

REGISTRO DE TRATAMIENTO

|  |  |
| --- | --- |
| **RESPONSABLE DE TRATAMIENTO** | PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. |
| **CIF** | B81763484 |
| **DIRECCIÓN** | C/ Chile Nº 10, oficina 119 Las Rozas 28290 MADRID |
| **RESPONSABLE SEGURIDAD** | Julian Ramos Martín |
| **FECHA REALIZACIÓN** | 22 de Abril de 2018 |
| **PERIODO REVISIÓN** | TRIMESTRAL |
| **APROBADO POR** | Julian Ramos Martín |

 

ÍNDICE

1. CONTROL DE SEGUIMIENTO Y ACTUALIZACIÓN
2. AMBITO DE APLICACIÓN DEL DOCUMENTO
3. **ANEXO I.** REGISTRO ACTIVIDADES DE TRATAMIENTO
4. **ANEXO II.** MEDIDAS TÉCNICAS Y ORGANIZATIVAS
	1. Novedades RGPD
	2. Medida para tratamientos automatizados
		1. Identificación y autenticación
		2. Acceso a través de redes de comunicaciones
		3. Copias de respaldo y recuperación
		4. Traslado de soportes
		5. Destrucción y reutilización de soportes.
	3. Medidas para tratamientos no automatizados.
		1. Criterio de archivo y almacenamiento de información.
		2. Traslado de documentación.
	4. Entorno de seguridad
		1. Centros de tratamiento y locales.
		2. Puestos de trabajo
		3. Inventario de soportes
5. **ANEXO III.** NOMBRAMIENTOS Y DELEGACIONES
	1. Nombramiento Delegado de Protección de Datos.
	2. Nombramiento Responsable de Seguridad
6. **ANEXO IV.** AUTORIZACIONES
	1. Autorización de salida de soportes fuera de las instalaciones.
	2. Registro trabajo fuera de las locales.
7. **ANEXO V.** GESTIÓN DE USUARIOS
	1. Funciones y obligaciones de los usuarios
		1. Obligaciones generales
		2. Puestos de trabajo
		3. Gestión de soportes.
		4. Destrucción y reutilización de soportes.
		5. Ficheros temporales o copias de trabajo de documentos.
		6. Documentación en papel
		7. Destrucción de documentación.
		8. Gestión de incidencias.
	2. Resumen de los usuarios con acceso a datos.
	3. Plan formación usuarios
8. **ANEXO VI.** GESTIÓN DE ENCARGADOS DE TRATAMIENTO
	1. Definición de encargado de tratamiento y función.
	2. Registro encargados de tratamiento
	3. Modelo contrato protección de datos Encargados tratamiento
9. **ANEXO VII.** BRECHAS DE SEGURIDAD
	1. Procedimiento notificación Brechas de seguridad
		1. Modelo notificación DPO
		2. Modelo resolución brecha seguridad.
10. **ANEXO VIII.** CLAUSULAS Y CIRCULARES

OBJETO DEL DOCUMENTO

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD), y por el que se deroga de la Directiva 95/46/CE, nace con objeto armonizar los tratamientos de datos personales de todos los ciudadanos de los Estados miembros de la UE garantizando un nivel coherente de protección de las personas en toda la UE, así como evitar divergencias que dificulten la libre circulación de datos dentro del mercado interior.

Debido al auge de las nuevas tecnologías de la información y a la sociedad del conocimiento, en los últimos años se ha intensificado el tratamiento automatizado de datos, lo que ha hecho que cobre especial importancia la protección de datos de carácter personal.

Gracias al desarrollo tecnológico, tanto empresas privadas como organismos públicos tienen acceso a infinidad de datos personales, por ello hay que establecer los mecanismos de protección adecuados para tratar la información de forma correcta y evitar usos inadecuados de los datos de carácter personal.

A pesar de que, tanto a nivel europeo como en nuestro país, existe una normativa consolidada en materia de protección de datos, desde la Unión Europea se ha llegado a la conclusión de que la legislación vigente no es acorde al elevado nivel de complejidad que tienen los procesos de tratamiento de datos en internet. Esto ha propiciado la necesidad de una nueva regulación jurídica dando lugar a la aparición de una nueva normativa europea: Reglamento (UE) 2016/679 Del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Este nuevo reglamento supone una adaptación a nivel europeo de la legislación en materia de protección de datos, es decir, todos los países de la Unión Europea deberán adaptar su normativa a este reglamento y más concretamente, todas las empresas, organizaciones o entidades públicas deberán adaptar el tratamiento de datos de carácter personal a las nuevas obligaciones que desarrolla este Reglamento Europeo.

AMBITO DE APLICACIÓN

El presente documento tiene como finalidad recoger las características del tratamiento de las actividades de tratamiento que se realizan en la entidad en el desarrollo de su actividad.

