

**INFORME DE AUDITORÍA DE
CUMPLIMIENTO DE LA NORMATIVA
DE PROTECCIÓN DE DATOS
PERSONALES DE:
CENTRE DE DESENVOLUPAMENT
RURAL LA SAFOR**

Fecha: 23/09/2025

1. ALCANCE DE LA AUDITORÍA

1.1. TIPO DE AUDITORÍA

Ámbito de la auditoría	Cumplimiento de la normativa de protección de datos personales
Tipo de auditoría	Auditoría periódica
Fecha de la auditoría	23/09/2025

1.2. ENTIDAD AUDITADA

Razón social	CENTRE DE DESENVOLUPAMENT RURAL LA SAFOR
NIF/NIE	G97197073
Domicilio	Carrer Major, 18 - 46716 - Rafelcofer - VALENCIA
Teléfono	960 434 840
Correo electrónico	cdr@cdrlasafor.org

1.3. ENTIDAD AUDITORA

Razón social	CONSTRUYENDO FUTURO INFORMATICO S.L.	
NIF/NIE	B34222950	
Domicilio	AVDA. MADRID, 10 - 34004 - PALENCIA	
Auditor	OSCAR HERRANZ MEGINO	Firma:

1.4. OBJETIVOS DE LA AUDITORÍA

El objetivo de este informe de auditoría es determinar si la entidad objeto de la auditoría cumple con los requisitos establecidos por la normativa de protección de datos personales.

En concreto, se ha verificado el cumplimiento de:

- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (en adelante, RGPD).
- La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDPGDD).
- Las medidas de seguridad implantadas para proteger los datos personales de la organización.
- Los procedimientos e instrucciones vigentes en materia de seguridad de datos personales.

1.5. METODOLOGÍA DEL TRABAJO DE AUDITORÍA

Las etapas de ejecución de la auditoría son las siguientes:

- 1) Reunión inicial.
- 2) La recogida de evidencias, que se realiza mediante cuatro estrategias:
 - a) Análisis de documentación aportada por la entidad auditada.
 - b) Comprobación de registros.
 - c) Inspección visual de los sistemas de la información y entorno físico.
 - d) Entrevistas con el personal, tanto Responsable/s de Seguridad como diversos usuarios.
- 3) Documentación de los resultados.
- 4) Reunión final para comentario de las evidencias con el Coordinador de protección de datos o el Delegado de Protección de Datos de la entidad auditada.
- 5) Elaboración del informe de auditoría.

1.6. EJECUCIÓN DEL TRABAJO DE AUDITORÍA

Se han analizado los siguientes ámbitos del cumplimiento de la normativa de protección de datos personales:

- Cumplimiento de los requisitos legales y documentales establecidos por la normativa de protección de datos personales para que el responsable pueda tratar datos personales.
- Cumplimiento de los principios establecidos por la normativa de protección de datos personales.
- Cumplimiento legal en la recogida, almacenamiento, utilización, comunicación y destrucción de los datos personales de los interesados.
- Implantación y eficacia de las medidas de seguridad de la organización para la protección de los datos personales.

1.7. TRATAMIENTOS PROPIOS AUDITADOS

Han sido objeto de auditoría los siguientes tratamientos de datos personales:

Tratamiento	Finalidad	Impacto
ATENCIÓN A LOS DERECHOS DE LAS PERSONAS	Gestionar y atender las solicitudes de los interesados en el ejercicio de los derechos establecidos en la normativa de protección de datos.	Bajo
GESTIÓN DE ACTIVIDADES SOCIOCULTURALES Y FORMATIVAS	Gestionar la participación en las actividades socioculturales y formativas gestionadas por la entidad, en su caso, gestionar la publicación de las imágenes tomadas durante la participación en las actividades en las RRSS de la entidad y	Alto

Tratamiento	Finalidad	Impacto
	memorias de justificación del Ministerio y de la Generalitat Valencia.	
GESTIÓN DE ASOCIADOS	Gestión fiscal, contable y administrativa de asociados, así como el envío de comunicaciones promocionales.	Bajo
GESTIÓN DE PERSONAL Y VOLUNTARIADO	Gestión de personal y voluntariado; formación; prevención de riesgos laborales y vigilancia de la salud; elaboración de nóminas, seguros sociales y cotizaciones.	Medio
GESTIÓN DE POTENCIALES ASOCIADOS Y CONTACTOS	Gestión de potenciales asociados que se han interesado sobre nuestros productos y/o servicios, así como otros contactos comerciales. Envío de comunicaciones promocionales, inclusive por vía electrónica.	Bajo
GESTIÓN DE PROGRAMAS DE DESARROLLO RURAL	Proyectos bajo los que se articulan los procedimientos, actuaciones y medidas que pretenden impulsar el Desarrollo Rural, a través de las Directrices Estratégicas Comunitarias, asumido por cada Estado a través de los Planes Estratégicos Nacionales y desarrollado por las CCAA mediante los Programas de Desarrollo Rural.	Alto
GESTIÓN DE PROVEEDORES	Gestión fiscal, contable y administrativa de proveedores así como los datos de contacto profesionales.	Bajo

Tratamiento	Finalidad	Impacto
GESTIÓN DE REGISTRO DE JORNADA LABORAL	Gestión de registro de jornada del personal laboral.	Medio
GESTIÓN DEL CANAL DE DENUNCIAS INTERNO	Gestión del canal de denuncias interno y de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, con la finalidad de informar al responsable de los actos o conductas, acontecidos en la entidad o causados por terceros que contraten con ella, y que pudieran ser contrarios a la normativa general o sectorial que le sea aplicable.	No está definido
GESTIÓN DEL PROTOCOLO PARA LA PREVENCIÓN DEL ACOSO SEXUAL O POR RAZÓN DE SEXO	Gestión del protocolo para la prevención del acoso sexual o por razón de sexo; regulación del procedimiento, gestión de la denuncia, recogida de datos personales y entrevistas con las partes afectadas.	Alto
NOTIFICACIÓN DE BRECHAS DE SEGURIDAD	Gestión y evaluación de las brechas de seguridad, redacción de informes y notificación a la Autoridad de Control y los interesados, en su caso.	Bajo
PROGRAMA DE ATENCIÓN URGENTE	Proyecto de desarrollo rural cuyos beneficiarios estén considerados como sujetos de atención social prioritaria o sean interesados en situación de especial vulnerabilidad.	Alto

Tratamiento	Finalidad	Impacto
SELECCIÓN DE PERSONAL	Gestión los Curriculum Vitae recibidos y realizar los procesos de selección de personal, entrevistas y demás trámites necesarios para la búsqueda del mejor candidato posible a un puesto de trabajo determinado.	Bajo

1.8. TRATAMIENTOS DE TERCEROS AUDITADOS

Han sido objeto de auditoría los siguientes tratamientos de terceros de datos personales:

Tratamiento	Finalidad	Impacto
GESTIÓN DE PROGRAMAS EXTERNOS	Programas de desarrollo encargados por otros CDR o por la CONFEDERACIÓN DE CENTROS DE DESARROLLO RURAL.	Alto

1.9. CENTROS DE TRATAMIENTO DE DATOS AUDITADOS

Se ha auditado los siguientes centros donde se tratan los datos personales:

Sede	Domicilio
Espai CDR la Safor	Carrer Major, 7 - 46716 - Rafelcofer - VALENCIA
Principal	CL. SANT MARC, 10 - 46722 - Beniarjo - VALENCIA
Sede administrativa	Carrer Major 18 - 46716 - Rafelcofer - VALENCIA

1.10. LIMITACIONES EN LA EJECUCIÓN DEL TRABAJO

No han existido limitaciones para la ejecución del trabajo de auditoría.

