

Registro de Actividades Reglamento General (UE) 2016/679 de Protección de Datos

Actividades de Tratamiento

<i>GESTIÓN CLIENTES</i>
<i>GESTIÓN PROVEEDORES</i>
<i>GESTIÓN DE RECURSOS HUMANOS</i>
<i>GESTIÓN NÓMINAS</i>
<i>CURRICULUM VITAE</i>

Responsable
RAXIA FORMACIÓN, S.L
B 70.576.475
Rúa das Cerdeiras, s/n,
15841, Santa Comba (A Coruña)



ORGANIZACIÓN Y ESTRUCTURA DEL INFORME

Capítulo 1	INTRODUCCIÓN, OBJETO, ÁMBITO, ALCANCE Y CONCEPTOS BÁSICOS
1.1	Introducción
1.2	Objeto del Registro de Actividades
1.3	Ámbito de Aplicación del Registro de Actividades
1.4	Alcance del Registro de Actividades
1.5	Conceptos Básicos
Capítulo 2	CONTROLES PERIÓDICOS
Capítulo 3	ANÁLISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO
3.1	Análisis de Riesgos
3.2	Evaluación de Impacto
3.2.1	Que debe incluir la Evaluación de Impacto
3.2.2	Metodología para realizar una Evaluación de Impacto
3.2.3	Equipo de Trabajo
3.2.4	Plantilla de análisis de riesgos
Capítulo 4	REGISTRO DE ACTIVIDADES
4.A	Descripción del Registro Actividades de Tratamiento
4.B	Encargados del Tratamiento
4.C	Locales de Tratamientos de Datos
4.D	Software y entorno de comunicaciones
4.E	Equipos, impresoras y otros periféricos
4.F	Nombramiento y autorizaciones de los usuarios
4.G	Procedimientos de control, copias de seguridad, cuentas de correo electrónico y usuarios
4.G.1	Procedimientos para altas, bajas o modificaciones de acceso a usuarios.
4.G.2	Procedimientos identificación y autenticación.
4.G.3	Procedimientos de respaldo y recuperación.
4.G.4	Procedimientos de gestión de soportes.
4.G.5	Procedimiento de gestión de entrada/salida de soportes.
4.G.6	Cuentas de Correo electrónico autorizadas.
4.G.7	Procedimiento para destrucción de desechos informáticos.
4.G.8	Autorización para el uso de PC Portátiles.
4. H	Notificación y Gestión de Incidencias Impreso notificación de incidencias
4. I	Modificaciones, Controles periódicos y Auditorías
Capítulo 5	CLÁUSULAS Y MODELOS
Capítulo 6	CONTRATOS ENCARGADOS DE TRATAMIENTO
Capítulo 7	CONTRATOS PERSONAL

INTRODUCCIÓN, OBJETO, ÁMBITO Y ALCANCE Y CONCEPTOS BÁSICOS.

1.1. Introducción

La **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)**, dispone en su artículo 9 la obligación del Responsable del Fichero de **adoptar las medidas de índole técnica y organizativas** que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

En su artículo 44.3, letra h) dispone que constituye una infracción grave el mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

La obligación de seguridad dispuesta por el artículo 9 de la LOPD, viene desarrollada en el **Reglamento de desarrollo** de la LOPD, aprobado por el **Real Decreto 1720/2007**, de 21 de diciembre (BOE 17, de 19 de enero de 2008), en adelante RLOPD.

EL Título VIII del RLOPD tiene por objeto el desarrollo de las **medidas de seguridad** de índole técnica y organizativas necesarias para garantizar la seguridad, confidencialidad e integridad de los ficheros de datos personales, con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales, frente a su alteración, pérdida, tratamiento o acceso no autorizado.

El 4 de mayo de 2016 se aprobó el **Reglamento General (UE) 2016/679 de Protección de Datos (RGPD)** que entra en vigor el 25 de mayo de 2018 y que supone que los usuarios deben tener un mayor control sobre sus datos de carácter personal. La norma contiene importantes novedades como un nuevo régimen sancionador; nuevos derechos para los usuarios (derecho al olvido; derecho de portabilidad); el derecho a obtener una indemnización por los daños o perjuicios causados al titular de los datos; surge la figura del DPO (Delegado de Protección de Datos o Data Protection Officer); aplicación del concepto ventanilla única y una nueva regulación de los datos de los menores.

El 5 de diciembre del 2018, se aprobó la nueva **Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**. Esta norma adapta el ordenamiento jurídico español al Reglamento General de Protección de Datos (RGPD) y completa y desarrolla sus disposiciones. Además, la Ley reconoce y garantiza un nuevo conjunto de derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución

En virtud de esta normativa, se realiza este Registro de Actividades el cual se dirige principalmente a todo el personal que dentro de la organización accede, debido a sus funciones laborales o de otra índole, a datos de carácter personal.

Al conjunto de Actividades de Tratamiento, programas, soportes, sistemas y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal, se aludirá de forma indistinta como **sistemas de información de la empresa**.

1.2. Objeto del Registro de Actividades

El presente documento responde a la obligación establecida en la Normativa Vigente, de protección de datos de carácter personal, en el que se regulan las **medidas de seguridad para las Actividades de Tratamiento automatizados o no, que contengan datos de carácter personal**.

Este documento ha sido elaborado bajo la responsabilidad de **RAXIA FORMACIÓN S.L.** que se compromete a implantar y actualizar ésta Normativa de Seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten al acceso a los mismos.

Este Documento **deberá mantenerse permanentemente actualizado y ser revisado** siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Por tanto, cualquier modificación relevante conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial. El contenido del Registro de Actividades deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

1.3. Ámbito de Aplicación del Registro de Actividades

El ámbito de aplicación del presente Registro de Actividades comprende las Actividades de Tratamiento que contienen datos de carácter personal que se encuentran bajo la responsabilidad de **RAXIA FORMACIÓN S.L.**, incluyendo los sistemas de información, soportes automatizados o no y equipos empleados, departamentos, instalaciones y personal propio o ajeno y perfiles de usuarios que intervienen en el tratamiento y los locales donde se ubican.

Las medidas de seguridad se clasifican, atendiendo a la naturaleza de los datos, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

1.4. Alcance del Registro de Actividades

El responsable de los tratamientos y los encargados del tratamiento, en caso de existir, deberán **implantar las medidas de seguridad** con arreglo a lo dispuesto en el RGPD, con independencia de cuál sea su sistema de tratamiento.

Todas las personas que tengan acceso a los datos, bien a través del Sistema de información habilitado para acceder al mismo, o bien a través de cualquier otro medio, automatizado o manual de acceso, se encuentran obligadas por ley a **cumplir lo establecido en este documento**, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Las medidas de seguridad recogidas en el presente Registro de Actividades, por tanto, afectan:

- A todas las áreas, divisiones, departamentos, servicios y dependencias de la organización y tanto a sus directivos como a otros empleados y también a las entidades y los profesionales contratados bajo otras modalidades cuando en sus contratos se especifique.
- A bases de datos, ficheros, tratamientos, equipos, soportes, documentación, programas y sistemas.

1.5. Conceptos Básicos.

A los efectos previstos en el Reglamento General (UE) 2016/679 de Protección de Datos (RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cabe destacar los siguientes conceptos:

Actividad de Tratamiento (Fichero): Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Datos de Carácter Personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Datos de carácter personal relacionados con la salud: Informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona física, incluida la prestación de servicios de atención sanitaria, datos referidos a porcentaje de discapacidad y a información genética.

Datos biométricos: Datos personales utilizados para el reconocimiento único de la persona basado en uno y/o más rasgos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única, tales como imágenes faciales o datos dactiloscópicos.

Tratamiento de datos: Operaciones y procedimientos técnicos realizados sobre datos personales, ya sean de carácter automatizado o no, que permitan la recogida, registro, grabación, conservación, elaboración, adaptación, modificación, extracción, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento de los datos.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Responsable de seguridad: Persona o personas a las que el responsable del fichero o Tratamiento ha asignado formalmente la función de coordinar las medidas de seguridad aplicables.

Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

Transferencia internacional de datos: es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español (art. 5.1.s RLOPD).

Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Soportes: Son aquellos objetos físicos que almacenan o contienen datos del Fichero. En un fichero manual no automatizado, estos datos pueden estar almacenados en los soportes en forma de documentos escritos, a mano o a máquina, impresos, fotocopias, cintas con grabaciones analógicas de audio o video, microfilms, placas radiográficas o de exploraciones médicas, fotografías no digitalizadas, dibujos o cualquier otro medio físico no informatizado. Es decir, los soportes y documentación en el caso de los ficheros manuales no son solamente documentos en papel, sino en cualquier medio físico, con la única diferencia respecto a los llamados ficheros automatizados, de que esa información no puede ser recuperada, grabada o modificada por medios informáticos.

Delegado de Protección de Datos: Es una nueva figura, este perfil, debe ser asumido por un especialista en protección de datos con amplios conocimientos jurídicos y técnicos en este campo, que se crea al lado de las figuras del responsable y del encargado del tratamiento. El Delegado de Protección de Datos tiene, como mínimo, las siguientes funciones:

- Informar y asesorar a los responsables y encargados del tratamiento de datos personales (y a sus empleados) de las obligaciones que tienen, derivadas tanto de la legislación europea como de la española.
- Supervisar el cumplimiento de dicha legislación y de la política de protección de datos de una Administración Pública, empresa o entidad privada: asignación de responsabilidades, concienciación y formación del personal, auditorías, etc.
- Ofrecer el asesoramiento que se le solicite para hacer la evaluación de impacto de un tratamiento de datos personales, cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, y supervisar luego su aplicación.

- Cooperar con las “autoridades de control” (Agencias de Protección de Datos)
- Actuar como “punto de contacto” de las autoridades de control para cualquier consulta sobre el tratamiento de datos personales; especialmente, la consulta previa obligatoria en los casos en los que el tratamiento entrañe un alto riesgo.

Derecho de información: En el momento en que se procede a la recogida de los datos personales, el interesado debe ser informado previamente de modo expreso, preciso e inequívoco de, entre otros, la existencia de un fichero, de la posibilidad de ejercitar sus derechos y del responsable del tratamiento.

Derecho de acceso: El derecho de acceso permite al ciudadano conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento.

