SoftwareLOPD

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

SILVIA DE VEGA ARRIAGA
50898353C

viernes, 23 de octubre de 2026

INTRODUCCIÓN

El RGPD especifica que se puede disponer de un solo documento que incluya todos los sistemas de tratamiento y tratamientos con datos personales de los que una persona física o jurídica sea responsable, un documento por cada sistema de tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido. Cualquiera de las opciones puede ser válida. En este caso se ha optado por el primer tipo, organizando el "registro de actividades de tratamiento" en dos partes: en la primera se recogen las medidas que afectan a todos los sistemas de información de forma común con independencia del sistema de tratamiento sobre el que se organizan: informatizado, manual o mixto, y en la segunda se incluye un anexo por cada sistema de tratamiento, con las medidas que le afecten de forma concreta. Además, se han especificado aquellas medidas que afectan sólo a sistemas de tratamiento automatizados y las que afectan a los no automatizados de forma exclusiva.

El modelo se ha redactado con el objeto de recopilar las exigencias mínimas establecidas por el Reglamento. Es posible y recomendable incorporar cualquier otra medida que se considere oportuna para aumentar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les correspondería, teniendo en cuenta la infraestructura y las circunstancias particulares de la organización.

DATOS ESPECIALMENTE PROTEGIDOS: Con esta marca se señalarán las medidas que sólo son obligatorias en los sistemas de tratamiento .

AUTOMATIZADOS: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a sistemas de tratamiento informatizados o automatizados.

MANUALES: Con esta marca se señalarán las medidas específicas para aplicar exclusivamente a sistemas de tratamiento manuales o no automatizados.

Las medidas que no van precedidas de ninguna de estas marcas deben aplicarse con carácter general, tanto a sistemas de tratamiento automatizados como no automatizados y con independencia del tipo de informaciÃ³n.

MODELO DEL REGISTRO DE ACTIVIADES DE TRATAMIENTO

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en la RGPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados.

- Ámbito de aplicación del documento.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
- Información y obligaciones del personal.
- Procedimientos de notificación, gestión y respuestas ante las incidencias.
- Procedimientos de revisión.

ANEXO I. Descripción de los sistemas de tratamiento.

ANEXO II. Nombramientos.

ANEXO III. Inventario de soportes.

ANEXO IV. Registro de Incidencias.

ANEXO V. Encargados de tratamiento.

ANEXO VI. Medidas alternativas

1 .ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los sistemas de tratamiento que contienen datos de carácter personal que se hallan bajo la responsabilidad de SILVIA DE VEGA ARRIAGA, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

En concreto, los sistemas de tratamiento sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

Sistema de tratamiento
CLIENTES-PROVEEDORES
GENERAL DE ADMINISTRACIÓN

En el Anexo I se describen detalladamente cada uno de los sistemas de tratamiento, junto con los aspectos que les afecten de manera particular.

2. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

IDENTIFICACIÓN Y AUTENTICACIÓN

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

AUTOMATIZADOS

Para acceder a los equipos implicados en el tratamiento de datos de carácter personal es obligatorio introducir un usuario y un password.

El Responsable del sistema de tratamiento hará activar el sistema de identificación y autenticación.

Para que el sistema de identificación y autenticación sea correcto es necesario que cada usuario con acceso al sistema de tratamiento de datos de carácter personal tenga su login y su password personal. Se requiere además el cambio obligatorio de la password semestralmente, con las características de longitud de cuatro caracteres y que no sean series repetitivas o continuas.

Todas las pantallas de trabajo donde se pueda trabajar con datos de carácter personal deben tener habilitado el salvapantallas y la password de desactivación del mismo, con los mismos criterios que la password de entrada al sistema. Hay que hacer especial hincapié en este aspecto en aquellos puestos de trabajo que sean de fácil acceso para el público o terceros ajenos.

DATOS ESPECIALMENTE PROTEGIDOS En los sistemas de tratamiento con datos especialmente protegidos, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del sistema de tratamiento establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados mediante perfiles de acceso.