2. ENTREVISTAS REALIZADAS Y DOCUMENTACIÓN REVISADA

Para realizar la auditoría, se han realizado las entrevistas y revisado la documentación que a continuación se indica:

2.1. ENTREVISTAS REALIZADAS

Fecha	Nombre y apellidos	Cargo	Departamento
23/09/2025	Joaquim Escrihuela Cholvi		Técnico Informático

2.2. DOCUMENTACIÓN REVISADA

Fecha	Documento/s	Observaciones
23/09/2025	Documentación contenida en la plataforma de gestión de protección de datos (Dashboard) y documentación facilitada por el cliente.	

3. ANÁLISIS DEL CUMPLIMIENTO LEGAL DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Se ha analizado el cumplimiento de los requisitos legales de la normativa de protección de datos personales de los tratamientos objeto de la auditoría, en los siguientes ámbitos:

- REGISTRO DE ACTIVIDADES DE TRATAMIENTO
- INFORMACIÓN A LOS INTERESADOS
- PRINCIPIOS Y LICITUD DEL TRATAMIENTO
- VIDEOVIGILANCIA
- CATEGORÍAS ESPECIALES DE DATOS PERSONALES
- DATOS RELATIVOS A CONDENAS E INFRACCIONES PENALES Y ADMINISTRATIVAS
- CONSENTIMIENTO DEL INTERESADO
- CONSENTIMIENTO DE LOS MENORES DE EDAD
- TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES
- ENCARGADOS DEL TRATAMIENTO
- DERECHOS DE LOS INTERESADOS
- SEGURIDAD DEL TRATAMIENTO
- PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO
- NOTIFICACIÓN DE LAS VIOLACIONES DE LA SEGURIDAD
- DELEGADO DE PROTECCIÓN DE DATOS
- EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS
- CORRESPONSABLES DEL TRATAMIENTO
- GARANTÍA DE LOS DERECHOS DIGITALES

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Referencia legal:

Artículo 30 del RGPD. Registro de las actividades de tratamiento.

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

- a) 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;*
- b) los fines del tratamiento;*
- c) una descripción de las categorías de interesados y de las categorías de datos personales;*
- d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;*
- e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;*
- f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;*
- g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.*

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

- a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;*
- b) las categorías de tratamientos efectuados por cuenta de cada responsable;*
- c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;*
- d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.*

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31 de la LOPDPGDD. Registro de las actividades de tratamiento.

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Inspección visual, Entrevistas con responsables, Entrevistas con usuarios.

Evidencias del auditor:

- Se ha comprobado que la entidad dispone de un registro de actividades de tratamiento.
- Se ha comprobado que el registro de actividades de tratamiento recoge 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.

- Se ha comprobado que el registro de actividades de tratamiento recoge todos los fines del tratamiento.
- Se ha comprobado que el registro de actividades de tratamiento recoge una descripción de las categorías de interesados y de las categorías de datos personales que se tratan.
- Se ha comprobado que el registro de actividades de tratamiento recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- Se ha comprobado que el registro de actividades de tratamiento recoge las transferencias de datos personales a un tercer país o a una organización internacional, incluida la identificación de dicho tercer país u organización internacional.
- Se ha comprobado que el registro de actividades de tratamiento incluye todos los plazos previstos para la supresión de las categorías de datos.
- Se ha comprobado que el registro de actividades de tratamiento incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos.
- Se ha comprobado que el registro de actividades de tratamiento recoge, de modo veraz y en detalle, todos los tratamientos de datos que realiza la entidad.
- Se ha comprobado que el registro de actividades de tratamiento incluye todos los tratamientos de datos personales que realiza la entidad.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

Se ha introducido un nuevo Tratamiento:

Tratamiento de los datos de las partes implicadas en el Canal de denuncias interno

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

INFORMACIÓN A LOS INTERESADOS

Referencia legal:

Artículo 12 del RGPD. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

Artículo 13 del RGPD. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

- a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;*
- b) los datos de contacto del delegado de protección de datos, en su caso;*
- c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;*
- d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;*
- e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;*
- f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.*

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

- a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 11 de la LOPDPGDD. Transparencia e información al afectado.

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.

b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su

derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

- a) Las categorías de datos objeto de tratamiento.*
- b) Las fuentes de las que procedieran los datos.*

Estrategias de verificación:

Análisis de documentación, Inspección visual.

Evidencias del auditor:

- Se comprueba que la información relativa al tratamiento se facilita en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.
- Se ha comprobado que la información básica contiene la identidad del responsable del tratamiento y de su representante, en su caso.
- Se ha comprobado que la información básica contiene la finalidad del tratamiento.
- Se ha comprobado que la información básica contiene la posibilidad de ejercer los derechos.
- Se ha comprobado que la información básica contiene la circunstancia de que los datos son tratados para la elaboración de perfiles.
- Se comprueba que en la información básica se indica una dirección electrónica u otro medio que permite acceder de forma sencilla e inmediata a la restante información.
- Se comprueba que en la información completa se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante.
- Se comprueba que en la información completa se facilitan los datos de contacto del delegado de protección de datos.
- Se comprueba que se facilita a los interesados toda la información relativa al tratamiento de datos personales.

- Se comprueba que en la información completa se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Se comprueba que en la información completa se facilita la información pertinente sobre el interés legítimo.
- Se comprueba que en la información completa se informa sobre los destinatarios o las categorías de destinatarios.
- Se ha comprobado que en la información completa se informa de la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o la referencia a las garantías adecuadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
- Se comprueba que en la información completa se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo.
- Se comprueba que en la información completa se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad.
- Se comprueba que en la información completa se informa de la existencia del derecho a retirarlo en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
- Se comprueba que en la información completa se informa del derecho a presentar una reclamación ante una autoridad de control.
- Se comprueba que en la información completa se facilita la información pertinente sobre si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato.
- Se comprueba que la información completa indica si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos.
- Se comprueba que en la información completa se facilita, en su caso, información sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles, así como sobre la lógica aplicada, la importancia y consecuencias previstas de dicho tratamiento para el interesado.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

PRINCIPIOS Y LICITUD DEL TRATAMIENTO

Referencia legal:

Artículo 5 del RGPD. Principios relativos al tratamiento.