Derecho de rectificación: El derecho de rectificación viene regulado en el art. 16 y en el considerando 65 del RGPD. Este derecho se caracteriza porque permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

Derecho de supresión: El derecho de supresión viene regulado en el art. 17 y en los considerandos 65 y 66 del RGPD. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernen 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) (Consentimiento), o el artículo 9, apartado 2, letra a) (Consentimiento en categorías especiales de datos), y este no se base en otro fundamento jurídico;
- c. **el interesado se oponga al tratamiento** con arreglo al artículo 21, apartado 1 (Derecho de oposición personal, interés público o interés legítimo), y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2 (Derecho de oposición marketing Directo);
- 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

Derecho de oposición o exclusión: El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo.

Derecho al olvido: Es la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de internet. El derecho al olvido hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).

Derecho a la portabilidad: Otorga las siguientes facultades al titular de los datos: Obtener una copia de sus datos personales en un formato electrónico estructurado y de uso habitual. Transferir sus datos, y otras informaciones que haya facilitado, de un sistema de tratamiento electrónico a otro

El titular del derecho a la portabilidad de los datos personales es la persona interesada, es decir, aquella persona física a la cual se refieren los datos personales sobre los cuales se pretenda ejercer el derecho a la portabilidad.

Derecho a la limitación del tratamiento: El derecho a la limitación viene regulado en los art. 18 y considerando 67 del RGPD. Si bien en nuestra normativa de protección de datos establecía que el bloqueo era una consecuencia derivada de la cancelación, en el caso de la limitación es un derecho en sí mismo considerado. De tal manera que el responsable de tratamiento deberá limitar el mismo en determinados supuestos:

- **Impugnación de exactitud de datos**, durante el plazo que se permite al responsable verificar la misma.
- **Tratamientos ilícitos en los que el interesado se opone a la supresión.**
- Los **datos ya no son necesarios** para la finalidad del tratamiento, **pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones.**
- **Oposición** conforme al art. 21 del RGPD.

Elaboración de Perfiles: Se refiere a toda forma de tratamiento automatizado de datos personales consistente en utilizar datos para evaluar aspectos personales propios de un individuo, en particular para analizar y predecir aspectos relativos a su rendimiento profesional, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o su comportamiento, su ubicación o sus movimientos.

Evaluación de impacto: Es un informe de un análisis de riesgos sobre los efectos potenciales del tratamiento de datos previsto, sobre los derechos y las libertades de los Interesados, en el que se valoran los posibles riesgos de las operaciones del tratamiento.

Seudonimización: Tratamiento de datos personales, de tal manera que no puedan atribuirse a un Interesado en particular sin recurrir a información adicional, siempre que dicha información adicional se mantenga separada y sujeta a medidas técnicas u organizativas y no esté vinculada a personas identificadas o que puedan identificarse.

Actos delegados: El artículo 290 del TFUE permite que el legislador de la UE (generalmente, el Parlamento Europeo y el Consejo) delegue en la Comisión la facultad de adoptar actos no legislativos de alcance general que complementen o modifiquen determinados elementos no esenciales de un acto legislativo.

Autoridad de Control: Autoridad Pública independiente establecida por un estado miembro. Cada estado miembro puede disponer de una o varias autoridades públicas independientes que se encarguen de supervisar la aplicación del RGPD dentro de su territorio. En el caso de España, la Autoridad de Control es la Agencia Española de Protección de Datos (AEPD).

Brecha de seguridad: Pérdida intencionada o no intencionada de información recogida, que contenga datos de carácter personal, así como su revelación a terceros que no tengan acceso legítimo a dichos datos. Destrucción accidental o ilícita, pérdida, alteración, comunicación no autorizada o acceso a datos personales transmitidos, conservados o tratados de forma distinta a la finalidad inicial.

2. Controles periódicos de verificación de cumplimiento

La veracidad de los datos contenidos en los Anexos de este documento, así como el cumplimiento de las normas que **contiene deberá ser periódicamente comprobado**, de forma que puedan detectarse y subsanarse anomalías.

El Responsable Tratamiento comprobará, con una periodicidad al menos trimestral, que la **lista de usuarios autorizados** en el **Apartado 4. F** se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso a datos y perfiles, para lo que recabará la lista de usuarios y sus códigos de acceso al administrador o administradores del Sistema. Además de estas comprobaciones periódicas, el administrador comunicará al Responsable Tratamiento, en cuanto se produzca, cualquier alta o baja de usuarios con acceso autorizado a datos.

Se comprobará al menos con periodicidad semestral, por los Administradores del Sistema, **la existencia de copias de respaldo** que permitan la recuperación de los Datos según lo estipulado en el apartado 4 G de este documento, enviando evidencias de esta comprobación al Responsable Tratamiento

A su vez, y también con periodicidad al menos semestral, los Administradores del Sistema comunicaran al Responsable de Tratamiento **cualquier cambio que se haya realizado en los datos técnicos del Documento**, como por ejemplo cambios en el software o hardware, base de datos o aplicación de acceso a datos, procediendo igualmente a la actualización de dichos apartados en el documento.

El responsable del tratamiento, o la persona autorizada, **analizará la información registrada en el registro de incidencias**, tomando las medidas oportunas.

El responsable de seguridad, verificará, con periodicidad al menos trimestral, el cumplimiento de lo previsto en relación con las **entradas y salidas de datos**, sean por red o en soporte magnético.

El responsable del Tratamiento junto con el de seguridad, analizarán con periodicidad al menos trimestral las **incidencias registradas en el libro correspondiente**, para independientemente de las medidas particulares que se hayan adoptado en el momento que se produjeron, adoptar las medidas correctoras que limiten esas incidencias en el futuro.

Para las Actividades de Tratamiento de nivel medio, al menos cada dos años **se realizará una Auditoría**, externa o interna, que dictamine el correcto cumplimiento y la adecuación de las medidas del presente documento de seguridad o las exigencias del Reglamento de Seguridad, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los informes de auditoría serán analizados por el Responsable de Seguridad, quien propondrá al Responsable de Tratamiento las medidas correctoras correspondientes.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad sin que se deba permitir, en ningún caso, la desactivación de los mismos.

El responsable de Seguridad se encargará de revisar periódicamente la información de control registrada y **elaborará un informe de las revisiones realizadas y los problemas detectados** al menos una vez al mes.

Los resultados de todos estos controles periódicos, así como de las auditorías, serán adjuntados a este documento de seguridad en el **Apartado 4. I.**

3. ANALISIS DE RIESGOS Y EVALUACIÓN DE IMPACTO

3.1 ANÁLISIS DE RIESGOS

El análisis de riesgos constituye el paso previo a la realización de la evaluación de impacto de la protección de datos personales, y consiste en realizar un análisis de los tratamientos de datos personales, atendiendo especialmente a los ciclos de vida de los datos, sus usos previstos, las finalidades para las que se tratarán, las tecnologías utilizadas y la identificación de los usuarios que accederán a ella. El objeto de este análisis es conocer los riesgos, reales o posibles, existentes para la privacidad.

A grandes rasgos, puede determinarse que los riesgos pueden ser de dos tipos; los que afectan a los interesados, y los que afectan a la organización.

- El riesgo que puede afectar a los interesados cuyos datos son tratados se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de sus datos.
- El riesgo que puede afrontar una organización viene determinado por no haber implantado una correcta política de protección de datos o por haberlo hecho de forma descuidada o errática, sin poner en marcha mecanismos de planificación, implantación, verificación y corrección eficaces.

El RGPD condiciona la adopción de las medidas de responsabilidad activa al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. Se maneja el riesgo de dos maneras:

- En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertades (por ejemplo, Evaluaciones de impacto sobre la Protección de Datos).
- En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve (por ejemplo, con las medidas de Protección de Datos desde el Diseño o con las medidas de seguridad).

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de:

- los tipos de tratamiento,
- la naturaleza de los datos,
- el número de interesados afectados,
- la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

El análisis deberá dar respuesta a cuestiones como las que se exponen a continuación:

- ¿Se tratan datos sensibles?
- ¿Se incluyen datos de una gran cantidad de personas?
- ¿Incluye el tratamiento la elaboración de perfiles?
- ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?
- ¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las Cosas?

3.2 EVALUACIÓN DE IMPACTO DE LA PROTECCIÓN DE DATOS (EIPD)

La aplicación del RGPD no debe entenderse como la necesaria obligación de realizar la evaluación de impacto de todos los tratamientos que hasta la fecha se vinieran realizando, sino que será necesario atender a las especificidades concretas de cada tratamiento.

La Evaluación de Impacto en la Protección de Datos Personales es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.

El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo “antes del tratamiento” en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Ello implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación.

Sin embargo, sí debiera realizarse una Evaluación cuando, en una operación iniciada con anterioridad a la aplicación del Reglamento, se hayan producido cambios en los riesgos que el tratamiento implica, en relación con los producidos en el momento en que el tratamiento se puso en marcha.

Este cambio en los riesgos puede derivar, por ejemplo, del hecho de que se hayan empezado a aplicar nuevas tecnologías a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén recogiendo más datos, o datos diferentes, de los que en principio se utilizaban para el tratamiento.

No hay que olvidar, que la Evaluación de Impacto (EIPD) es una herramienta con carácter preventivo que debe realizar el Responsable del Tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

En la práctica, permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

El resultado de la EIPD se debe tener en cuenta, necesariamente, a la hora de tomar las decisiones de la viabilidad o no de llevar a cabo el tratamiento de los datos.

3.2.1 QUE DEBE INCLUIR LA EVALUACIÓN DE IMPACTO.

A la hora de realizar la Evaluación de Impacto, se debe disponer de una metodología que considere los requerimientos exigidos en su artículo 35.7 del RGPD, donde se establece que deberá incluir como mínimo:

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

3.2.2 METODOLOGÍA PARA REALIZAR UNA EVALUACIÓN DE IMPACTO.

Una EIPD se compone de una serie de fases que convergen hacia un único objetivo, proporcionar una visión detallada de la gestión de los riesgos relativos a la protección de datos que se realiza durante el ciclo de vida de los datos asociados a las actividades de tratamiento para poder garantizar los derechos y libertades de las personas físicas.

La ejecución de una EIPD implica la consideración de varios factores que permitan establecer una ruta de trabajo, las fases y pasos a seguir para poder realizarla de una forma adecuada.

Antes de realizarla, debemos considerar los siguientes factores:

- ¿Quién debe estar involucrado? (Recursos necesarios y el equipo de trabajo involucrado en la ejecución).
 - Es necesario definir quién va a realizar la Evaluación y que figuras o personas se van a involucrar en la ejecución de la misma (por ejemplo, la realizará el Responsable del Tratamiento, con el asesoramiento del DPD y del Responsable de Seguridad de la información).

