y proporcionada a la urgencia y gravedad de esta.
- Asimismo, también debe llevarse a cabo un proceso de gestión de riesgos, que incluya:
  - Amenazas y riesgos: Identificación de las amenazas y riesgos potenciales a los que están expuestos las actividades de tratamiento.
  - Evaluación los riesgos: Evaluación de la probabilidad y el impacto de que se materialicen los riesgos a los que está expuesta la organización.
  - Tratamiento los riesgos: Respuesta ante los riesgos identificados con el objetivo de minimizar la probabilidad y el impacto de que estos se materialicen hasta un nivel de riesgo aceptable que permita garantizar los derechos y libertades de las personas físicas.

- Por último, se debe emitir un informe con las conclusiones y el plan de acción que debe recoger:
- El resultado obtenido junto con el plan de acción que incluya las medidas de control a implantar para gestionar los riesgos identificados y poder garantizar los derechos y libertades de las personas físicas.
- Un proceso de supervisión y revisión de la implantación o puesta en marcha del nuevo tratamiento con el objetivo de garantizar la implantación de las medidas de control descritas en el Plan de acción.

El proceso de evaluación de impacto en privacidad, debe ser entendido como un proceso continuo, de tal manera que los datos del análisis realizado se revisen ante cualquier cambio relevante en las actividades de tratamiento.

1.4.- DELEGADO DE PROTECCIÓN DE DATOS (DPO).

El Delegado de Protección de Datos es la figura dentro de la organización que se encarga de velar por la protección de la información.

El RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

O bien cuando la organización pertenezca a los siguientes sectores:

- Educación.
- Servicios de comunicaciones.
- Entidades de crédito.
- Aseguradoras.
- Energía.
- Publicidad e investigación.
- Sanidad.

El DPD ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. Aunque no debe tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.

La designación del DPD y sus datos de contacto deben hacerse públicos por los responsables y encargados y deberán ser comunicados a las autoridades de supervisión competentes.

La posición del DPD en las organizaciones tiene que cumplir los requisitos establecidos, entre los que se encuentran:

- Total autonomía en el ejercicio de sus funciones.
- Necesidad de que se relacione con el nivel superior de la dirección.
- Obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.
- Conocimiento en derecho en la rama de protección de datos.
- Sus datos deben ser notificados a la AEPD.
- Puede ser interno o un servicio externalizado.

Sus funciones son:

- Informar y asesorar de las obligaciones en materia de protección de datos (similar al compliance officer).
- Supervisar el cumplimiento legal en protección de datos, al menos en la asignación de responsabilidades, concienciación y formación y la ejecución de auditorías.
- Proponer y supervisar la ejecución de Evaluaciones de Impacto de Protección de Datos.
- Punto de contacto para las Agencias de Protección de Datos.

Respuestas
Autoevaluación I: c)
Autoevaluación II: b)
TEST I: 1 c), 2 c), 3 b), 4 c), 5 b), 6 a), 7 c), 8 d), 9 b), 10 c)
TEST II; 1 d), 2 a), 3 c), 4 b), 5 a), 6 b), 7 a), 8 a), 9 a), 10 b)

Autoevaluación I

Un cliente insatisfecho nos llama porque quiere darse de baja de nuestro servicio de telecomunicaciones. Además, no quiere que la empresa ACME tenga más sus datos. ¿Qué derecho relacionado de protección de datos tendría que solicitar?

a. Portabilidad
b. Oposición.
c. Supresión

Autoevaluación II

Para atender a los clientes que llaman la atención al cliente. ACME ha contratado un servicio de call center en Valladolid. Ellos son los encargados de dar respuesta a las solicitudes de los clientes. ¿Qué rol tiene el call center con respecto a los datos de los clientes?

a) Responsable de tratamiento.
b) Encargado de Tratamiento.
c) Propietario de la Información

TEST I

1.¿Cuál de los siguientes NO es un dato de carácter personal?
a. 73579525H
b. 80.20.14.52
c. ******45C
d. Calle príncipe de Vergara, 32, 5D.

2.¿Cuál de los siguientes países se considera tiene un nivel de seguridad adecuado para una transferencia internacional de datos?
a. Marruecos.
b. Chile.
c. Argentina.
d. Australia.

3.Un usuario quiere que una empresa borre todos los datos que tiene sobre él, ¿Qué derecho solicitará?
a. Derecho de Acceso.
b. Derecho de supresión.
c. Derecho a la limitación de tratamiento.
d. Derecho a la portabilidad.

4.¿Cuál de los siguientes es un dato sensible?
a. 73579525H
b. 643 093 485.
c. Musulmán.
d. Juan Pérez.

5.¿En qué casos un encargado de tratamiento no tiene que notificar una brecha de seguridad a la AEPD?
a. Cuando los datos filtrados no incluyen contraseñas.
b. Cuando los datos filtrados se encuentran anonimizados.
c. Cuando los datos filtrados no son sensibles.
d. Cuando solo se ha filtrado la mitad de los datos.