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante periodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6 del RGPD. Licitud del tratamiento.

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Entrevistas con responsables, Entrevistas con usuarios.

Evidencias del auditor:

- Se ha comprobado que el responsable del tratamiento ha designado un Coordinador Protección de Datos o un Delegado de Protección de Datos.
- Se ha comprobado que se recogen los datos personales con fines determinados, explícitos y legítimos.
- Se ha comprobado que los datos personales se utilizan solo y exclusivamente para las finalidades informadas a los interesados.
- Se ha comprobado que para ejecutar un contrato o prestar los servicios, se solicitan sólo los datos necesarios.

- Se ha comprobado que las cláusulas informativas incluyen la base jurídica utilizada para el tratamiento de los datos personales.
- Se comprueba que la base jurídica indicada en los tratamientos es coherente con la finalidad de dichos tratamientos.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

VIDEOVIGILANCIA

Referencia legal:

Artículo 22 de la LOPDPGDD. Tratamientos con fines de videovigilancia.

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos

competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 89 de la LOPDPGDD. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Estrategias de verificación:

Análisis de documentación, Inspección visual.

Evidencias del auditor:

No hay evidencias.

Deficiencias encontradas:

- Se ha observado que no se está informando adecuadamente del sistema de videovigilancia a los interesados.

Propuesta de medidas correctoras o complementarias:

- Colocar carteles informativos en un lugar visible que contengan, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos y cómo obtener la información completa del tratamiento.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

CATEGORÍAS ESPECIALES DE DATOS PERSONALES

Referencia legal:

Artículo 9 del RGPD. Tratamiento de categorías especiales de datos personales.

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o

social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 9 de la LOPDPGDD. Categorías especiales de datos.

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Entrevistas con responsables.

Evidencias del auditor:

- Se ha comprobado que solo se tratan categorías especiales de datos cuando existen normas que exceptúan la prohibición general de tratamiento.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

DATOS RELATIVOS A CONDENAS E INFRACCIONES PENALES Y ADMINISTRATIVAS

Referencia legal:

Artículo 10 del RGPD. Tratamiento de datos personales relativos a condenas e infracciones penales.

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 10 de la LOPDPGDD. Tratamiento de datos de naturaleza penal.

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Artículo 27 de la LOPDPGDD. Tratamiento de datos relativos a infracciones y sanciones administrativas.

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Estrategias de verificación:

Análisis de documentación, Revisión de registros.

Evidencias del auditor:

No hay evidencias.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

CONSENTIMIENTO DEL INTERESADO

Referencia legal:

Artículo 7 del RGPD. Condiciones para el consentimiento.

- 1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.*
- 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, 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. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.*
- 3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.*
- 4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.*

Artículo 6 de la LOPDPGDD. Tratamiento basado en el consentimiento del afectado.

- 1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.*
- 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.*
- 3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.*

Estrategias de verificación:

Análisis de documentación, Revisión de registros.

Evidencias del auditor:

- Se comprueba que se solicita el consentimiento de forma clara e independiente de los demás asuntos.
- Se ha comprobado que antes de recoger el consentimiento de los interesados, se les está informando correctamente de la finalidad o finalidades para las que están otorgando dicho consentimiento.
- Se ha comprobado que cuando se solicita el consentimiento a los interesados, se hace de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
- Se comprueba que se ofrecen medios para retirar el consentimiento en cualquier momento.
- Se comprueba que se permite al interesado retirar el consentimiento con la misma facilidad que se recaba.
- Se comprueba que el consentimiento se otorga de forma libre por el interesado.
- Se comprueba que no se supedita la ejecución de un contrato al consentimiento para el tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.
- Se comprueba que existen registros que permitan demostrar que el responsable ha obtenido el consentimiento de los interesados para el tratamiento de los datos personales.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

CONSENTIMIENTO DE LOS MENORES DE EDAD

Referencia legal:

Artículo 8 del RGPD. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 7 de la LOPDPGDD. Consentimiento de los menores de edad.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Estrategias de verificación:

Revisión de registros.

Evidencias del auditor:

- Se ha comprobado que el responsable verifica que el consentimiento fue dado por el titular de la patria potestad o tutela sobre el niño.
- Se comprueba que en el caso de los menores, se recaba el consentimiento de menores de 14 años al titular de la patria potestad o tutela sobre el niño.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

Referencia legal:

Artículo 44 del RGPD. Principio general de las transferencias.

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45 del RGPD. Transferencias basadas en una decisión de adecuación.

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46 del RGPD. Transferencias mediante garantías adecuadas.

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

- a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
- b) normas corporativas vinculantes de conformidad con el artículo 47;
- c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;
- d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;
- e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o
- f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

- a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o
- b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido

modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47 del RGPD. Normas corporativas vinculantes.

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas

corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48 del RGPD. Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49 del RGPD. Excepciones para situaciones específicas.

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) 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;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) 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.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para

situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 40 de la LOPDPGDD. Régimen de las transferencias internacionales de datos.

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41 de la LOPDPGDD. Supuestos de adopción por la Agencia Española de Protección de Datos.

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas

contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42 de la LOPDPGDD. Supuestos sometidos a autorización previa de las autoridades de protección de datos.

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43 de la LOPDPGDD. Supuestos sometidos a información previa a la autoridad de protección de datos competente.

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional

de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

Estrategias de verificación:

Análisis de documentación, Entrevistas con responsables.

Evidencias del auditor:

- Se comprueba que todas las transferencias de datos a terceros países u organizaciones internacionales están identificadas e incluidas en el registro de actividades de tratamiento y en las cláusulas informativas pertinentes.
- Se comprueba que, en las transferencias de datos basadas en una decisión de adecuación de la Comisión, se realiza un seguimiento de su validez.
- Se comprueba que las transferencias de datos realizadas mediante garantías adecuadas disponen de una copia de dichas garantías y las mismas cumplen los requisitos necesarios.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

ENCARGADOS DEL TRATAMIENTO

Referencia legal:

Artículo 28 del RGPD. Encargado del tratamiento.

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 33 de la LOPDPGDD. Encargado del tratamiento.

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Entrevistas con responsables, Entrevistas con usuarios.

Evidencias del auditor:

- Se comprueba que las relaciones entre el responsable y los encargados se están regulando mediante un contrato escrito u otro acto jurídico que vincula al encargado respecto del responsable.
- Se ha comprobado que, en los contratos de acceso a datos por cuenta de terceros, se documentan de forma precisa las instrucciones respecto al encargo.
- Se ha comprobado que en los contratos se establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados.
- Se ha comprobado que, en los contratos de acceso a datos por cuenta de terceros, se establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable.
- Se ha comprobado que los contratos establecen las instrucciones respecto a las transferencias de datos a terceros países u organizaciones internacionales y los detalles de las mismas.
- Se ha comprobado que los contratos garantizan que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
- Se ha comprobado que los contratos establecen que el encargado del tratamiento tomará las medidas de seguridad necesarias para proteger la confidencialidad, integridad y disponibilidad de la información.
- Se ha comprobado que los contratos incluyen las medidas de seguridad en una lista o se remite a un estándar reconocido.
- Se ha comprobado que en los contratos se establece que no se recurrirá a otro encargado sin la autorización del responsable, así como que cumplirán las obligaciones que establece la normativa para recurrir a otro encargado del tratamiento.
- Se ha comprobado que los contratos establecen que el encargado asistirá al responsable para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.
- Se ha comprobado que los contratos establecen que se suprimirán o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales.