- ¿Qué tareas se deben realizar y cómo? (Metodología, actividades a desarrollar e hitos temporales asociados)
 - Una EIPD puede constar de varias fases, por tanto, es importante tener claro cuáles son cada una de las fases y los objetivos y tareas que se deben conseguir en cada una de ellas.
- ¿Qué y cómo documentar el proceso llevado a cabo? (Documentación de análisis, conclusiones y plan de acción)
 - La documentación de las tareas, análisis y evaluaciones realizadas, así como las conclusiones obtenidas, deben ser documentadas. Es importante mantener trazabilidad de las acciones realizadas y disponer de una base que justifique las conclusiones o decisiones tomadas.

Esta metodología se compone de 3 secciones diferenciadas que, a su vez, se desglosan en diferentes tareas:

1. Contexto:

- **Describir el ciclo de vida de los datos:** Descripción detallada del ciclo de vida y del flujo de datos en el tratamiento. Identificación de los datos tratados, intervinientes, terceros, sistemas implicados y cualquier elemento relevante que participe en la actividad de tratamiento.
- **Analizar la necesidad y proporcionalidad del tratamiento:** Análisis de la base de legitimación, la finalidad y la necesidad y proporcionalidad del tratamiento que se pretenden llevar a cabo.

2. Gestión de riesgos:

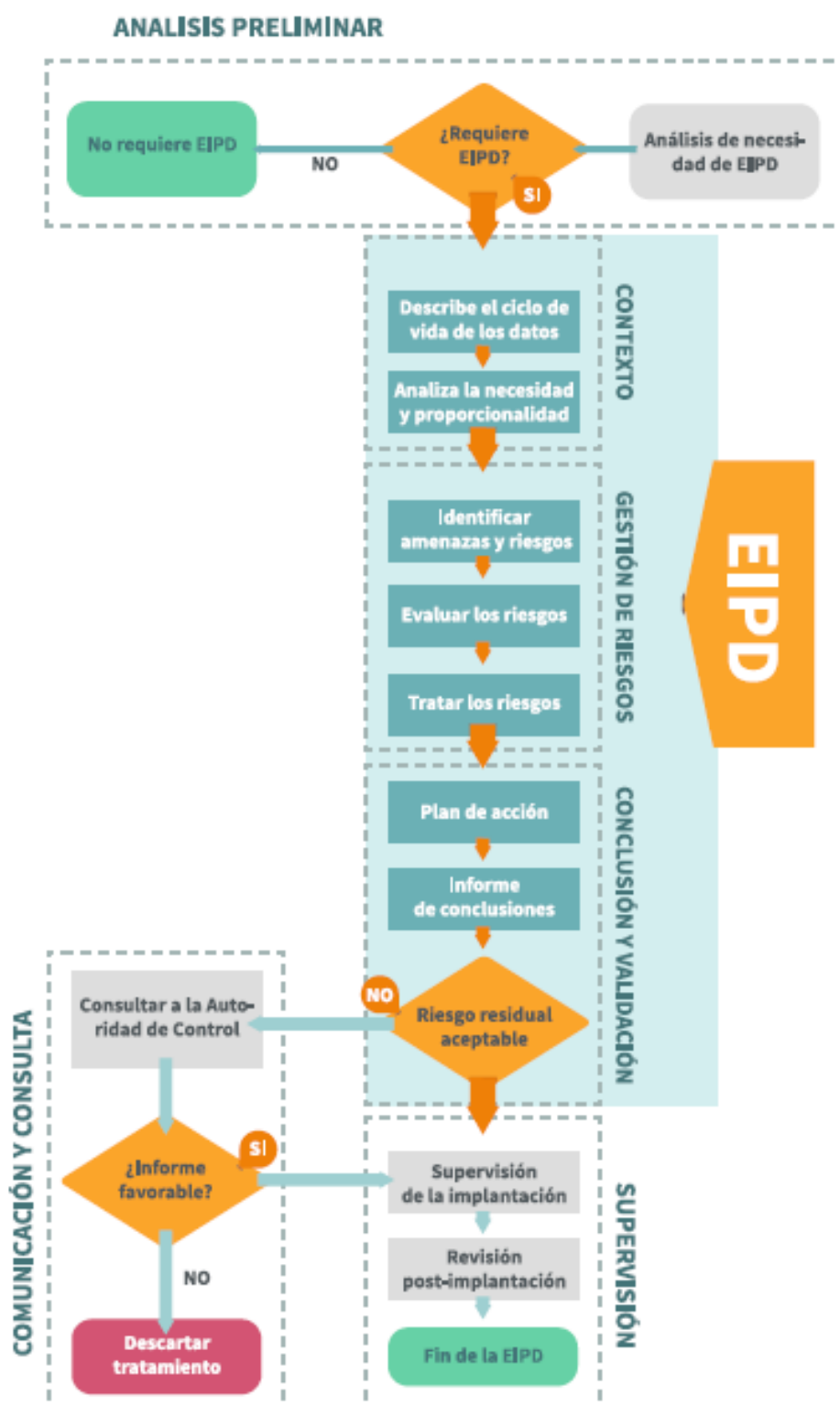
- **Identificar amenazas y riesgos:** Identificación de las amenazas y riesgos potenciales a los que están expuestas las actividades de tratamiento.
- **Evaluar los riesgos:** Evaluación de la probabilidad y el impacto de que se materialicen los riesgos a los que está expuesta la organización.
- **Tratar los riesgos:** Respuesta ante los riesgos identificados con el objetivo de minimizar la probabilidad y el impacto de que estos se materialicen hasta un nivel de riesgo aceptable que permita garantizar los derechos y libertades de las personas físicas.

3. Conclusión y validación:

- **Plan de acción y conclusiones:** Informe de conclusiones de la EIPD donde se documente el resultado obtenido junto con el plan de acción que incluya las medidas de control a implantar para gestionar los riesgos identificados y poder garantizar los derechos y libertades de las personas físicas y, si procede, el resultado de la consulta previa a la autoridad de control a la que se refiere el artículo 36 del RGPD.

Adicionalmente a estas fases, es recomendable que exista un proceso de supervisión y revisión de la implantación o puesta en marcha del nuevo tratamiento con el objetivo de garantizar la implantación de las medidas de control descritas en el Plan de acción.

Esquema de la Evaluación de impacto



3.2.3 EQUIPO DE TRABAJO

La obligación, en su caso, de realizar la Auditoría corresponde al Responsable de Tratamiento, y para ello se recomienda la creación de un equipo o grupo de trabajo interdisciplinar que se encargue de obtener la información necesaria para un correcto desarrollo de la EIPD

Hay que hacer hincapié en que dicho equipo, para que pueda tener éxito en su labor, debe contar con el apoyo y el compromiso de la alta dirección de la organización, ya que sin ellos es muy difícil que sus tareas se puedan desarrollar adecuadamente.

No existen reglas fijas sobre quién debería participar en el grupo o liderarlo, pues dependerá mucho de la organización de que se trate, su tamaño, estructura, etc., así como del proyecto que se vaya a evaluar.

En el Apartado 2 del Artículo 35 del Reglamento General (UE) 2016/679 de Protección de Datos dice:

“El responsable del tratamiento recabará el asesoramiento del Delegado de Protección de Datos (DPD), si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos”.

Es importante destacar que el DPD no es una figura de obligado nombramiento. El RGPD establece los supuestos en los cuales se considera obligatorio disponer de DPD. Sin embargo, las organizaciones que llevan a cabo tratamientos que, por su número o por sus características, impliquen un cierto grado de complejidad, deberían contar con el asesoramiento técnico adecuado para estar en condiciones de cumplir con el RGPD y poder demostrarlo. Por ello, resultaría recomendable que estas organizaciones designen un DPD que pueda proporcionar este asesoramiento.

En cualquier caso, sí se pueden ofrecer unas directrices sobre quiénes no podrían faltar en el mismo:

- El Responsable de Tratamiento (Responsable de Dirección o un representante –con capacidad de decisión)
- El Responsable de Seguridad
- El Delegado de protección de datos (DPD) o la persona que ejerza esta responsabilidad (o el asesor externo al que se le haya confiado esta misión).
- Representantes cualificados del departamento TIC y de las áreas o departamentos a los que más afecte el proyecto dentro de la organización.

3.2.4 PLANTILLA DE ANÁLISIS DE RIESGOS

El siguiente cuestionario pretende analizar si en el tratamiento de datos concurren circunstancias y situaciones que obliguen a realizar una Evaluación de Impacto.

TIPOLOGÍA DE DATOS Y ASPECTOS GENERALES	SI	NO	NO APLICA	Evidencias/ Observaciones
Se van a tratar datos Personales	X			
Se van a Tratar Datos Especialmente Protegidos		X		
La transmisión de datos de nivel alto a través de redes de comunicación es mediante sistemas de cifrado eficaces	X			
Existe un Registro de Actividades / Documento de Seguridad	X			
Está el contenido adecuado a la normativa vigente	X			
Clasificación Adecuada del Nivel de Seguridad.	X			
Existen avisos y Clausulas para la información de los afectados por el tratamiento de datos de carácter personal.	X			
Están los avisos y clausulas adaptados a la normativa vigente	X			
Posibilita el ejercicio de los derechos	X			
FINALIDADES DEL TRATAMIENTO	SI	NO	NO APLICA	Evidencias/ Observaciones
El tratamiento involucra contacto con los interesados de forma intrusiva en su privacidad		X		
La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad		X		
Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones		X		
El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados		X		
El tratamiento implica que un elevado número de personas que no participe en el tratamiento tenga acceso a los datos personales tratados		X		
Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.		X		
ENCARGADOS DE TRATAMIENTO	Si	No	No Aplica	Evidencias Observaciones
Existen Encargados del tratamiento	X			
Están formalizados los contratos según el RGPD	X			
Consta en el contrato el compromiso de confidencialidad del personal del Encargado del tratamiento	X			
Se identifica las Actividades de tratamiento a los que accede el encargado del tratamiento	X			
Se autoriza expresamente el tratamiento fuera de los locales del responsable o el acceso Remoto.	X			

DOCUMENTO DE PROTECCIÓN DE DATOS

RAXIA FORMACIÓN S.L.