Las medidas de seguridad implantadas buscan proteger la privacidad y confidencialidad de todas las actividades realizadas, incluidas en ficheros, aplicaciones, recursos de la entidad, redes de comunicaciones y equipos informáticos o soportes no automatizados.

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de la entidad 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.

El RGPD establece que el ámbito de ampliación puede ser tanto material como territorial:

AMBITO DE APLICACIÓN MATERIAL

* Tratamiento total o parcialmente automatizado de datos personales.
* Tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
* Tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión.

AMBITO DE APLICACIÓN TERRITORIAL

* Tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado de la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
* Tratamiento de datos personales interesados que residan en la UE por parte de un responsable o encargado no establecido en la UE, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados de la UE, independientemente de si a estos se les requiere su pago o el control de su comportamiento, en la medida que tenga lugar en la UE.
* Tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión, sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho Internacional.

ANEXO I

REGISTRO DE LAS CATEGORÍAS DE ACTIVIDADES DE TRATAMIENTO

Conforme indica la normativa vigente, la entidad llevará un registro de las actividades de tratamiento que realiza para el desarrollo de su actividad.

Dicho registro deberá ser revisado y actualizado con la finalidad de reflejar la situación real de los tratamientos en cada momento.

El contenido de cada una de las actividades es el siguiente:

* COLECTIVO OBJETO DE TRATAMIENTO
* CATEGORIA DE DATOS
* TIPOLOGÍA DE ESTOS
* FINALIDAD DEL TRATAMIENTO
* CATEGORÍA DE DESTINATARIOS
* EXISTENCIA DE TRANSFERENCIAS INTERNACIONALES
* MEDIDAS TECNICAS Y ORGANIZATIVAS
* PLAZOS DE SUPRESIÓN
* PERFILES AUTORIZADOS A SU ACCESO.

ANEXO II

NOVEDADES RGPD

1. **CONSENTIMIENTO DEL INTERESADO**

Será necesario un consentimiento inequívoco, libre y revocable.

El consentimiento debe expresarse mediante una acción afirmativa clara de conformidad, ya no se permite el consentimiento tácito.

1. **DATOS DE MENORES**

Se establecen especificaciones sobre los datos de menores ya que no podrán ofrecerse servicios de la sociedad de la información a menores de 16 años sin el consentimiento paterno o del tutor legal, salvo que una ley nacional establezca una edad inferior que no puede ser menos de 13 años.

1. **DERECHOS DE LOS INTERESADOS**

Establecimiento de nuevos derechos:

- Derecho al olvido.

- Derecho de portabilidad.

1. **DEBER DE INFORMAR**

Deber de informar de la base legal para el tratamiento de los datos, del período de conservación de los mismos y de que se pueden dirigir las reclamaciones a las autoridades de protección de datos.

Surge la obligación de notificar los fallos de seguridad que se produzcan en la empresa a la Agencia Española de Protección de Datos en un plazo de 72 h.

1. **DATOS RECABADOS DE TERCEROS**

Cuando los datos personales se hayan obtenido de terceros, se debe informar al interesado en un plazo un mes.

1. **APLICACIÓN DE MEDIDAS DE SEGURIDAD**

No se distinguen niveles de seguridad (básico, medio o alto). Las medidas de seguridad se aplicarán teniendo en cuenta en función del riesgo.

1. **IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD**

Surge una nueva figura el Delegado de Protección de Datos (DPO).

1. **INSCRIPCIÓN DE FICHEROS**

No será obligatoria la inscripción de ficheros ante la AEPD (salvo para empresas de más de 250 trabajadores).

Se debe llevar un registro interno y por escrito del tratamiento de datos que se realice.

Se debe llevar un registro de las actividades de tratamiento siempre que se traten datos de riesgo o sensibles.

MEDIDAS DE SEGURIDAD PARA FICHEROS Y/O TRATAMIENTOS AUTOMATIZADOS.

**Identificación y Autenticación**

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

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

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

En general, cualquier soporte que vaya a ser desechado, de cualquier tipo, que pueda contener datos de carácter personal, ya sea papel impreso, soportes magnéticos, ópticos u otros, o los propios ordenadores obsoletos que vayan a desecharse, deberán ser tratados mediante los procedimientos de destrucción y reutilización de soportes informáticos con el fin de impedir la pérdida de confidencialidad de los datos personales. Aquellos medios que sean reutilizables, y que hayan contenido copias de datos de carácter personal, deberán ser borrados físicamente de forma segura antes de su reutilización, de forma que los datos que contenían no sean recuperables.