6.¿Cuál de los siguientes NO es un principio de protección de datos?
a. Conservación de datos.
b. Confidencialidad de los datos.
c. Seguridad de los datos.
d. Responsabilidad activa.

7.¿Cuál de las siguientes empresas tiene que tener obligatoriamente un DPO?
a. Una empresa de automoción.
b. Una empresa de transportes.
c. Una empresa de servicios de comunicaciones.
d. Una cadena de supermercados.

8.¿Cuál de los siguientes es un dato de carácter personal?
a. Una dirección de correo departamental de empresa.
b. El número de teléfono atención al cliente.
c. Un CIF de una empresa.
d. Una dirección de correo de un empleado de la empresa.

9. El único compromiso legal que tienen las empresas es la LOPD y la RGPD. ¿Verdadero o falso?
a. Verdadero
b. Falso

10. ¿Cuál de los siguientes NO es un dato sensible?
a. Origen racial.
b. Afiliación política.
c. Tarjeta de crédito.
d. Salud.

TEST II

1. ¿Cuál de los siguientes es un principio de protección de datos?
    a. Consentimiento.
    b. Tratamiento de datos.
    c. Eliminación de datos.
    d. Conservación de los datos.
2. Un análisis de impacto en privacidad será obligatorio cuando:
    a. Cuando se utilice una tecnología novedosa para tratar los datos.
    b. Se trate al menos un dato identificativo de los clientes.
    c. Cuando la organización subcontrate un servicio.
    d. Cuando se traten datos de empleados.
3. El tratamiento de datos sensibles estará siempre prohibido salvo...
    a. sea cedido a terceras empresas.
    b. el encargado de tratamiento este interesado.
    c. que el interesado consienta explícitamente su tratamiento.
    d. sea necesario para el proceso de negocio de la empresa.
4. El tratamiento de datos biométricos está prohibido salvo que sea necesario para el control de acceso de los empleados. ¿Verdadero o falso?
    a. Verdadero
    b. Falso
5. La Ley Orgánica de Protección de Datos se aprobó en 2018 y es la adaptación española de la Regulación General de Protección de Datos Europea. ¿Verdadero o falso?
    a. Verdadero
    b. Falso
6. ACME subcontrata los servicios de atención al cliente en un tercero. ¿Qué figura ejerce este tercero ante los datos?
    a. Propietario de información.
    b. encargado de tratamiento.
    c. Responsable de tratamiento.
    d. Interesado.
7. La facturación del servicio, es una de las finalidades de tratamiento de ACME. ¿Verdadero o falso?
    a. Verdadero
    b. Falso
8. Un cliente de ACME que este ejerciendo un derecho de acceso. ¿Qué figura ejerce ante los datos?
    a. Interesado.
    b. encargado de tratamiento.
    c. Delegado de información.
    d. Responsable de tratamiento.
9. La RGPD aplica al tratamiento de datos de ciudadanos europeos alojados en servidores en Estados Unidos. ¿Verdadero o falso?
    a. Verdadero
    b. Falso
10. La Agencia Española de Protección de Datos es la única autoridad competente en materia de protección de datos en España. ¿Verdadero o falso?
    a. Verdadero
    b. Falso

Caso práctico

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.

ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.

ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.

Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.

La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.

Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.

Dada su cartera de clientes, ACME es responsable de la información de su cartera de 300.000 clientes, de los cuales maneja diversos datos como pueden ser, datos identificativos, de residencia, bancarios, de trafico de llamadas, etc... con diferentes sensibilidades.

Existen dos regulaciones cuyo objetivo es la protección de los datos personales de los individuales, la Regulación General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPD- GDD).

Teniendo en cuenta la compañía descrita en el escenario anterior, da respuesta a las siguientes preguntas:

Apartado 1: Principios de protección de datos.

Enumera 10 datos de carácter personal que trate ACME en la prestación de sus servicios.

Datos de carácter personal que trata ACME:
Nombre y apellidos
Dirección de residencia del cliente
Número de teléfono
Dirección de correo electrónico
Número de identificación (DNI / NIE)
Datos bancarios
Datos de localización
Datos de facturación
Dirección IP
Historial de llamadas realizadas

¿Alguno de los datos enumerados es sensible?

Algunos de los datos anteriormente enumerados son de carácter sensible, como los datos bancarios o los datos de localización, debido a su naturaleza y el potencial impacto en la privacidad de los individuos si se divulgan o se utilizan de manera indebida. Estos requerirán de protección adicional debido a ser datos con mayor sensibilidad que el resto.

Apartado 2: Regulación General de Protección de Datos.

¿Bajo qué escenarios se podría legitimar ACME en el tratamiento de datos de sus clientes?