PRESTACIÓN DE SERVICIO SIN ACCESO A DATOS	Si	No	No Aplica	Evidencias /Observaciones
Existen medidas para limitar el acceso del personal no autorizado a los datos personales, soportes y recursos	X			
En caso de personal ajeno. Existe un contrato con la prohibición expresa de acceso a datos y confidencialidad en caso incidental o necesario			X	
FUNCIONES Y OBLIGACIONES DEL PERSONAL	Si	No	No Aplica	Evidencias/ Observaciones
Se identifica y existe nombramiento Responsable o Responsables de seguridad	X			
Se identifica y existe nombramiento Administrador o Administradores del Sistema	X			
Funciones y Obligaciones del personal con acceso a datos claramente definidas	X			
Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones	X			
Conoce las consecuencias del incumplimiento	X			
Contratos y compromisos firmados y actualizados.	X			
REGISTRO DE INCIDENCIAS	Si	No	No Aplica	Evidencias/Observaciones
Existe un procedimiento para la notificación y gestión de incidencias	X			
Existe un registro de incidencias con todos los datos exigidos por el reglamento	X			
Se revisan periódicamente y se adoptan las medidas correctoras necesarias	X			
IDENTIFICACIÓN Y AUTENTIFICACIÓN	Si	No	No Aplica	Evidencias/Observaciones
Se identifica de forma única e inequívoca y personalizada a cada usuario	X			Usuario y contraseña
Existe un procedimiento de asignación y almacenamiento de contraseñas	x			
Se limita el intento reiterado de accesos no autorizados al sistema	X			A tres intentos
CONTROL Y REGISTROS DE ACCESO	Si	No	No Aplica	Evidencias/Observaciones
Existen mecanismos para impedir accesos no autorizados	X			
Existe una relación de usuarios actualizada donde se reflejan los tratamientos a los que están autorizados			X	
Los accesos autorizados a usuarios son exclusivos a datos y recursos necesarios para el desarrollo de sus funciones	X			
Existe un registro de accesos			X	
Recoge este registro la información mínima exigida en el reglamento (Identificación del Usuario, Fecha y Hora en la que se realizó el acceso, fichero accedido, tipo de acceso y si ha sido autorizado o denegado)	X			
COPIAS DE RESPALDO Y RECUPERACIÓN	Si	No	No Aplica	Evidencias/Observaciones
Se realizan las copias de seguridad, al menos, con la periodicidad que marca la normativa Vigente	X			
Se verifica cada seis meses el correcto funcionamiento del sistema de copias de respaldo y su recuperación	X			
Se conserva la copia de seguridad en lugar diferente a los equipos que tratan datos	X			
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	Si	No	No Aplica	Evidencias/Observaciones
Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo	X			A los Encargados de Tratamiento
Se realizan transferencias internacionales de datos a países fuera de la Unión Europea.		X		

ANÁLISIS DE RIESGO
CONCLUSIONES / OBSERVACIONES
<p>Tras la presente Auditoría, RAXIA FORMACIÓN S.L. ha sido adaptada a la normativa vigente en Protección de datos, y tiene elaborado documento de seguridad, posee clausulados, la posibilidad del ejercicio de derechos, contratos de confidencialidad y compromisos con los empleados/as, y contratos con los encargados con Encargados de Tratamiento.</p> <p>RAXIA FORMACIÓN S.L. no trata datos sensibles/especialmente protegidos. Realiza las copias de seguridad de sus datos conforme a lo establecido en la normativa vigente y no realiza transferencias internacionales de datos.</p> <p>Posee un Registro de Actividades, según marca el Reglamento General (UE) 2016/679 de protección de datos, así como los nombramientos de Responsable de Seguridad y Administrador del Sistema.</p> <p>Desde AYS INNOVA concluimos que:</p> <p>Riesgo RG-01-01: Pérdida por Incumplimiento de la Legislación sobre Datos Personales <i>Probabilidad: Baja (0-33%) Impacto: Bajo Nivel de Riesgo: BAJO</i></p> <p>Riesgo RG-01-03: Pérdidas por Carencia de Medidas de Seguridad. <i>Probabilidad: Baja (0-33%) Impacto: Bajo Nivel de Riesgo: BAJO</i></p> <p>Riesgo RG-01-04: Deficiente Gestión de la Privacidad. <i>Probabilidad: Baja (0-33%) Impacto: Bajo Nivel de Riesgo: BAJO</i></p>



AYS INNOVA, S.L

4. A Descripción detallada de la estructura física de las Actividades de Tratamiento

Nombre: GESTIÓN CLIENTES

Responsable del Tratamiento

Nombre	RAXIA FORMACIÓN S.L.	C.I.F.	B 70.576.475
Dirección	Rúa das Cerdeiras, s/n	C.P.	15841
Localidad	Santa Comba	Provincia	A Coruña
Teléfono	981 561 890	E-mail	admin@raxiaformacion.es

Base Jurídica

Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. RGPD artículo 6.1b

Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD artículo 6.1c

Finalidad

Gestión de clientes contable, fiscal y administrativa; Publicidad y Prospección Comercial; Otro tipo de finalidad.

Colectivo

Procedencia de los datos	El propio interesado o su representante legal;
Colectivos o categorías de interesados	Cliente y usuarios; Personas de contacto.

Categoría de datos

Categorías especiales de datos

Datos de carácter identificativo	Nombre y apellidos; DNI/NIF; Dirección; Número teléfono, firma y correo electrónico.
Otros datos tipificados	Características personales; Información comercial; Transacciones de bienes y servicios; Económicos, financieros y de seguros.

Categoría de destinatarios

Organizaciones o personas directamente relacionadas con el responsable; Administración tributaria; Bancos, cajas de ahorros y cajas rurales; Administración pública con competencia en la materia; Otros órganos de la administración pública; Entidades aseguradoras.

Transferencia Internacional de Datos

Plazo de Supresión

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron así como los previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

Responsables de Seguridad

Raquel Estévez Pombo

Administradores del Sistema

MANTENIMIENTOS INFORMÁTICOS NOROESTE, S.L.

Delegado de Protección de Datos

Ejercicio de derechos

Unidad	Departamento administración
Dirección	La misma que la de ubicación de la actividad de tratamiento
Procedimiento	Una vez recibida la solicitud, será inmediatamente comunicada al Responsable de Seguridad

Nombre: GESTIÓN PROVEEDORES

Responsable del Tratamiento

Nombre	RAXIA FORMACIÓN S.L.	C.I.F.	B 70.576.475
Dirección	Rúa das Cerdeiras, s/n	C.P.	15841
Localidad	Santa Comba	Provincia	A Coruña
Teléfono	981 561 890	E-mail	admin@raxiaformacion.es

Base Jurídica

Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. RGPD artículo 6.1b

Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD artículo 6.1c

Finalidad

Gestión contable, fiscal y administrativa; Otro tipo de finalidad.

Colectivo

Procedencia de los datos	El propio interesado o su representante legal;
Colectivos o categorías de interesados	Proveedores; Personas de contacto.

Categoría de datos

Categorías especiales de datos

Datos de carácter identificativo	Nombre y apellidos; DNI/NIF; Dirección; Número teléfono, firma y correo electrónico.
Otros datos tipificados	Características personales; Información comercial; Transacciones de bienes y servicios; Económicos, financieros y de seguros.

Categoría de destinatarios

Organizaciones o personas directamente relacionadas con el responsable; Administración tributaria; Bancos, cajas de ahorros y cajas rurales; Administración pública con competencia en la materia; Otros órganos de la administración pública; Entidades aseguradoras.

Transferencia Internacional de Datos

Plazo de Supresión

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron así como los previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

Los datos económicos de esta actividad de tratamiento se conservarán al amparo de lo dispuesto en la normativa legal de aplicación (Código de Comercio y Ley General Tributaria)

Responsables de Seguridad

Raquel Estévez Pombo

Administradores del Sistema

MANTENIMIENTOS INFORMÁTICOS NOROESTE, S.L.

Delegado de Protección de Datos

Ejercicio de derechos

Unidad	Departamento administración
Dirección	La misma que la de ubicación de la actividad de tratamiento
Procedimiento	Una vez recibida la solicitud, será inmediatamente comunicada al Responsable de Seguridad

Nombre: GESTIÓN RECURSOS HUMANOS

Responsable del Tratamiento

Nombre	RAXIA FORMACIÓN S.L.	C.I.F.	B 70.576.475
Dirección	Rúa das Cerdeiras, s/n	C.P.	15841
Localidad	Santa Comba	Provincia	A Coruña
Teléfono	981 561 890	E-mail	admin@raxiaformacion.es

Base Jurídica

Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. RGPD artículo 6.1b

Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD artículo 6.1c

Real Decreto Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y lucha contra la precariedad laboral en la jornada de trabajo.

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social

Ley 58/2003, de 17 de diciembre, General Tributaria

Finalidad

Gestión integral de procesos de Recursos humanos, contrataciones, bajas, conceptos, retribuciones; prevención de riesgos laborales, gestión de personal; control horario; Formación

Colectivo

Procedencia de los datos	El propio interesado o su representante legal
Colectivos o categorías de interesados	Empleados.

Categoría de Datos

Categorías especiales de Datos	Datos de salud (bajas por enfermedad, accidentes laborales y grado de discapacidad, sin inclusión de diagnósticos); afiliación sindical, a los exclusivos efectos del pago de cuotas sindicales (en su caso); representante sindical (en su caso)
Datos de carácter identificativo	Nombre y apellidos; DNI; Dirección; Número SS; Imagen/ voz; Teléfono; Firma y correo electrónico.
Otros datos tipificados	Características personales, académicas y profesionales; detalles de empleo; económicos, financieros y de seguros; transacciones de bienes y servicios; circunstancias sociales.

Categorías de destinatarios

Organizaciones o personas directamente relacionadas con el responsable; organismos de la Seguridad Social; Administración Tributaria; Bancos, cajas de ahorros y cajas rurales; entidades aseguradoras. Administración pública con competencia en la materia.

Transferencia Internacional de Datos

Plazo de Supresión

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron así como los previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

Los datos económicos de esta actividad de tratamiento se conservarán al amparo de lo dispuesto en la Ley 58/2003, del 17 de diciembre, General Tributaria

Responsables de Seguridad

Raquel Estévez Pombo

Administradores del Sistema

MANTENIMIENTOS INFORMÁTICOS NOROESTE, S.L.