- Se ha comprobado que los contratos establecen que el encargado pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable.
- Se ha comprobado que se han identificado todos los encargados del tratamiento que prestan servicio a la entidad.

Deficiencias encontradas:

- Se ha observado que no están firmados todos los contratos de acceso a datos por cuenta de terceros por ambas partes y tampoco existe evidencia de que se hayan formalizado jurídicamente por otros medios.

Propuesta de medidas correctoras o complementarias:

- Firmar todos los contratos de acceso a datos por cuenta de terceros por ambas partes y/o, en su caso, obtener evidencias de que se han formalizado jurídicamente por otros medios.

Observaciones del auditor:

Falta por firmar varios contratos de acceso a datos por cuenta de terceros

Recomendaciones del auditor:

Es necesario firmar todos los contratos de acceso a datos por cuenta de terceros para cumplir la normativa.

DERECHOS DE LOS INTERESADOS

Referencia legal:

Artículo 15 del RGPD. Derecho de acceso del interesado.

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Artículo 16 del RGPD. Derecho de rectificación.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17 del RGPD. Derecho de supresión («el derecho al olvido»).

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concorra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18 del RGPD. Derecho a la limitación del tratamiento.

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado lo necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19 del RGPD. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea

imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20 del RGPD. Derecho a la portabilidad de los datos.

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Artículo 21 del RGPD. Derecho de oposición.

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernen, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22 del RGPD. Decisiones individuales automatizadas, incluida la elaboración de perfiles.

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Artículo 12 de la LOPDPGDD. Disposiciones generales sobre ejercicio de los derechos.

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

- 2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.*
- 3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.*
- 4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.*
- 5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.*
- 6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.*
- 7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.*

Artículo 13 de la LOPDPGDD. Derecho de acceso.

- 1. El derecho de acceso del afectado se ejercerá de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.*

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

- 2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.*

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14 de la LOPDPGDD. Derecho de rectificación.

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15 de la LOPDPGDD. Derecho de supresión.

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16 de la LOPDPGDD. Derecho a la limitación del tratamiento.

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17 de la LOPDPGDD. Derecho a la portabilidad.

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18 de la LOPDPGDD. Derecho de oposición.

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

Estrategias de verificación:

Análisis de documentación, Revisión de registros.

Evidencias del auditor:

- Se ha comprobado que existen protocolos específicos para el ejercicio de los derechos de los interesados.
- Se comprueba que se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

SEGURIDAD DEL TRATAMIENTO

Referencia legal:

Artículo 32 del RGPD. Seguridad del tratamiento.

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 28 de la LOPDPGDD. Obligaciones generales del responsable y encargado del tratamiento.

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular

valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Estrategias de verificación:

Análisis de documentación.

Evidencias del auditor:

- Se ha comprobado que se ha realizado un análisis de riesgos para valorar el riesgo a qué es expuesto cada uno de los tratamientos de datos personales.
- Se ha comprobado que el análisis de riesgos contempla el impacto que supondría para los interesados que la seguridad de la información se viese afectada por un incidente.
- Se ha comprobado que el análisis de riesgos identifica los distintos activos involucrados en el tratamiento de los datos personales.
- Se ha comprobado que los activos identificados en el análisis de riesgos incluyen todos los que tiene la entidad.
- Se ha comprobado que el análisis de riesgos identifica las distintas amenazas a las que están expuestos los activos involucrados en el tratamiento de los datos personales, así como las vulnerabilidades que podrían aprovechar dichas amenazas para causar el daño.
- Se ha comprobado que se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado.
- Se ha comprobado que el análisis de riesgos realiza el cálculo del riesgo para cada una de las amenazas y vulnerabilidades identificadas en cada uno de los activos involucrados en el tratamiento de los datos personales.
- Se ha comprobado que el análisis de riesgos identifica aquellos riesgos que se han de tratar para reducir dicho riesgo.
- Se ha comprobado que el análisis de riesgos detalla los controles y las medidas de seguridad que se han de implantar para reducir los riesgos identificados.
- Se ha comprobado que para determinar las medidas a aplicar se ha tenido en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.
- Se comprueba que se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
- Se comprueba que se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Se comprueba que se han incluido medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- Se ha comprobado que existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Deficiencias encontradas:

- Se observa que no se han implantado plenamente los controles y las medidas de seguridad detalladas en el análisis de riesgos.

Propuesta de medidas correctoras o complementarias:

- Implantar todas las medidas de seguridad detalladas en el análisis de riesgos.

Observaciones del auditor:

Falta por implantar varios controles y medidas de seguridad detalladas

Recomendaciones del auditor:

Es necesario implantar todos los controles y medidas de seguridad detalladas para cumplir la normativa.

PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

Referencia legal:

Artículo 25 del RGPD. Protección de datos desde el diseño y por defecto.

1. 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, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización 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.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Estrategias de verificación:

Análisis de documentación, Entrevistas con responsables.

Evidencias del auditor:

- Se ha comprobado que se analizan las medidas técnicas y organizativas apropiadas tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento.
- Se ha comprobado que durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD.
- Se ha comprobado que se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines.
- Se ha comprobado que las medidas implantadas garantizan que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

NOTIFICACIÓN DE LAS VIOLACIONES DE LA SEGURIDAD

Referencia legal:

Artículo 33 del RGPD. Notificación de una violación de la seguridad de los datos personales a la autoridad de control.

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará 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 presente artículo.

Artículo 34 del RGPD. Comunicación de una violación de la seguridad de los datos personales al interesado.

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Entrevistas con responsables.

Evidencias del auditor:

- Se comprueba que se ha establecido un procedimiento para identificar y gestionar las incidencias y las violaciones de la seguridad.
- Se ha comprobado que existe un procedimiento para que los encargados del tratamiento notifiquen las violaciones de la seguridad al responsable en el momento en que tengan conocimiento de ellas.
- Se ha comprobado que existe un procedimiento para valorar y notificar, en su caso, las violaciones de la seguridad a la autoridad de control en el plazo de 72 horas.

- Se ha comprobado que el personal conoce el procedimiento de notificación de incidencias.
- Se ha comprobado que existe un procedimiento para comunicar la violación de la seguridad sin dilación indebida cuando sea probable que entrañe un alto riesgo para los derechos y libertades.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

DELEGADO DE PROTECCIÓN DE DATOS

Referencia legal:

Artículo 37 del RGPD. Designación del delegado de protección de datos.