La empresa ACME puede legitimar el tratamiento de datos de sus clientes bajo varios escenarios, de acuerdo con el Reglamento General de Protección de Datos (RGPD).
1. ACME puede tratar los datos personales si obtiene el consentimiento explícito de los clientes para fines específicos. Este consentimiento debe ser libre, específico e informado.
2. El tratamiento de esos datos es legítimo si es necesario para la ejecución de un contrato en el que el cliente es parte, como por ejemplo para poder proporcionarles la prestación de servicios de telecomunicaciones.
3. La empresa puede tratar datos personales para cumplir con las obligaciones legales, como la facturación y el pago de impuestos.
4. Puede tratar datos personales si tiene un interés legítimo que no prevalezca sobre los derechos y libertades del cliente, como los datos de navegación en su sitio web.
5. En situaciones de emergencia, ACME puede tratar datos personales para proteger los intereses vitales (vida) del cliente o de otra persona física.
6. La empresa puede tratar los datos de forma legítima cuando es necesario para el cumplimiento de alguna actividad de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (ACME).

Indica al menos un ejemplo de cada figura de tratamiento de datos.

- Responsable del tratamiento de datos o controlador: es la entidad que decide los fines y los medios de tratamiento de los datos personales de sus clientes.
La empresa ACME S.A., decide recopilar y almacenar datos de contacto de sus clientes para gestionar sus cuentas y proporcionar soporte técnico.
La organización determina cómo se utilizarán los datos de tráfico de llamadas para analizar patrones de uso y mejorar sus servicios.
- Encargado de tratamiento o procesador: en la entidad que trata los datos personales por cuenta del responsable del tratamiento.
Una empresa de call center contratada por ACME que se dedica a gestionar las llamadas de atención al cliente y dar soporte.
Una empresa de servicios de facturación contratada por ACME para procesar los pagos de los clientes.
- Propietario de los datos / Interesado: la persona física titular de los datos personales.
Un cliente de la empresa que proporciona sus datos personales para obtener los servicios de telecomunicaciones.
Un empleado de ACME que comparte sus datos para la gestión de su contrato laboral.

Indica tres actividades de tratamiento que estén llevadas a cabo por ACME.

1. Gestión de contratos y facturación,
ACME recopila y almacena datos personales de facturación y datos bancarios para emitir y gestionar correctamente las facturas mensuales de los clientes. Al suscribirse a los servicios de la organización, los clientes facilitan sus datos bancarios y de contacto, que son almacenados y utilizados para enviar las facturas mensuales.
2. Atención al cliente,
La empresa utiliza datos personales, como datos de contacto e historial de llamadas para resolver consultas y problemas técnicos de los clientes. Cuando un cliente contacta con el servicio de atención al cliente de ACME para resolver un problema técnico, la empresa accede al historial de llamadas y datos del cliente para ofrecer una solución adecuada.
3. Marketing y promociones,

ACME trata datos personales, como datos de contacto y preferencias del cliente, para enviar ofertas promocionales y campañas de marketing. Se envían correos electrónicos a los clientes con ofertas especiales basadas en sus preferencias y patrones de uso de los servicios.

Apartado 3: Análisis de impacto en privacidad.
Realiza un análisis de impacto de las tres actividades de tratamiento descritas en el apartado anterior.
Gestión de facturación,
Riesgos: la recopilación y almacenamiento de datos bancarios y de facturación conlleva riesgos significativos, como los posibles accesos no autorizados, la pérdida de datos y el uso indebido de la información financiera. Estos riesgos pueden resultar en fraudes financieros y pérdida de confianza por parte de los clientes.
Medidas de mitigación: para minimizar estos riesgos, ACME debe implementar medidas de seguridad robustas, como la encriptación de datos, controles de acceso estrictos (doble autenticación) y auditorías regulares. Además, es crucial que la empresa cumpla con las normativas de protección de datos, con el RGPD y que informe a los clientes sobre cómo utilizar y proteger sus datos personales.
Atención al cliente,
Riesgos: el tratamiento de datos de contacto e historial de llamadas puede exponer información sensible sobre las comunicaciones y preferencias de los clientes. Existe el riesgo de que estos datos sean accedidos por personas no autorizadas o utilizados de manera indebida lo que podría comprometer la privacidad de los clientes.
Medidas de mitigación: debe asegurar que sólo el personal autorizado tenga acceso a estos datos y que se utilicen únicamente para los fines previstos. La implementación de políticas de privacidad claras, la capacitación del personal empleado en protección de datos y el uso de tecnologías de seguridad, como la encriptación y el monitoreo continuo, son esenciales para proteger la privacidad de los clientes.
Marketing y promociones,
Riesgos: el uso de datos personales para marketing puede ser intrusivo si no se gestiona adecuadamente. Los clientes pueden sentirse invadidos si reciben comunicaciones no deseadas o si sus datos se utilizan sin su consentimiento. Además, existe el riesgo de que los datos sean compartidos con terceros sin el conocimiento o consentimiento de los clientes
Medidas de mitigación: me debe obtener el consentimiento explícito de los clientes antes de utilizar sus datos para fines de marketing. Es importante que las políticas de privacidad sean transparentes y que los clientes tengan la opción de optar por no recibir comunicaciones promocionales. Además, la empresa debe garantizar que los datos se almacenen de forma segura y que no se compartan con terceros sin el consentimiento del cliente.