Delegado de Protección de Datos

Ejercicio de derechos

Unidad	Departamento administración
Dirección	La misma que la de ubicación de la actividad de tratamiento
Procedimiento	Una vez recibida la solicitud, será inmediatamente comunicada al Responsable de Seguridad

Nombre: GESTIÓN DE NÓMINAS

Responsable del Tratamiento

Nombre	RAXIA FORMACIÓN S.L.	C.I.F.	B 70.576.475
Dirección	Rúa das Cerdeiras, s/n	C.P.	15841
Localidad	Santa Comba	Provincia	A Coruña
Teléfono	981 561 890	E-mail	admin@raxiaformacion.es

Base Jurídica

Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. RGPD artículo 6.1b

Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. RGPD artículo 6.1c

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social

Ley 58/2003, de 17 de diciembre, General Tributaria

Finalidad

Gestión y emisión de la nómina, así como de todos los productos derivados de la misma.

Colectivo

Procedencia de los datos	El propio interesado o su representante legal
Colectivos o categorías de interesados	Empleados.

Categoría de Datos

Categorías especiales de Datos	Datos de salud (bajas por enfermedad, accidentes laborales y grado de discapacidad, sin inclusión de diagnósticos); afiliación sindical, a los exclusivos efectos del pagos de cuotas sindicales (en su caso); representante sindical (en su caso)
Datos de carácter identificativo	Nombre y apellidos; DNI; Dirección; Número SS; Imagen/ voz; Teléfono; Firma y correo electrónico.
Otros datos tipificados	Características personales, académicas y profesionales; detalles de empleo; económicos, financieros y de seguros; transacciones de bienes y servicios; circunstancias sociales.

Cesión Categorías de destinatarios

Organizaciones o personas directamente relacionadas con el responsable; organismos de la Seguridad Social; Administración Tributaria; Bancos, cajas de ahorros y cajas rurales; entidades aseguradoras. Administración pública con competencia en la materia.

Transferencia Internacional de Datos

Plazo de Supresión

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron así como los previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

Los datos económicos de esta actividad de tratamiento se conservarán al amparo de lo dispuesto en la Ley 58/2003, del 17 de diciembre, General Tributaria

Responsables de Seguridad

Raquel Estévez Pombo

Administradores del Sistema

MANTENIMIENTOS INFORMÁTICOS NOROESTE, S.L.

Delegado de Protección de Datos

Ejercicio de derechos

Unidad	Departamento administración
Dirección	La misma que la de ubicación de la actividad de tratamiento
Procedimiento	Una vez recibida la solicitud, será inmediatamente comunicada al Responsable de Seguridad

Nombre: CURRICULUM VITAE

Responsable del Tratamiento

Nombre	RAXIA FORMACIÓN S.L.	C.I.F.	B 70.576.475
Dirección	Rúa das Cerdeiras, s/n	C.P.	15841
Localidad	Santa Comba	Provincia	A Coruña
Teléfono	981 561 890	E-mail	admin@raxiaformacion.es

Base Jurídica

Tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales. RGPD artículo 6.1b

El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos RGPD 6.1.a)

Finalidad

Gestión de los aspirantes a un empleo en la organización; Gestión de bolsas de empleo y de selección; evaluación de candidatos para puestos de personal de la organización.

Colectivo

Procedencia de los datos	El propio interesado o representante legal; Entidad privada; Administraciones públicas.
Colectivos o categorías de interesados	Solicitantes

Estructura

Datos especialmente protegidos

Datos de carácter identificativo

Nombre y Apellidos; Nif / Dni, Dirección, Imagen/ Voz; Teléfono, Firma, Correo electrónico y datos suministrados por el solicitante en el curriculum.

Otros datos tipificados

Características personales; circunstancias sociales; Académicos y profesionales; detalles de empleo.

Cesión o comunicación de datos

Administración pública con competencia en la materia.

Transferencia Internacional de Datos

Plazo de Supresión

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron así como los previstos por la legislación fiscal respecto a la prescripción de responsabilidades.

Responsables de Seguridad

Raquel Estévez Pombo

Administradores del Sistema

MANTENIMIENTOS INFORMÁTICOS NOROESTE, S.L.

Delegado de Protección de Datos

Ejercicio de derechos

Unidad	Departamento administración
Dirección	La misma que la de ubicación de la actividad de tratamiento
Procedimiento	Una vez recibida la solicitud, será inmediatamente comunicada al Responsable de Seguridad

4. B Encargados del tratamiento

El responsable del tratamiento debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del responsable.

El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento.

Dicho contrato establecerá expresamente que el encargado del tratamiento tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que no los comunicará ni siquiera para su conservación a otras personas.

Para demostrar que el encargado ofrece garantías suficientes, el RGPD prevé la adhesión a códigos de conducta o la posesión de un certificado de protección de datos como mecanismos de prueba.

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico.

En este contrato como mínimo debe establecerse 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.

El contrato estipulará las medidas de seguridad a que se refieren los artículos 6, 20.2 y 40 del RGPD, que el encargado del tratamiento está obligado a implementar.

Consultoría en Protección de Datos				
Nombre	AYS INNOVA, S.L		C.I.F.	B 70.310.255
Dirección	Hedras, 6 1º Q		C.P.	15.895
Localidad	Milladoiro - Ames		Provincia	A Coruña
Teléfono	881 819 799	Fax	E-mail	rgpd@aysinnova.es
Actividad:	Consultoría en Protección de Datos			
GESTIÓN PROVEEDORES				
Permisos	Consulta bajo entrega, siempre vinculada a la prestación de servicios de consultoría en RGPD			
Accesos	Bajo entrega			
Forma de servicio	En el local de responsable, en su propio local			
GESTIÓN RECURSOS HUMANOS				
Permisos	Consulta bajo entrega, siempre vinculada a la prestación de servicios de consultoría en RGPD			
Accesos	Bajo entrega			
Forma de servicio	En el local de responsable, en su propio local			

Asesoría Fiscal, Contable y Laboral			
Nombre	ASESORÍA ESPIÑEIRA (IVÁN ESPIÑEIRA)		N.I.F. 33209847D
Dirección	C/ Puente de Sar, 43 - A bajo A Pl. Pepe Noya		C.P. 15702
Localidad	Santiago de Compostela		Provincia A Coruña
Teléfono	981561864	Fax	E-mail laboral@espineira.es
Actividad	Asesoría laboral, fiscal y contable		
GESTIÓN CLIENTES			
Permisos	Consulta, modificación, borrado, copia, e-mail		
Accesos	Acceso físico y lógico a ficheros, almacenes		
Forma de servicio	En el local de responsable, en su propio local		
GESTIÓN PROVEEDORES			
Permisos	Consulta, modificación, borrado, copia, e-mail		
Accesos	Acceso físico y lógico a ficheros, almacenes		
Forma de servicio	En el local de responsable, en su propio local		
GESTIÓN NÓMINAS			
Permisos	Consulta, modificación, borrado, copia, e-mail		
Accesos	Acceso físico y lógico a ficheros, almacenes		
Forma de servicio	En el local de responsable, en su propio local		

PREVENCION DE RIESGOS LABORALES

Nombre	INTECTOMA, S.L.	C.I.F.	B24277493
Dirección	C/ Torres Quevedo, 3 bajo	C.P.	24400
Localidad	Ponferrada	Provincia	León
Teléfono	881966033	Fax	
		E-mail	administracion@intectoma.com
Actividad	Prevención de riesgos laborales		

GESTION DE RECURSOS HUMANOS

Permisos	Consulta, modificación, borrado, copia, e-mail
Accesos	Acceso físico y lógico a ficheros, almacenes
Forma de servicio	En el local de responsable, en su propio local

Mantenimiento informático			
Nombre	MANTENIMIENTOS INFORMÁTICOS NOROESTE S.L.	C.I.F.	B56827686
Dirección	Rúa Habitat Puente Pasaje Portal 2, bajo 2B	C.P.	15172
Localidad	Oleiros	Provincia	A Coruña
Teléfono	981110071	Fax	
		E-mail	jl.morquillas@mininformatica.com
Actividad	Mantenimiento informático/ Administrador del Sistema		
GESTIÓN CLIENTES			
Permisos	Consulta, modificación, borrado, copia, e-mail		
Accesos	Acceso físico y lógico a ficheros, almacenes		
Forma de servicio	En el local de responsable, en su propio local		
GESTIÓN PROVEEDORES			
Permisos	Consulta, modificación, borrado, copia, e-mail		
Accesos	Acceso físico y lógico a ficheros, almacenes		
Forma de servicio	En el local de responsable, en su propio local		
CURRICULUM VITAE			
Permisos	Consulta, modificación, borrado, copia, e-mail		
Accesos	Acceso físico y lógico a ficheros, almacenes		
Forma de servicio	En el local de responsable, en su propio local		

LICENCIAS, ISOS, CIBERSEGURIDAD			
Nombre	DOOINGIT CIBERSEGURIDAD S.L.		C.I.F. B 70.540.208
Dirección	Rúa das Hedras, 6, local 1E		C.P. 15.895
Localidad	Ames		Provincia A Coruña
Teléfono	981042159	Fax	E-mail paz.carinena@dooingit.com
Actividad	Gestión de licencias, ISOS y Ciberseguridad.		
TODAS LAS ACTIVIDADES DE TRATAMIENTO			
Permisos	Consulta, modificación, borrado, copia, e-mail		
Accesos	Acceso a ficheros, almacenes		
Forma de servicio	En el local de responsable, en su propio local		

El servicio de LIMPIEZA lo realiza LIMPIEZAS GERMANIA, S.L.; accediendo a instalaciones en donde se encuentran datos personales y empresariales.

4. C LOCALES DE TRATAMIENTO DE DATOS

SEDE SOCIAL			
Nombre	RAXIA FORMACIÓN S.L.		
Dirección	Rúa do Rego 6, Bajo D	C.P.	15.895
Localidad	Ames	Provincia	A Coruña
Teléfono	981 561 890	Fax	
		E-mail	admin@raxiaformacion.es
Servidor			
Papel	Archivadores A-Z por fichero, orden alfabético y orden cronológico. Dependencia “almacén”.		
Respaldo	COPIAS DE SEGURIDAD CON VEEAM BACKUP DIARIAS CON RETENCION DE 7 DIAS EN BUCKET S3 WASABI.		
Notas	Acceso al público restringido a recepción. Atención al público en sala de reuniones o en biblioteca, desprovista de ordenadores o archivadores.		