Exclusivamente el Responsable de Seguridad está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del sistema de tratamiento.

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista deberá mantenerse actualizada.

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

DATOS ESPCIALMENTE PROTEGIDOS:REGISTRO DE ACCESOS

AUTOMATIZADOS

En los accesos a los datos de los sistemas de tratamiento con datos especialmente protegidos, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el sistema o fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

Los datos del registro de accesos se conservaran durante al menos dos años.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe según se detalla en el capítulo de "Comprobaciones para la realización de la auditoría de seguridad" de este documento.

No será necesario el registro de accesos cuando:

- el responsable del sistema de tratamiento es una persona física,
- el responsable del sistema de tratamiento garantice que sólo él tiene acceso y trata los datos personales,
- y se haga constar en el registro de actividades de tratamiento.

MANUALES

El acceso a la documentación se limita exclusivamente al personal autorizado.

Se establece el siguiente mecanismo para identificar los accesos realizados en el caso de los documentos relacionados en soporte papel

GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en zonas de acceso restringido al que solo tendrán acceso las personas con autorización.

Los siguientes soportes en formato papel se identificarán utilizando los sistemas de etiquetado.

Los soportes se almacenarán de acuerdo a las siguientes normas: Bajo llave y en un lugar que no sea de libre acceso.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del sistema de tratamiento o aquel en que se hubiera delegado. En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes que vayan a ser desechados, deberán ser previamente formateados o destruidos de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior.

En el traslado de la documentación se adoptarán las medidas pertinentes para evitar la sustracción, pérdida o acceso indebido a la información.

DATOS ESPECIALMENTE PROTEGIDOS: GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

AUTOMATIZADOS

En este caso los soportes se identificarán mediante el sistema de etiquetado.

La distribución y salida de soportes que contengan datos de carácter personal de los sistemas de tratamiento con datos especialmente protegidos se realizará en medios cifrados. Los dispositivos portátiles que, no se pudieran cifrar, se utilizarán en el tratamiento de datos personales adoptándose las medidas que impidan su libre acceso.

CRITERIOS DE ARCHIVO

MANUALES

El archivo de los soportes o documentos se realizará de manera que se puedan garantizar los derechos de acceso, rectificación, cancelación y oposición.

ALMACENAMIENTO DE LA INFORMACIÓN

MANUALES

Los dispositivos contarán con mecanismos que impidan su libre acceso y se utilizarán para guardar los documentos con datos personales.

DATOS ESPECIALMENTE PROTEGIDOS: Todos los elementos de almacenamiento respecto de los documentos con datos personales, se encuentran en los locales del responsable del sistema de tratamiento contarán con mecanismos que impidan su libre acceso y solamente podrá tener acceso el personal autorizado.

CUSTODIA DE SOPORTES

MANUALES

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

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, sean o no públicas, garantizarán un nivel de seguridad equivalente al exigido para los accesos en modo local.

AUTOMATIZADOS Y DATOS ESPECIALMENTE PROTEGIDOS: Los datos personales correspondientes a los sistemas de tratamiento con datos especialmente protegidos, que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando previamente estos datos.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL SISTEMA DE TRATAMIENTO

Se pueden llevar a cabo tratamientos de datos personales fuera de los locales del responsable del sistema de tratamiento, así como mediante dispositivos portátiles. Esta autorización regirá durante la vigencia del registro de activiades de tratamiento.

Se debe garantizar el nivel de seguridad correspondiente.

DATOS ESPECIALMENTE PROTEGIDOS: TRASLADO DE DOCUMENTACIÓN

MANUALES

Siempre que se proceda al traslado físico de la documentación contenida en un sistema de tratamiento, deberán adoptarse medidas de custodia que impidan el acceso a terceras personas.

SISTEMAS DE TRATAMIENTO TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los sistemas de tratameinto temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

COPIA O REPRODUCCIÓN

MANUALES

La realización de copias o reproducción de los documentos con datos personales sólo se podrán llevar a cabo bajo el control del Responsable de Seguridad. Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida, utilizando destructora de papel.