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38 del RGPD. Posición del delegado de protección de datos

1. *El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.*
2. *El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.*
3. *El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.*
4. *Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.*
5. *El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.*
6. *El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.*

Artículo 39 del RGPD. Funciones del delegado de protección de datos.

1. *El delegado de protección de datos tendrá como mínimo las siguientes funciones:*
 - a) *informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;*
 - b) *supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;*
 - c) *ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;*
 - d) *cooperar con la autoridad de control;*

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Artículo 34 de la LOPDPGDD. Designación de un delegado de protección de datos.

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

- a) Los colegios profesionales y sus consejos generales.*
- b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.*
- c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.*
- d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.*
- e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.*
- f) Los establecimientos financieros de crédito.*
- g) Las entidades aseguradoras y reaseguradoras.*
- h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.*
- i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.*
- j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.*
- k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.*

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35 de la LOPDPGDD. Cualificación del delegado de protección de datos.

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36 de la LOPDPGDD. Posición del delegado de protección de datos.

- 1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.*
- 2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.*
- 3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.*
- 4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.*

Artículo 37 Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Entrevistas con responsables, Entrevistas con usuarios.

Evidencias del auditor:

No hay evidencias.

Deficiencias encontradas:

- Se ha observado que al DPO/DPD no se le facilitan los recursos necesarios para mantener sus conocimientos.

Propuesta de medidas correctoras o complementarias:

- Facilitar al DPO/DPD los recursos necesarios para mantener sus conocimientos.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

Referencia legal:

Artículo 35 del RGPD. Evaluación de impacto relativa a la protección de datos.

- 1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*
- 2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.*
- 3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:*
 - a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;*
 - b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o*
 - c) observación sistemática a gran escala de una zona de acceso público.*
- 4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.*
- 5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.*
- 6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.*
- 7. La evaluación deberá incluir como mínimo:*

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36 del RGPD. Consulta previa.

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la

solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Entrevistas con responsables.

Evidencias del auditor:

- Se ha comprobado que se realiza el análisis de la necesidad de realizar una EIPD en todos los tratamientos de datos que realiza la entidad.
- Se ha comprobado que el análisis de la necesidad de realizar EIPD es correcto.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

CORRESPONSABLES DEL TRATAMIENTO

Referencia legal:

Artículo 26 del RGPD. Corresponsables del tratamiento.

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 29 de la LOPDPGDD. Supuestos de corresponsabilidad en el tratamiento.

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Estrategias de verificación:

Análisis de documentación.

Evidencias del auditor:

No hay evidencias.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

GARANTÍA DE LOS DERECHOS DIGITALES

Referencia legal:

Artículo 87 de la LOPDPGDD. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

- 1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.*
- 2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.*
- 3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.*

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los periodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88 de la LOPDPGDD. Derecho a la desconexión digital en el ámbito laboral.

- 1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.*
- 2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.*
- 3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de*

realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 90 de la LOPDPGDD. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Estrategias de verificación:

Análisis de documentación, Revisión de registros, Inspección visual, Entrevistas con responsables, Entrevistas con usuarios.

Evidencias del auditor:

- Se comprueba que la organización dispone de unos criterios o normas de uso de los dispositivos digitales documentadas.
- Se comprueba que la organización ha comunicado los criterios o normas de uso de los dispositivos digitales al personal afectado de la organización o están colocados en algún sitio común donde pueden ser consultadas.
- Se comprueba que la organización dispone de una política de desconexión digital documentada que reúne los requisitos del art. 88 de la LOPDPGDD.
- Se comprueba que la organización ha comunicado la política de desconexión digital al personal afectado o está colocada en algún sitio común donde puede ser consultada.

Deficiencias encontradas:

No hay deficiencias.

Propuesta de medidas correctoras o complementarias:

No hay medidas correctoras para esta categoría.

Observaciones del auditor:

El auditor no ha hecho observaciones.

Recomendaciones del auditor:

El auditor no ha hecho recomendaciones.

4. ANÁLISIS DE LA IMPLANTACIÓN Y EFICACIA DE LAS MEDIDAS DE SEGURIDAD

Se ha analizado la implantación y eficacia de las siguientes medidas de seguridad:

- ACCESO RESTRINGIDO A LAS ÁREAS
- ACTUALIZACIÓN DE LOS SISTEMAS
- ALMACENAMIENTO EN ÁREAS RESTRINGIDAS
- ALMACENAMIENTO DE SOPORTES DIGITALES Y DOCUMENTOS
- BLOQUEO DEL SISTEMA DESATENDIDO
- COMPROMISOS DE CONFIDENCIALIDAD
- CONFIGURACIÓN DE SEGURIDAD PROTEGIDA
- COPIA O REPRODUCCIÓN DE DOCUMENTOS
- COPIAS DE SEGURIDAD
- COPIAS DE SEGURIDAD REMOTAS
- DESTRUCCIÓN DE DOCUMENTACIÓN EN PAPEL
- DESTRUCCIÓN Y REUTILIZACIÓN DE EQUIPOS Y SOPORTES
- FORMACIÓN DEL PERSONAL
- POLÍTICA DE CONTROL DE ACCESO
- POLÍTICA DE SEGURIDAD DE LA RED
- POLÍTICA DE SEGURIDAD FÍSICA
- TRABAJO FUERA DE LOS LOCALES
- TRASLADO DE SOPORTES Y DOCUMENTOS
- REGISTRO DE LA ACTIVIDAD EN LOS SISTEMAS
- RESTRICCIÓN EN LA INSTALACIÓN DE SOFTWARE
- ROLES Y RESPONSABILIDADES EN SEGURIDAD
- IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS
- SOFTWARE ANTI-MALWARE

ACCESO RESTRINGIDO A LAS ÁREAS

Medida de seguridad:

El acceso al área en el que se encuentren los servidores y otros sistemas críticos, deberá estar protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente.

Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a las mismas.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

ACTUALIZACIÓN DE LOS SISTEMAS

Medida de seguridad:

Los ordenadores, portátiles, tabletas, smartphones y demás dispositivos utilizados para el almacenamiento, tratamiento o transmisión de datos personales, deberán mantenerse actualizados a lo largo del tiempo en la medida de lo posible.

Sistemas operativos: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.

Programas: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.

Dispositivos (routers, firewalls, videocámaras, etc.): se ha de mantener el firmware actualizado a la última versión estable proporcionada por el fabricante.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

ALMACENAMIENTO EN ÁREAS RESTRINGIDAS

Medida de seguridad:

Los armarios, archivadores u otros elementos en los que se almacenen la documentación y los soportes deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente.

Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a dichos documentos o soportes.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

ALMACENAMIENTO DE SOPORTES DIGITALES Y DOCUMENTOS

Medida de seguridad:

Los dispositivos de almacenamiento de los soportes y documentos que contengan datos de carácter personal, deberán disponer de mecanismos que obstaculicen su apertura, mediante llaves u otros medios que realicen la misma función.

Solo los usuarios autorizados deberán disponer de las llaves y medios que facilitan la apertura de dichos dispositivos.

Cuando las características físicas no permitan adoptar esta medida, se deberán adoptar las medidas necesarias para impedir el acceso de personas no autorizadas.

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados anteriormente, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

Implementación:

Todos los soportes y documentos con datos personales se almacenan en dispositivos que disponen de mecanismos que obstaculizan su apertura mediante llave.

Siempre que una persona no autorizada pueda tener acceso a soportes o documentos con datos personales, está en todo momento supervisada por alguien autorizado para acceder a dichos documentos, no dejándola sola con ellos bajo ninguna circunstancia.

Deficiencias encontradas:

Se ha comprobado que la medida de seguridad no está plenamente implantada.

BLOQUEO DEL SISTEMA DESATENDIDO

Medida de seguridad:

El sistema debe tener configurado el bloqueo automático después de transcurrir un tiempo determinado en el que el usuario no ha estado activo.

Deficiencias encontradas:

Se ha comprobado que la medida de seguridad no está plenamente implantada.

COMPROMISOS DE CONFIDENCIALIDAD

Medida de seguridad:

Todo el personal involucrado en el tratamiento de datos personales debe firmar un compromiso de confidencialidad y deber de secreto.

En dicho compromiso, se estipulará que los datos a los que tenga acceso esa persona en el ejercicio de sus funciones son confidenciales y tiene el deber de guardar secreto profesional respecto a ellos.

Dicho deber de secreto subsistirá aún después de terminada la relación con el responsable del tratamiento.

Implementación:

Todo el personal, antes de iniciar su actividad, firma el compromiso de confidencialidad estipulado por la organización.

CONFIGURACIÓN DE SEGURIDAD PROTEGIDA

Medida de seguridad:

Los usuarios no deben desactivar ni omitir las configuraciones de seguridad establecidas por el responsable ni desinstalar ningún software de seguridad del sistema.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

COPIA O REPRODUCCIÓN DE DOCUMENTOS

Medida de seguridad:

La realización de copias o reproducción de los documentos con datos personales sensibles, sólo se podrá realizar bajo el control del personal autorizado para ello.

Asimismo, las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida según los procedimientos establecidos para la destrucción segura de documentos.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

COPIAS DE SEGURIDAD

Medida de seguridad:

La seguridad de los datos personales no solo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad, es necesario que existan unos procesos de respaldo y recuperación, de forma que, ante un fallo informático, permitan reconstruir el fichero en el estado que se encontraba antes de la pérdida.

Se realizarán copias de respaldo periódicamente, en función del volumen y de la frecuencia de actualización de los datos.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado que se encontraban al tiempo de producirse la pérdida o destrucción.

Las copias de seguridad deben recibir un nivel apropiado de protección física y ambiental.

Se debe monitorizar la ejecución de las copias de seguridad para garantizar que estén completas.

En caso de realizar copias incrementales de la información, se deben realizar copias de seguridad completas con regularidad.

Se verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Únicamente, en el caso de que la pérdida o destrucción afectase a tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos, quedando constancia motivada de este hecho en el Registro de Incidencias.

Las pruebas anteriores a la implantación o modificación de sistemas de información que traten con datos de carácter personal no se realizarán con datos reales, salvo que se asegure la seguridad correspondiente al tratamiento realizado y se registre su realización. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Implementación:

Las copias de respaldo se realizan semanalmente a un disco duro externo.

COPIAS DE SEGURIDAD REMOTAS

Medida de seguridad:

Se conservará una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente a aquel en el que se encuentran los equipos informáticos que los tratan, que deberá cumplir, en todo caso, las medidas de seguridad exigidas.

En caso de que se utilice un servicio de terceros para el almacenamiento de respaldo, la copia debe estar cifrada antes de enviarla, se deberá suscribir el correspondiente contrato de acceso a datos por cuenta de terceros y el lugar deberá reunir los requisitos de seguridad requeridos en función de la sensibilidad de la información que aloja.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

DESTRUCCIÓN DE DOCUMENTACIÓN EN PAPEL

Medida de seguridad:

Uno de los mayores peligros para la confidencialidad de los datos son los documentos desechados.

Todos los documentos en papel desechados que contengan datos personales deberán ser eliminados o destruidos de acuerdo a las siguientes instrucciones:

- 1. Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.*
- 2. Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.*
- 3. En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.*
- 4. El Responsable del tratamiento deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.*

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

DESTRUCCIÓN Y REUTILIZACIÓN DE EQUIPOS Y SOPORTES

Medida de seguridad:

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores, tabletas o smartphone obsoletos que contengan discos o memorias de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- 1. Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.*
- 2. Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.*
- 3. En todos los disquetes y otros soportes removibles desechados, los datos personales deberán ser eliminados con alguna aplicación de borrado seguro de soportes que haga imposible su recuperación. Posteriormente, estos disquetes y soportes removibles serán entregados, para su reutilización, al Responsable de Seguridad o al Delegado de Protección de Datos. Si los soportes contienen datos sensibles, se deben dar varias pasadas de sobreescritura basada en software por todos los soportes antes de eliminarlos.*
- 4. Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al Responsable de Seguridad o al Delegado de Protección de Datos para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.*
- 5. El Responsable del tratamiento deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado y deberá existir un registro de la destrucción.*

Deficiencias encontradas:

Se ha comprobado que la medida de seguridad no está plenamente implantada.

FORMACIÓN DEL PERSONAL

Medida de seguridad:

La formación del personal es fundamental para la ciberseguridad y la protección de datos personales de la organización.

Para que el tratamiento de los datos personales se realice en todo momento según los requisitos legales y de seguridad que marca la normativa, todo el personal involucrado en el tratamiento (recogida, registro, utilización, destrucción, etc.), ya sea interno o externo, debe recibir formación apropiada a las funciones que realice, tanto en materia de protección de datos personales como en materia de ciberseguridad.

De igual forma, todo el personal debe conocer las políticas, procedimientos y protocolos de la organización, en relación a la ciberseguridad y la protección de datos personales, que le afectan en el desempeño de sus funciones dentro de ella.

El personal que realice tareas de administración de sistemas debe recibir formación apropiada en relación a los sistemas que gestiona, de forma que no se produzcan omisiones o errores accidentales que afecten, o puedan afectar, a la confidencialidad, integridad y disponibilidad de los datos personales.

La persona que actúe como Coordinador o Delegado de Protección de Datos en la organización debe también disponer de la formación y las competencias necesarias para desempeñar sus funciones con rigor y solvencia.