SEDE FISCAL			
Nombre	RAXIA FORMACIÓN S.L.		
Dirección	Rúa das Cerdeiras, s/n	C.P.	15841
Localidad	Santa Comba	Provincia	A Coruña
Teléfono	981 561 890	Fax	
		E-mail	admin@raxiaformacion.es
Servidor			
Papel	Archivadores A-Z por fichero, orden alfabético y orden cronológico. Dependencia “almacén”.		
Respaldo	COPIAS DE SEGURIDAD CON VEEAM BACKUP DIARIAS CON RETENCION DE 7 DIAS EN BUCKET S3 WASABI.		
Notas	Acceso al público restringido a recepción. Atención al público en sala de reuniones o en biblioteca, desprovista de ordenadores o archivadores.		

4. D SOFTWARE Y ENTORNO DE COMUNICACIONES

INVENTARIO DE SOFTWARE		
Ofimática	MICROSOFT OFFICE 365	Descripción: Se emplean las aplicaciones estándar Word y Excel para el tratamiento de los datos personales contenidos en los ficheros.
Contabilidad/ Facturación/ Gestión Integrada	ODOO	Descripción: Odoo es un software de gestión empresarial de código abierto (ERP) que integra múltiples aplicaciones para gestionar todas las áreas de un negocio (ventas, contabilidad, inventario, RRHH, marketing, etc.)
IA	COPILOT MICROSOFT PROFESIONAL (NO BUSSINES)	Descripción: Copilot es un asistente de inteligencia artificial de Microsoft que usa modelos de lenguaje avanzados.
IA	CHATGPT	Descripción: ChatGPT es un chatbot de inteligencia artificial conversacional desarrollado por OpenAI, diseñado para entender, procesar y generar texto similar al humano en respuesta a las indicaciones o "prompts" de los usuarios.

Para tratar las Actividades de tratamiento se utiliza lo siguiente:

- *Microsoft Word y/o Excel, que es una aplicación integrada en Microsoft Office.*
- *Los ordenadores usan un sistema de contraseñas proporcionado por el sistema operativo Microsoft Windows.*
- *El sistema se haya protegido mediante un antivirus ESET XDR, y un firewall/ IDS PFSENSE+SNORT.*

Entorno de comunicaciones

Acceso a Internet vía VODAFONE Fibra.

4. E INVENTARIO DE EQUIPOS Y PERIFÉRICOS

NOMBRE / IDENTIFICADOR / ID PROCESADOR	UBICACIÓN (Local y lugar)	MARCA Y MODELO	SISTEMA OPERATIVO	USUARIOS	PORTATIL/ FIJO
SX013 MP1ZFVWY Intel(R) Core(TM) i5- 1035G1 CPU @ 1.00GHz	AMES	LENOVO 11LA005VSP	WINDOWS 11 PRO	SONIA FACHAL	FIJO
RX007 67389FEW300085W 13th Gen Intel(R) Core(TM) i5-1340P	AMES	SAMSUNG 730QFG	WINDOWS 11 PRO	ISABEL GARCIA	PORTATIL
RX005 0B33X3H23433GP 12th Gen Intel(R) Core(TM) i5-1235U	AMES	SURFACE LAPTOP GO 3	WINDOWS 11 PRO	MARINHA GUIZÁN	PORTATIL

4. F Nombramientos y autorizaciones de los usuarios.

En esta sección figurarán todas las personas nombradas por el responsable, indicando la responsabilidad y la fecha del nombramiento o el cese. Asimismo, se incluirá las autorizaciones de accesos concedidas a los usuarios.

Nombramientos

El Responsable del tratamiento podrá realizar un nombramiento para delegar en otra persona la firma de autorizaciones, en ningún caso esta designación supone una delegación de la responsabilidad que le corresponde.

Cada nombramiento o autorización deberá hacer constar:

El nombre de la persona autorizada.
El tipo de autorización o responsabilidad
La fecha de alta
La fecha de baja en su caso

Podrá haber nombramientos, designados por el responsable del tratamiento para los siguientes tipos de responsabilidades,

1. Responsables que puedan autorizar consultas, altas, bajas, modificaciones de la Actividad de Tratamiento
2. Responsables de Salida Soportes
3. Responsables de Salida por Red
4. Responsable de autorizar el trabajo fuera de los locales
5. Responsables de Entrada de Soportes
6. Responsables de Seguridad, si existen varios, se indicarán las Actividades/ ficheros y tratamientos asignados

Autorizaciones de accesos a Usuarios

Las autorizaciones de accesos de usuarios, deberán ser realizadas por el Responsable del tratamiento o la persona en la que delegue, constarán del nombre del usuario, el perfil y los recursos a los que se concede el acceso, así como el nombre y cargo de la persona que realiza la autorización.

1. El nombre del Usuario o de la persona autorizada.
2. Perfil
3. El tipo de privilegio de acceso
4. La fecha de alta
5. La fecha de baja, o de modificación en su caso
6. El nombre y cargo de la persona que realiza la autorización

Se incluirán estas autorizaciones o bien se referenciará la herramienta o recurso que permita obtenerlas puntual y/o periódicamente.

ADMINISTRADOR DEL SISTEMA

Nombre y apellidos	MANTENIMIENTOS INFORMÁTICOS NOROESTE, S.L.	NIF	B56827686
Cargo	Mantenimiento informático		
Actividad de Tratamiento	Todas. Ver apartado correspondiente		
Permisos	Total (recogida, consulta, modificación, borrado, copia, adjuntos e-mail)		
Accesos	Acceso físico y a ficheros, acceso al almacén soportes, acceso al almacén documentos		

RESPONSABLE DE SEGURIDAD

Nombre y apellidos	Raquel Estévez Pombo	DNI	44.821.234-F
Cargo	Administración		
Actividad de Tratamiento	Todas. Ver apartado correspondiente		
Permisos	Total (recogida, consulta, modificación, borrado, copia, adjuntos e-mail)		
Accesos	Acceso físico y a ficheros, acceso al almacén soportes, acceso al almacén documentos		

USUARIO 1

Nombre y apellidos	RAQUEL ESTÉVEZ POMBO	DNI	44821234F
Cargo	CEO/RRHH/ DPTO. FINANCIERO	Alta	
		Baja	
Actividad de Tratamiento	Todas		
Permisos	Total (recogida, consulta, modificación, borrado, copia, adjuntos e-mail)		
Accesos	Acceso físico y a ficheros, acceso al almacén soportes, acceso al almacén documentos		

USUARIO 2

Nombre y apellidos	HÉCTOR TEJIDO VIÑA	DNI	72396959C
Cargo	CEO/CONSEJERO/DPTO. FINANCIERO	Alta	
		Baja	
Actividad de Tratamiento	Todas		
Permisos	Total (recogida, consulta, modificación, borrado, copia, adjuntos e-mail)		
Accesos	Acceso físico y a ficheros, acceso al almacén soportes, acceso al almacén documentos		

USUARIO 3

Nombre y apellidos	Isabel García Vila	DNI	33307570M
Cargo	Directora Formación	Alta	
		Baja	
Actividad de Tratamiento	Clientes y/o proveedores		
Permisos	Total (recogida, consulta, modificación, borrado, copia, adjuntos e-mail)		
Accesos	Acceso físico y a ficheros, acceso al almacén soportes, acceso al almacén documentos		

USUARIO 4

Nombre y apellidos	Marinha Guizan Cascon	DNI	45845760K
Cargo	Técnico proyectos	Alta	
Actividad de Tratamiento	Clientes y/o proveedores	Baja	
Permisos	Total (recogida, consulta, modificación, borrado, copia, adjuntos e-mail)		
Accesos	Acceso físico y a ficheros, acceso al almacén soportes, acceso al almacén documentos		

USUARIO 5

Nombre y apellidos	Sonia Fachal Crespo	DNI	78793340D
Cargo	Administrativa	Alta	
Actividad de Tratamiento	Clientes y/o proveedores	Baja	
Permisos	Total (recogida, consulta, modificación, borrado, copia, adjuntos e-mail)		
Accesos	Acceso físico y a ficheros, acceso al almacén soportes, acceso al almacén documentos		

4.G Procedimientos de control, copias de seguridad, cuentas de correo electrónico y usuarios

1. Procedimiento para dar altas, baja o modificación de acceso a usuarios

Cada alta de autorización deberá estar aprobada por el Responsable del Tratamiento o persona autorizada, conteniendo el nombre y datos identificativos del usuario, el fichero, los sistemas de información y/o recursos a los que accede, y el perfil de acceso (tipo de usuario).

2. Procedimiento de control de identificación y autenticación

Asignación de códigos de usuario

Cada usuario tendrá un solo código para acceder al sistema operativo. Los usuarios serán responsables ante **RAXIA FORMACIÓN S.L.** de todas las actividades y accesos que se realicen con sus códigos de usuario, por lo que está expresamente prohibido ceder o comunicar la contraseña a otros.

Se hace especial hincapié en que la contraseña es personal e intransferible, no puede comunicarse a otros, debe ser distinta para cada usuario y cambiada por una nueva al recibirse la primera atribuida.

Es competencia del Responsable de Seguridad, que la atribución y asignación de contraseñas, así como la custodia de la relación de usuarios se realice de forma que se garantice su confidencialidad e integridad.

El Responsable del Tratamiento o el Responsable de Seguridad, asignará un nombre de usuario y propondrá una contraseña para cada uno de los usuarios, que, tras el primer acceso, vendrán obligados a cambiarlas.

Cada usuario podrá intentar repetir el proceso de introducción de contraseñas 3 veces, una vez superado este número de intentos, la cuenta de usuario quedará bloqueada.

Con una periodicidad de cada 12 meses, el Responsable del Tratamiento o Responsable de Seguridad propondrá a los usuarios que cambien su contraseña por una nueva, volviendo a quedar almacenada por una nueva.

Comunicación de códigos de usuario y contraseñas

Se comunicarán a los usuarios mediante correo interno y nunca por teléfono o fax. Los códigos de usuario y las contraseñas tendrán una vigencia máxima de 12 meses.

Autorización de acceso a datos y recursos.

Los usuarios tendrán acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. El Responsable del Tratamiento establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

Archivo de las contraseñas

Durante el tiempo que estén vigentes, las contraseñas se almacenan de forma ininteligible mediante el propio sistema de encriptación que utiliza el sistema operativo. El archivo donde se almacenen las contraseñas estará protegido y bajo la responsabilidad del Administrador del Sistema.

3. Procedimiento de respaldo y recuperación.

Actividades de Tratamiento automatizadas

La seguridad de los datos personales del Fichero no sólo 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 de recuperación** que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos.