COPIAS DE RESPALDO Y RECUPERACIÓN

AUTOMATIZADOS

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, con la siguiente periodicidad al menos una vez por semana.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En el caso de los sistemas de tratamiento parcialmente automatizados siguientes, se grabarán manualmente los datos.

El responsable del sistema de tratamiento verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada sistema de tratamiento.

DATOS ESPECIALMENTE PROTEGIDOS: En los sistemas de tratamiento con datos espcialmente protegidos se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente al que se ubique el centro de tratamiento.

DATOS ESPECIALMENTE PROTEGIDOS: RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad, a gerencia, que con carácter general se encargará de coordinar y controlar las medidas definidas en este registro de activiades de tratamiento.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a SILVIA DE VEGA ARRIAGA como responsable del sistema de tratamiento de acuerdo con el RGPD.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de un año. Una vez transcurrido este plazo se podrá nombrar al mismo responsable de seguridad o a otro diferente.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

3. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL

INFORMACIÓN AL PERSONAL

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento: *CLAUSULA DEBER DE SECRETO PROFESIONAL*.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al responsable del sistema de tratamiento las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias".

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

CONSECUENCIAS DEL INCUMPLIMIENTO DEL REGISTRO DE ACTIVIADES DE TRATAMIENTO

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a la normativa vigente.

4. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Registro de Actividades de Tratamiento, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de Responsable del Sistema de Tratamiento. El procedimiento a seguir para la notificación de incidencias será el Registro de Incidencias.

El registro de incidencias se gestionará mediante el REGISTRO DE INCIDENCIAS.

AUTOMATIZADOS CON DATOS ESPECIALMENTE PROTEGIDOS:

- En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los sistemas de tratamiento de datos espcialmente protegidos.
- Para ejecutar los procedimientos de recuperación de datos en los sistemas de tratamiento mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del sistema de tratamiento.

En el Anexo III se incluirán los documentos de autorización del responsable del sistema de tratamiento relativos a la ejecución de procedimientos de recuperación de datos.

5. PROCEDIMIENTOS DE REVISIÓN

REVISIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los sistemas de tratamiento o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

DATOS ESPECIALMENTE PROTEGIDOS: AUDITORÍA

Se deberá realizar una auditoría en el plazo no superior a dos años.

Asimismo deberá realizarse cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado

El informe analizará la adecuación de las medidas y controles a la RGPD, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema de tratamiento para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos.

AUTOMATIZADOS Y ESPECIALMENTE PROTEGIDOS: Informe mensual sobre el registro de accesos.

En los accesos a los datos de los sistemas de tratamiento especialmente protegidos, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el sistema de tra accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido. Dicho informe se realizará a través del software que trata los datos de carácter personal especialmente protegidos.

ANEXO I - DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO

CLIENTES-PROVEEDORES

Descripción: FICHERO DESTINADO A LA GESTION DE CLIENTES Y PROVEEDORES

DATOS DEFINIDOS EN EL SISTEMA DE TRATAMIENTO

Estructura

Datos de carácter identificativo	☑D.N.I. / N.I.F. ☑Nombre y Apellidos ☑Dirección (postal, electrónica) ☑Firma ☑Teléfono ☑Imagen / Voz ☑Firma electrónica
Otros tipos de datos	☑Características personales ☑Detalles del empleo ☑Información comercial ☑Económicos, financieros y de seguros ☑Transacciones de bienes y servicios

Finalidades

☑Gestión de clientes contable, fiscal y administrativa

Origen y colectivo

Origen	☑El propio interesado o su representante legal
Colectivos o categorías de interesados	☑Proveedores ☑Solicitantes ☑Cliente y usuarios ☑Personas de contacto