Las acciones de concienciación y capacitación que se desarrollen en este ámbito deben ser periódicas, incluyendo actualizaciones sobre las políticas y procedimientos de la organización, según correspondan al puesto de trabajo de cada empleado o externo.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

POLÍTICA DE CONTROL DE ACCESO

Medida de seguridad:

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Se deberán establecer mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Dichos mecanismos, en el caso de soportes informáticos, podrán consistir en la asignación de contraseñas para el acceso a los mismos, u otros dispositivos más sofisticados: biométricos, llaves USB, etc.; y en el caso de documentos en papel, en la entrega de llaves que facilitan la apertura de los dispositivos de almacenamiento donde se recopila la información.

Deberá existir también una relación actualizada de perfiles, usuarios y accesos autorizados.

Exclusivamente el Administrador de cada fichero está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el Responsable del Tratamiento.

Asimismo, deberán existir procedimientos para efectuar el alta, modificación y baja de las autorizaciones de acceso a los datos, así como los controles de acceso a los sistemas de información y las ubicaciones donde se almacenan datos personales.

De existir personal ajeno al responsable del tratamiento con acceso a los recursos, deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Implementación:

Los procedimientos para dar de alta, baja o modificación de acceso autorizado a los tratamientos son los siguientes:

- 1. Alta: cuando un nuevo empleado se incorpora, el administrador de ese tratamiento construye un identificador único para ese usuario según el procedimiento establecido y le asigna privilegios en función del perfil al que pertenece. Asimismo, el administrador del fichero le asigna una contraseña provisional que el usuario deberá cambiar en el primer acceso al sistema.*
- 2. Baja: en caso de que la baja sea temporal, el administrador procederá a bloquear la identificación del usuario, y en caso de que sea definitiva, procederá a la eliminación inmediata de todos sus derechos de acceso.*
- 3. Modificación: cuando un usuario desempeñe distintas funciones en la empresa, o tenga que acceder a datos a los que anteriormente no accedía, al administrador del fichero deberá cambiar sus privilegios de acceso en función al nuevo perfil al que pertenece.*

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

POLÍTICA DE SEGURIDAD DE LA RED

Medida de seguridad:

SEGURIDAD DE LA RED CABLEADA

Para evitar accesos remotos indebidos a los datos personales a través de Internet, el tráfico hacia y desde el sistema de TI debe monitorizarse y controlarse a través de un firewall o cortafuegos que filtre el tráfico y prevenga de posibles intrusiones.

Siempre que se acceda a servicios que estén publicados en Internet y desde los cuáles se realice algún tratamiento de datos personales (ya sea registro, descarga o consulta), la comunicación debe estar cifrada de extremo a extremo a través de TLS o tecnologías similares, de forma que los datos viajen cifrados en todo momento y estén seguros frente a posibles interceptaciones.

En el caso de que existan sistemas que traten datos especialmente sensibles, el responsable debe valorar aislar esa red de otras redes que pudiera tener, de forma que la superficie de ataque sea limitada, y el impacto en caso de incidente de seguridad, sea el menor posible.

Los puntos de red no utilizados deben encontrarse desactivados para evitar un posible acceso no autorizado a la red interna de la entidad.

SEGURIDAD DE LA RED WIFI

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio pueden viajar más allá de las paredes y filtrarse en habitaciones contiguas o llegar hasta la calle.

La infiltración no autorizada en redes inalámbricas es una tarea muy sencilla si la red WIFI no está adecuadamente configurada y protegida.

Para evitar esto, se debe proteger la red WIFI de las siguientes formas:

- 1. Cambiar la contraseña de acceso al WIFI que viene por defecto siguiendo el procedimiento establecido por la entidad para la construcción de contraseñas seguras.*
- 2. Activar el cifrado WPA2 (en ningún caso dejarla en abierto o con cifrado WEP).*
- 3. Cambiar el SSID de fábrica. En ningún caso debe identificar a la entidad.*
- 4. Valorar la activación del filtrado por MAC.*
- 5. Cambiar la clave de acceso regularmente.*
- 6. Cuando sea posible, aislar la red WIFI de la red interna*

El acceso inalámbrico a la red interna del sistema TI debe permitirse solo para los usuarios específicos y estar protegido mediante cifrado. Además, debe activarse el filtrado a través de MAC a los dispositivos a

los que se va a permitir conectarse, de forma que los dispositivos no autorizados previamente, no dispongan de conexión aunque conozcan la contraseña de acceso.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

POLÍTICA DE SEGURIDAD FÍSICA

Medida de seguridad:

Los locales donde se realizan los tratamientos de datos personales deben ser objeto especial de protección que garanticen la confidencialidad, integridad y disponibilidad de los datos protegidos, así como la adecuada protección del equipamiento utilizado para el tratamiento. A tal efecto, la documentación, los soportes y el equipamiento informático deberán ser protegidos frente robo o acceso no autorizado.

Para ello, los locales deberán contar con los medios mínimos de seguridad siendo conveniente que dispongan de dispositivos extintores de incendios, alarmas, etc.

Asimismo, los equipos, soportes y sistemas estarán ubicados en sitios seguros frente a inundaciones o fugas de agua.

Implementación:

Se dispone de extintores.

El acceso a los lugares donde se encuentran los sistemas de información y los soportes están protegidos por puertas que disponen de cerradura y se encuentran cerradas cuando no es necesario acceder a dichos sistemas o soportes.

Deficiencias encontradas:

Se ha comprobado que la medida de seguridad no está plenamente implantada.

TRABAJO FUERA DE LOS LOCALES

Medida de seguridad:

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del tratamiento, o del encargado del tratamiento, será preciso que exista una autorización previa, y en todo caso, deberán garantizarse los requisitos de seguridad correspondientes al tipo de tratamiento realizado.

Deficiencias encontradas:

Se ha comprobado que la medida de seguridad no está plenamente implantada.

TRASLADO DE SOPORTES Y DOCUMENTOS

Medida de seguridad:

Cuando los soportes y/o documentos vayan a salir fuera de los locales en que se encuentran ubicados los tratamientos, se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información durante el transporte.

Para ello, el traslado de soportes y documentos fuera de las instalaciones se realizará en un maletín o contenedor similar que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.

En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

En el caso de los soportes digitales, siempre que sea posible, se debe cifrar la información que contiene o bien utilizar otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Deficiencias encontradas:

Se ha comprobado que la medida de seguridad no está plenamente implantada.

REGISTRO DE LA ACTIVIDAD EN LOS SISTEMAS

Medida de seguridad:

Los archivos de registro deben activarse en cada sistema y aplicación utilizada para el procesamiento de datos personales con objeto de disponer de una adecuada trazabilidad de los usuarios de la misma.

Dichos registros de acceso deben tener una marca temporal de tiempo y estar protegidos frente a manipulaciones.

Se deben registrar también las acciones de los administradores y operadores del sistema, incluyendo la adición, eliminación o cambios de derechos.