Los procedimientos para la **recuperación de los datos** deben garantizar en todo momento su reconstrucción en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción.

Existirá una persona, bien sea el administrador, encargado de tratamiento, o bien otro usuario expresamente designado, que **será responsable de obtener periódicamente una copia de seguridad**, a efectos de respaldo y posible recuperación en caso de fallo. Estas copias deberán realizarse con una **periodicidad, al menos, semanal**,

En caso de **fallo del sistema con pérdida total o parcial de los datos** existirá un procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos al estado en que se encontraban en el momento del fallo. Ese procedimiento está descrito en este documento. Al menos cada seis meses el Responsable del Tratamiento deberá verificar la correcta definición y funcionamiento de los procedimientos de respaldo y recuperación.

Las pruebas anteriores a la implantación o modificación de los sistemas de información

que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se aplique a esos el mismo tratamiento de seguridad, y se deberán relacionarse en el **Apartado 4. A.**

Si se van a **realizar pruebas con datos reales**, deberá realizarse previamente una copia de seguridad.

Para las Actividades de Tratamiento de nivel medio, será necesaria la **autorización por escrito del Responsable del Tratamiento** para la ejecución de los procedimientos de recuperación de los datos, y deberá dejarse constancia en el registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

Para las Actividades de Tratamiento de nivel alto, **deberá conservarse una copia de respaldo** y de los procedimientos de recuperación de los datos **en un lugar diferente de aquel en el que se encuentren los equipos informáticos** que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en el Reglamento, o bien se utilizarán elementos que garanticen la integridad y recuperación de la información de modo que sea posible su recuperación.

Actividades de Tratamiento manuales

Aquellas copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares **deberán cumplir el nivel de seguridad** que les corresponda conforme a los criterios establecidos en el Reglamento vigente.

Toda copia de trabajo será destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación. Esta destrucción se atenderá a las normas para la destrucción de desechos descritas en este documento.

Deberá procederse a la **destrucción de las copias o reproducciones desechadas** de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Para las Actividades de Tratamiento de nivel alto, la generación de copias o reproducción de documentos únicamente podrá ser realizada bajo el **control del personal autorizado en el documento de seguridad**.

Respaldo

La salvaguarda de los datos de carácter personal constituye uno de los aspectos más importantes del Reglamento de Seguridad. La seguridad de los datos personales no sólo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos.

El responsable de la realización de las copias de seguridad es el Administrador del Sistema.

Cuando existen varias copias de un mismo fichero, archivo, grupo de registros, datos, grupo de datos de carácter personal sometidos a control, independientemente del soporte en el que estén, se tratan con el mismo rigor que si fueran copias de seguridad.

Con periodicidad diaria, se realiza una copia de seguridad CON VEEAM BACKUP DIARIAS CON RETENCION DE 7 DIAS EN BUCKET S3 WASABI, que se guarda bajo responsabilidad del Administrador del Sistema.

De esta forma, las copias de seguridad de datos, se realizan cada vez que se actualiza o incorpora a la entidad alguno cuyo contenido contenga datos de carácter personal.

Recuperación

La realización de copias de seguridad tiene como último fin el poder proceder a la recuperación de los datos en el caso de producirse una corrupción o pérdida de los mismos.

La recuperación de los datos se realizará mediante volcado total de los datos contenidos en el disco duro permanente del PC correspondiente.

Finalizado el procedimiento se dejará constancia en el Registro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación, requiriendo autorización expresa del Responsable de Seguridad.

Nombre	
Persona encargada de la operación	
Actividades de las que se restauran los datos	
Metodología seguida	
Fecha y firma del Responsable de Seguridad autorizando dicha recuperación	
Notas adicionales	

4. Procedimiento de gestión de soportes

Entendemos como **Soportes informáticos** aquellos medios de grabación y recuperación de datos que se utilizan para realizar copias.

Dado que la mayor parte de los soportes que hoy en día se utilizan, como, CDs, DVDs o memorias removibles de todo tipo (como memorias flash o “pendrives”), son fácilmente transportables, reproducibles y/o copiables, es evidente la importancia que tiene el **control de estos medios**, para la seguridad de los datos.

En este Anexo se describe el sistema utilizado por la empresa para identificar, inventariar y almacenar en un lugar con acceso restringido, los soportes informáticos distintos de los discos duros insertos en los PC`S que contienen datos de carácter personal.

Los discos duros de los PC que contienen datos de carácter personal se registrarán por el principio de acceso; quien tenga acceso responderá de la información. Si el acceso es libre, responderá quien tenga las llaves de acceso al lugar donde se encuentre el disco duro.

Si el lugar no tiene llave de acceso, responderá el Responsable de Seguridad.

4.1 Identificación de etiquetas

Los soportes que contengan datos de carácter personal, deben ser **etiquetados** para permitir su identificación, conocer de qué actividad de tratamiento se trata, el tipo de información que contienen y la fecha de creación. Estos sistemas de etiquetado **permitirán la identificación de soportes a los usuarios, pero dificultará la identificación para el resto de las personas.**

Los soportes que contengan datos, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique que tipo de datos contiene, proceso que los ha originado y fecha de creación.

En el caso de que la organización lo considerase, podrán utilizarse sistemas de etiquetado en los soportes que contienen información especialmente sensible para la organización, que permitan a los usuarios identificar los citados soportes y la dificulten para el resto de las personas

4.2 Inventario de soportes

El supervisor de soportes, el **Responsable de Seguridad**, llevará una relación detallada de los soportes que contengan datos personales.

En la relación se especificará la situación de cada soporte.

Dicha relación se actualizará una vez al mes, mediante el correspondiente inventario, siempre que exista alguna baja o alta de soportes.

INVENTARIO DE SOPORTES			EDICIÓN	
			Pág. 1 de 1	
			FECHA: 26/01/2026	
Fecha de alta	Soporte	Actividades de Tratamiento	Responsable de custodia	Fecha de baja
Enero 2026	COPIAS DE SEGURIDAD CON VEEAM BACKUP DIARIAS CON RETENCION DE 7 DIAS EN BUCKET S3 WASABI	TODAS	ADMINISTRADOR DEL SISTEMA/ RESPONSIBLE DE SEGURIDAD	

4.3 Lugar de almacenamiento

Se almacenarán los soportes que contengan datos de las Actividades de Tratamiento en lugares a los que únicamente tengan acceso las personas autorizadas en este Documento de Seguridad. Los lugares y controles de acceso físico pertinentes para cumplir esta normativa de seguridad se describen en el apartado correspondiente.

Los soportes utilizados para copias de seguridad se almacenarán en armarios cerrados con llave, en un lugar distinto al de ubicación del servidor.

Los únicos soportes homologados para albergar datos de carácter personal en la empresa son los siguientes:

Disco duro de los PC autorizados como soporte permanente.

Soportes homologados por la empresa para realizar copias de seguridad.

Queda prohibida la utilización de soportes no homologados para albergar datos de carácter personal.

Los ficheros manuales se encuentran guardados en un armario bajo llave, y el responsable de la custodia de dichas llaves son los Administradores del Sistema.

5. Procedimiento de gestión de entrada / salida de soportes

La salida de soportes que contengan datos fuera de los locales donde están ubicadas las Actividades de Tratamiento deberán ser expresamente autorizados por el Responsable de Tratamiento, utilizando para ello el documento adjunto al final de este apartado.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicadas las Actividades de Tratamiento se adoptarán las medidas necesarias para impedir la sustracción, pérdida o acceso indebido a la información durante el transporte.

Para las Actividades de Tratamiento de nivel medio, se mantendrá un **Libro de registro de entradas y salidas**, dónde se guardarán los formularios de entradas/ salidas de soportes, con indicación del tipo de transporte, fecha y hora, número de soportes, tipo de información que contienen, forma de envío., destinatario o persona responsable de la recepción, que deberán estar debidamente autorizados.

Siempre que se proceda al traslado físico de la documentación que contenga datos de carácter personal, deberán adoptarse medidas para impedir el acceso o manipulación de la información objeto de traslado.

La generación de copias o la reproducción de los documentos, únicamente podrá ser realizada bajo el control del personal autorizado en este documento de seguridad.

Para Actividades de Tratamiento de nivel alto, la **distribución de soportes** que contengan datos de carácter personal se realizará cifrando datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte

Los usuarios **están autorizados** para sacar los documentos y soportes magnéticos a los que tienen acceso fuera de los locales bajo el control del Responsable del Tratamiento, teniendo esta autorización una validez anual, esta autorización es renovable automáticamente.

La persona responsable de la recepción de soportes estará debidamente autorizada por el Responsable de Tratamiento

Los responsables de la entrada de soportes son los administradores del sistema (ver apartado correspondiente

Entrada y salida de datos por red y Telecomunicaciones

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, o mediante aplicaciones Web, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales deberá ser autorizada por el Responsable de Tratamiento o la persona autorizada en el Documento de Seguridad.

Con respecto a los documentos también se consideran incluidos en la salida de documentos los siguientes supuestos:

- Envío por **correo electrónico** en el cuerpo del mensaje como adjuntos datos de un fichero o tratamiento.
- Los **faxes** cuando incorporan datos de un fichero o tratamiento.
- Cualquier otro procedimiento tipo **ftp**, descargas desde la **web** o carpetas compartidas, etc.

Todas las entradas y salidas de datos de carácter personal que se efectúen mediante correo electrónico se realizarán desde una única cuenta o dirección de correo controlada por un usuario especialmente autorizado por el Responsable del Tratamiento. Igualmente, si se realiza la entrada o salida de datos mediante sistemas de transferencia de ficheros por red, únicamente un usuario o administrador estará autorizado para realizar esas operaciones.

Se guardarán copias de todos los correos electrónicos que involucren entradas o salidas de datos de las Actividades de Tratamiento, en directorios protegidos y bajo el control del responsable citado. También se guardarán en directorios protegidos, una copia de los recibidos o transmitidos por sistemas de transferencia por red, junto con un registro de la fecha y hora en que se realizó la operación y el destino o el origen del fichero recibido o enviado.

La **transmisión de datos de carácter personal de nivel alto** a través de redes de comunicaciones públicas, ya sea por correo electrónico, transferencia de ficheros o mediante aplicaciones Web, se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

El sistema informático, la red corporativa y los terminales utilizados por cada usuario son propiedad de la empresa.