Cesiones

ℹNo se realizan cesiones

Transferencias internacionales

ℹNo se realizan transferencias internacionales

EQUIPOS RELACIONADOS CON EL SISTEMA DE TRATAMIENTO

Nombre del equipo Equipo SILVIA DE VEGA ARRIAGA

Descripción: Equipo SILVIA DE VEGA ARRIAGA

Nombre programa	Usuarios
Programa gestión	SILVIA DE VEGA ARRIAGA
Programas de correo electrónicos	SILVIA DE VEGA ARRIAGA
Programas de paquete ofimático	SILVIA DE VEGA ARRIAGA

GENERAL DE ADMINISTRACIÓN

Descripción: FICHERO DESTINADO A LA GESTIÓN ECONÓMICA, CONTABLE, ADMINISTRATIVA, FISCAL Y DE FACTURACIÓN

DATOS DEFINIDOS EN EL SISTEMA DE TRATAMIENTO

Estructura

Datos de carácter identificativo	☑D.N.I. / N.I.F. ☑Nombre y Apellidos ☑Dirección (postal, electrónica) ☑Firma ☑Teléfono ☑Huella ☑Imagen / Voz ☑Firma electrónica
Otros tipos de datos	☑Características personales ☑Detalles del empleo ☑Información comercial ☑Económicos, financieros y de seguros ☑Transacciones de bienes y servicios

Finalidades

☑Gestión de clientes contable, fiscal y administrativa

Origen y colectivo

Origen	☑El propio interesado o su representante legal
Colectivos o categorías de interesados	☑Proveedores ☑Solicitantes ☑Cliente y usuarios ☑Personas de contacto

Cesiones

☑Administración Pública con competencia en la materia
☑Administración tributaria
☑Otros órganos de la administración pública
☑Bancos

Transferencias internacionales

ℹNo se realizan transferencias internacionales

EQUIPOS RELACIONADOS CON EL SISTEMA DE TRATAMIENTO

Nombre del equipo Equipo SILVIA DE VEGA ARRIAGA

Descripción: Equipo SILVIA DE VEGA ARRIAGA

Nombre programa	Usuarios
Programa de facturación	SILVIA DE VEGA ARRIAGA
Programa de bancos	SILVIA DE VEGA ARRIAGA
Programas de paquete ofimático	SILVIA DE VEGA ARRIAGA

ANEXO II - NOMBRAMIENTOS

RESPONSABLE DE SEGURIDAD

Nombre: SILVIA
Apellidos: DE VEGA ARRIAGA
Dni: 50898353C
Área: Encargado/a

ANEXO III - INVENTARIO DE SOPORTES

SOPORTE PAPEL

Sistema de tratamiento: CLIENTES-PROVEEDORES

Ubicación:

Local:	Local general
Departamento:	Departamento general
Zar:	Zar documentación en papel
Descripción:	Zona de acceso restringido para el almacenamiento de la documentación en papel.

Sistema de tratamiento: GENERAL DE ADMINISTRACIÓN

Ubicación:

Local:	Local general
Departamento:	Departamento general
Zar:	Zar documentación en papel
Descripción:	Zona de acceso restringido para el almacenamiento de la documentación en papel.

SOPORTE DIGITAL

No se ha definido ningún soporte digital

ANEXO IV - REGISTRO DE INCIDENCIAS

No hay registrada ninguna incidencia

ANEXO V - ENCARGADOS DE TRATAMIENTO

CLIENTES-PROVEEDORES

GENERAL DE ADMINISTRACIÓN

Nombre: CAFSA, S.L.
Cif: B83845925
Dirección: CALLE SAIZ DE LA RUEDA , 1 BAJO, VELILLA DE SAN ANTONIO (28891), Madrid

ANEXO VI - REGISTRO DE COPIAS DE SEGURIDAD

No existe ningún registro de copia de seguridad

ANEXO VII - MEDIDAS ALTERNATIVAS

En el caso de que no sea posible adoptar las medidas exigidas por el RGPD en relación con la identificación de los soportes, los dispositivos de almacenamiento de los documentos o los sistemas de almacenamiento de la información, indicar las causas que justifican que ello no sea posible y las medias alternativas que se han adoptado