Los relojes de todos los sistemas deben estar sincronizados con una fuente común.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

RESTRICCIÓN EN LA INSTALACIÓN DE SOFTWARE

Medida de seguridad:

Los usuarios no deben tener privilegios para instalar aplicaciones que no han sido autorizadas por el responsable.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

ROLES Y RESPONSABILIDADES EN SEGURIDAD

Medida de seguridad:

Todos los empleados y contratistas deben conocer y aplicar las normas, políticas y procedimientos que la organización tiene establecidos para el tratamiento de los datos personales.

Para ello, la organización debe informar a todo el personal, interno y externo, de las funciones y obligaciones en materia de protección de datos personales, así como de las normas y buenas prácticas que deben seguir en materia de seguridad de la información.

También deben ser informados de los pasos a seguir la realizar la notificación de las incidencias que se puedan producir así como las peticiones de derechos de los interesados.

Implementación:

En el Anexo IV se encuentran detalladas las funciones y obligaciones del personal en materia de protección de datos, así como de los pasos a seguir para notificar los incidentes de seguridad y las peticiones de derechos de los interesados.

Dicho Anexo IV es entregado y/o se encuentra a disposición de todo el personal, interno y externo.

Por otro lado, al personal interno y externo se le han comunicado los protocolos y procedimientos que le afectan en relación al tratamiento de los datos personales y la seguridad, en función de su puesto.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS

Medida de seguridad:

Se establecerán las medidas de seguridad necesarias en los sistemas informáticos de forma que se garantice que únicamente accederá a los tratamientos el personal autorizado para ello.

Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

De la misma forma, se establecerá un sistema que permita la identificación inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información, y la debida autenticación para verificar la identidad del usuario que intenta acceder.

Aunque ya existen procedimientos de identificación basados en certificado electrónico, o incluso en datos biométricos, como huellas dactilares, las contraseñas personales constituyen todavía hoy en día uno de los métodos más usados para proteger el acceso a los datos, y por tanto, deben estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

La periodicidad máxima con la que tienen que ser cambiadas las contraseñas no debe ser superior a un año. Se almacenarán de forma ininteligible en los sistemas informáticos mientras estén vigentes.

Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, como “casa”, el nombre propio, etc. Para ello se seguirán las siguientes pautas en la construcción de contraseñas: longitud de al menos 8 caracteres, mezcla de números y letras; no deberán coincidir, ni siquiera en parte, con el código del usuario; y no deberán estar basadas en cadenas de caracteres que sean fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).

En el caso de dispositivos que no permitan varios nombres de usuario (como routers, firewalls, cámaras, etc.), el responsable de seguridad establecerá la contraseña de dicho dispositivo según las pautas indicadas anteriormente y la almacenará de forma que se garantice su confidencialidad e integridad.

Antes de colocar cualquier dispositivo en la red o para su uso, debe cambiarse la contraseña de fábrica por otra que siga las pautas antes indicadas.

Implementación:

El sistema de identificación y autenticación que da acceso a los ficheros automatizados, dispone de las siguientes características:

- 1. Identificación: inicial del nombre más el apellido.*
- 2. Autenticación: contraseña escogida por el usuario.*
- 3. Longitud y contenido de las contraseñas: deben tener una longitud mínima de 8 caracteres y contener mezcla de números y letras.*
- 4. Periodicidad de cambio: el cambio de las contraseñas es cada 365 días.*
- 5. Acceso al sistema por primera vez: el administrador asignará una contraseña provisional al nuevo usuario, que deberá ser cambiada en su primer acceso al sistema por una que sólo conozca el usuario y en base a las características definidas anteriormente.*

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

SOFTWARE ANTI-MALWARE

Medida de seguridad:

En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema anti-malware que evite, en la medida de lo posible, el robo y la destrucción de la información y datos personales.

El sistema anti-malware deberá ser actualizado, al menos, semanalmente.

Evidencias del auditor:

Se ha comprobado que la medida de seguridad está implantada y es eficaz.

5. RESUMEN DE LAS MEDIDAS CORRECTORAS O COMPLEMENTARIAS A ADOPTAR

En cuanto al cumplimiento de los requisitos legales de la normativa de protección de datos personales de los tratamientos objeto de la auditoría, el resumen de las deficiencias encontradas, así como de las medidas correctoras o complementarias a adoptar, se indica a continuación:

Deficiencia	Medida correctora o complementaria
Se ha observado que no se está informando adecuadamente del sistema de videovigilancia a los interesados.	Colocar carteles informativos en un lugar visible que contengan, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos y cómo obtener la información completa del tratamiento.
Se ha observado que no están firmados todos los contratos de acceso a datos por cuenta de terceros por ambas partes y tampoco existe evidencia de que se hayan formalizado jurídicamente por otros medios.	Firmar todos los contratos de acceso a datos por cuenta de terceros por ambas partes y/o, en su caso, obtener evidencias de que se han formalizado jurídicamente por otros medios.
Se observa que no se han implantado plenamente los controles y las medidas de seguridad detalladas en el análisis de riesgos.	Implantar todas las medidas de seguridad detalladas en el análisis de riesgos.
Se ha observado que al DPO/DPD no se le facilitan los recursos necesarios para mantener sus conocimientos.	Facilitar al DPO/DPD los recursos necesarios para mantener sus conocimientos.

5.1. OBSERVACIONES DEL AUDITOR

Las observaciones que el auditor ha realizado son las siguientes:

- Se ha introducido un nuevo Tratamiento: Tratamiento de los datos de las partes implicadas en el Canal de denuncias interno
- Falta por firmar varios contratos de acceso a datos por cuenta de terceros
- Falta por implantar varios controles y medidas de seguridad detalladas

5.2. RECOMENDACIONES DEL AUDITOR

Las recomendaciones que el auditor ha realizado son las siguientes:

- Es necesario firmar todos los contratos de acceso a datos por cuenta de terceros para cumplir la normativa.
- Es necesario implantar todos los controles y medidas de seguridad detalladas para cumplir la normativa.

6. RESUMEN DE LAS MEDIDAS DE SEGURIDAD QUE NO ESTÁN PLENAMENTE IMPLEMENTADAS

En cuanto al cumplimiento de las medidas de seguridad, a continuación, se indican aquellas medidas de seguridad que no están plenamente implantadas:

- ALMACENAMIENTO DE SOPORTES DIGITALES Y DOCUMENTOS
- BLOQUEO DEL SISTEMA DESATENDIDO
- DESTRUCCIÓN Y REUTILIZACIÓN DE EQUIPOS Y SOPORTES
- POLÍTICA DE SEGURIDAD FÍSICA
- TRABAJO FUERA DE LOS LOCALES
- TRASLADO DE SOPORTES Y DOCUMENTOS

6.1. OBSERVACIONES DEL AUDITOR

Las observaciones que el auditor ha realizado son las siguientes:

El auditor no ha hecho observaciones.

6.2. RECOMENDACIONES DEL AUDITOR

Las recomendaciones que el auditor ha realizado son las siguientes:

El auditor no ha hecho recomendaciones.