Ningún mensaje de correo electrónico será considerado como privado. Se considerará correo electrónico tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas y, especialmente, Internet. Todos estos mensajes irán abiertos.

RAXIA FORMACIÓN S.L. se reserva el derecho a revisar, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa y los archivos LOG del servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la organización como responsable civil subsidiario.

Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a la propiedad intelectual e industrial y a control de virus.

Acceso a internet

El uso del sistema informático de la Organización **RAXIA FORMACIÓN S.L.** para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de la organización y los cometidos del puesto de trabajo del usuario.

El acceso a debates en tiempo real es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido.

El acceso a páginas web (www), grupos de noticias y otras fuentes de información como FTP, se limita a aquellos que contengan información relacionada con la actividad de la organización o con los cometidos del puesto de trabajo del usuario.

RAXIA FORMACIÓN S.L. se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.

REGISTRO Y AUTORIZACIÓN DE ENTRADA /SALIDA DE SOPORTES

Fecha y hora de salida del soporte

SOPORTE

Tipo de soporte y número	
Contenido	
Ficheros de donde proceden los datos	
Fecha de creación	

FINALIDADYDESTINO

Finalidad	
Destino	
Destinatario	

FORMADEENVÍO

Medio de envío	
Remitente	
Precauciones para el transporte	

AUTORIZACIÓN

Persona responsable de la entrega	
Persona que autoriza	
Cargo/Puesto	
Observaciones	
Periodicidad	
Firma	

6. Cuentas de correo electrónico autorizadas para enviar

Las únicas cuentas de correo electrónico autorizadas para enviar datos de carácter personal objeto de este documento de seguridad son:

CUENTAS DE CORREO ELECTRÓNICO	
Usuarios Autorizados	Cuenta de Correo
ISABEL GARCÍA VILA	Isabel.garcia@raxiaformacion.es
MARINHA GUIZAN CASCON	Marinha.guizan@raxiaformacion.es
SONIA FACHAL CRESPO	administrativo@raxiaformacion.es
RAQUEL ESTÉVEZ POMBO	admin@raxiaformacion.es

Responsable de transferencias electrónicas

Se nombran responsables de transferencias electrónicas al perfil de administradoras del sistema (ver apartado correspondiente).

7. Procedimiento para la destrucción de desechos informáticos

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados. En este apartado se describirá el método empleado para la destrucción o borrado de los mismos. Como mínimo se deberá exigir el siguiente procedimiento,

Todos los desechos informáticos de cualquier tipo que puedan contener información del Fichero, como CDs, cintas, discos removibles, listados, memorias removibles de cualquier tipo, o incluso los propios ordenadores obsoletos que contengan discos e almacenamiento, deberán ser eliminados o destruidos de acuerdo con el siguiente Procedimiento para la Destrucción de Desechos Informáticos.

Aquellos soportes que se vayan a reutilizar deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables de ningún modo, evitando el acceso a la información contenida o su recuperación posterior.

Los soportes o documentos que se vayan a eliminar deberán ser destruidos o borrados, mediante la adopción de medidas dirigidas a evitar el acceso a la información en el mismo o su recuperación posterior.

Como norma general ningún desecho informático, ya sea listado u otro tipo de soporte, debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

Aquellos informes en papel o CDs que contengan datos de carácter personal más sensible y no sean voluminosos, deberán ser destruidos en una destructora de papel si es que existe en la organización.

En caso de no existir máquina destructora de papel y CDs o en el caso de que los listados e informes sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una compañía de reciclaje que garantice mediante contrato la destrucción de los mismos.

Todos los disquetes y otros soportes removibles desechados deberán ser formateados y entregados para su reutilización al Responsable de Seguridad o al Responsable de Tratamiento. En el caso de que no se vayan a reutilizar deberán ser formateados si se puede, y depositados en los Contenedores confidenciales de la organización para ser entregadas a la empresa encargada de la destrucción de los datos.

Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras instituciones, deberá comunicarse al Responsable de Seguridad para que se formatee el disco duro o se pase un programa especial que elimine de forma segura todos los datos de los discos duros. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpieza, se deberán desmontar los discos duros y depositarlos en el Contenedor de la empresa de reciclaje para su destrucción.

El responsable del fichero 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.

8. Autorización para el uso de PC portátiles

El Reglamento establece que no se realizará trabajo fuera de los locales sin la debida autorización del responsable del fichero. Para ello no se deberá copiar ni transportar información de los sistemas centrales en portátiles o estaciones de trabajo que se encuentren fuera de las oficinas sin la correspondiente autorización del Responsable del Tratamiento.

El tratamiento, acceso y transporte de los datos del fichero en ordenadores portátiles, estará sujeto en todo caso a una autorización expresa del Responsable del Tratamiento o persona delegada, y sujeta a las mismas normas de seguridad que las de un puesto de trabajo fijo.

Se deberán adjuntar en este apartado las autorizaciones explícitas por parte del Responsable del Tratamiento, o persona autorizada, para el trabajo en ordenadores portátiles fuera del local habitual, indicando la identificación de la persona autorizada, la identificación del equipo, el fichero o los datos que contiene, y las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o, pérdida del equipo.

Se cifrarán los datos que contengan los ordenadores portátiles cuando estos se encuentren fuera de las instalaciones que están bajo el control del responsable, si esto no es posible se hará constar las medidas alternativas que se adopten.

4. H Incidencias o Quiebras de Seguridad

El RGPD define las **violaciones de seguridad** de los datos, más comúnmente conocidas como “**quiebras de seguridad**” o **Incidencias**, de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad a la luz del RGPD y deben ser tratadas como el Reglamento establece.

Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la **quiebra o Incidencia** a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las **72 horas** siguientes a que el responsable tenga constancia de ella.

Puede haber casos en que la notificación no pueda realizarse dentro de esas 72 horas, por ejemplo, por la complejidad en determinar completamente su alcance. En esos casos, es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso.

La información puede proporcionarse **de forma escalonada** cuando no sea posible hacerlo en el mismo momento de la notificación.

La notificación ha de incluir un contenido mínimo:

- la naturaleza de la violación
- categorías de datos y de interesados afectados
- medidas adoptadas por el responsable para solventar la quiebra
- si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados

En los casos en que sea probable que la **violación de seguridad entrañe un alto riesgo** para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a los interesados (afectados)

El objetivo de la **notificación a los afectados** es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

El RGPD añade a los contenidos de la notificación las recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra

Se considera que **se tiene constancia de una violación de seguridad cuando** hay una certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance. La mera **sospecha** de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

La valoración del riesgo de la quiebra es distinta del análisis de riesgos previo a todo tratamiento. Esta valoración trata de establecer hasta qué punto el incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede tener, pueden causar daño en los derechos o libertades para los afectados.

Los daños pueden ser materiales o inmateriales, e ir desde la posible discriminación de los afectados como consecuencia de su uso por quien ha accedido a ellos de forma no autorizada hasta usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.

En casos de **quiebras que por sus características pudieran tener gran impacto**, sí podría ser recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

El **criterio de alto riesgo** debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

La **notificación a los interesados no será necesaria** cuando:

- El responsable hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado.
- Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

Gestión y Registro de incidencias

El **mantener un registro de las incidencias o Brechas de Seguridad** que comprometan la seguridad de los datos es una herramienta imprescindible para aplicar las medidas correctoras necesarias, así como posibilitar la prevención de posibles ataques a esa seguridad y la persecución de los responsables de los mismos.

Se habilitará un **registro de incidencias** con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo.

Cualquier usuario que tenga conocimiento de una incidencia es responsable del registro de la misma, si el registro de incidencias está automatizado, o de la notificación por escrito al Responsable de Seguridad o al superior inmediato, si el registro se realiza manualmente.

El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad por parte de ese usuario.

La **notificación o registro de una incidencia** deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma.

El Administrador del Sistema, cubrirá íntegramente el modelo de formulario de incidencias conservándolo en el libro registro de incidencias.

El Responsable de Seguridad habilitará un registro de incidencias a disposición de todos los usuarios, de las Actividades de Tratamiento, de las que es titular la organización.

Este registro tiene la finalidad de registrar en él cualquier incidencia que pueda suponer un peligro para la seguridad de los datos de carácter personal.

Procedimiento de notificación de incidencias

La incidencia se pondrá en conocimiento de Responsable del tratamiento y/o el Responsable de Seguridad, quienes recabarán la información complementaria necesaria en cada caso.

La notificación de la incidencia se hará preferentemente por medio escrito, que deberá contener la siguiente información:

- Fecha y hora en que se produce la incidencia y en que ésta se conoce.
- Descripción del tipo de incidencia.
- Persona que realiza la comunicación.
- Persona a la que se comunica.
- Posibles causas.

Las incidencias notificadas se incorporarán al registro por el Responsable de Seguridad. Éste realizará las gestiones y análisis necesarios para completar la información que pudiera faltar sobre la incidencia y para reparar o minorar los efectos negativos de la incidencia, así como los controles y comunicaciones que sean precisos.

Junto a la información recogida en el formulario, el Responsable de Seguridad deberá completar en el registro de incidencias la siguiente:

- Efectos derivados de la incidencia.
- Medidas adoptadas y controles implantados o reforzados.
- Fecha de “cierre” de la incidencia.
- Persona que ha cerrado la incidencia.

El Responsable de Seguridad podrá adoptar, al margen del procedimiento descrito, acciones inmediatas de control, especialmente de carácter técnico: recuperación de datos, bloqueo de usuarios, etc.

Se mantendrán las incidencias registradas de los **12 últimos meses**. En el caso de que se trate de una incidencia que provoque una **recuperación de datos**, se deberá contar con la autorización expresa y por escrito del Responsable del Tratamiento. Se consignarán, además, la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de recuperación.

Impreso de notificación de incidencias

Incidencia N1: _____ (Este número será rellenado por el Responsable de seguridad)	
Fecha de notificación: / __ / __ / __ / __	
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Fecha y hora en que se produjo la incidencia:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella	
Medidas correctoras aplicadas:	
Recuperación de Datos : (A rellenar sólo si la incidencia es de este tipo)	
Procedimiento realizado:	
Datos restaurados:	
Datos grabados manualmente:	
Persona que ejecutó el proceso:	
Firma del Responsable del Tratamiento:	
Fdo _____	
Persona que realiza la comunicación:	
Fdo.: _____	

4. I Controles periódicos y auditorías

26/01/2026: Reunión técnica de Protección de Datos para explicación de documentación.