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

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

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

Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, como “casa”, el nombre propio, etc. Para ello se seguirán las siguientes pautas en la construcción de contraseñas:

* Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
* No deberán coincidir, ni siquiera en parte, con el código de usuario.
* No deberán estar basados en cadenas de caracteres que sean fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).
* Se recomienda aplicar las reglas nemotécnicas para poder construir una contraseña lo suficientemente compleja como para que no pueda ser adivinada por terceros y a la vez sean muy fáciles de recordar por él.
* Acceso al sistema por primera vez: el administrador asignará una contraseña provisional al nuevo usuario, que deberá ser cambiada en su primer acceso al sistema por una que sólo conozca el usuario y en base a las características definidas anteriormente.

**Acceso a través de redes de comunicaciones**

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar el nivel de seguridad equivalente al correspondiente a los accesos en modo local.

**Copias de respaldo y recuperación.**

Se realizarán copias de respaldo para asegurar la integridad y disponibilidad de los datos ante cualquier fallo informático, esta copia garantizará la reconstrucción del fichero en el estado que se encontraba antes de la pérdida. Estas copias se realizarán al menos una vez por semana, salvo que en este intervalo no se haya producido ninguna actualización de datos.

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

El Responsable del Fichero verificará semestralmente los procedimientos de copias de respaldo y seguridad.

**Traslado de soportes**

Para el traslado físico de soportes fuera de las instalaciones del Responsable del Fichero se deberá realizar garantizando la seguridad de los datos contenidos. Para ello, se deberán adoptar las medidas dirigidas a impedir el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma. Dichas medidas consisten en:

* El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.
* Cifrar siempre que sea posible la información que contiene o bien utilizar otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

**Destrucción y reutilización de soportes**

Hay que prestar especial atención a los desechos informáticos de cualquier tipo que puedan contener información de carácter personal. Es necesario seguir el siguiente procedimiento para su destrucción:

* Estos soportes siempre deberán ser destruidos de manera efectiva asegurándonos que se haga imposible la extracción de ningún dato posteriormente.

**Régimen de trabajo fuera de los locales de la ubicación de los ficheros.**

Se pueden llevar a cabo los tratamientos de datos personales fuera de los locales del Responsable del Fichero, así como mediante dispositivos portátiles, para aquellos ficheros y por aquellas personas designadas a ello según la información incluida en el Modelo – “Autorizaciones”

**Ficheros temporales o copias de trabajo de documentos**

Los ficheros 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 hayan dejado de ser necesarios para los fines que motivaron su creación

**MEDIDAS DE SEGURIDAD PARA FICHEROS Y/O TRATAMIENTOS NO AUTOMATIZADOS.**

**Criterio de archivo y almacenamiento de la información**

Estos criterios se realizarán de acuerdo a la legislación prevista, cuando no exista dicha legislación será el Responsable del Fichero el encargado de definir dichos procedimientos y siempre garantizando la localización, consulta y posibilitar los ejercicios de los derechos de acceso, rectificación, cancelación y oposición.

El almacenamiento de los documentos que contengan datos de carácter personal, deberán disponer de mecanismos que obstaculicen su apertura al personal no autorizado a su tratamiento.

**Traslado de documentación**

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las medidas que impidan el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma. Dichas medidas son:

* El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.
* En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

**ENTORNO DE SEGURIDAD**

**Centros de tratamiento y locales**

Los locales donde se ubican los ficheros deben ser objeto especial de protección que garanticen la confidencialidad e integridad de los datos protegidos, siempre deberán contar con los medios de seguridad que garanticen la confidencialidad e integridad de los datos protegidos.

**Puestos de trabajo**

Cada puesto de trabajo estará bajo la responsabilidad de las personas usuarias de él y deberá proteger la confidencialidad de los datos personales tratados en él, debe imposibilitar el acceso a personal no autorizado a ellos, en especial cuando se abandone el puesto de trabajo.

Es conveniente fijar un protector de pantalla que impida la visualización de datos, para la reanudación será necesaria la introducción de una contraseña. En el caso de impresoras, los usuarios deberán asegurarse de no dejar documentos con datos personales en las bandejas de salida.

Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a sistemas o redes exteriores, que no esté autorizada previamente por el Responsable del Fichero. Para la realización de trabajos fuera de los locales del Responsable del Fichero, será necesaria una autorización del Responsable de Seguridad.

**INVENTARIO APLICACIONES INFORMATIVAS**

Los soportes y documentos que contengan datos de carácter personal, 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 permita identificar el tipo de información que contienen, ser inventariados y serán almacenados en un lugar con acceso restringido al que solo tendrá acceso el personal debidamente autorizado.

El inventario de soportes, normas de etiquetado, lugar concreto donde se almacenarán, así como el personal autorizado para acceder a dichos soportes se encuentra en el ANEXO III.

Cuando existan soportes cuyas características físicas imposibiliten el cumplimiento de las obligaciones descritas anteriormente, quedará constancia motivada en el ANEXO III de los soportes afectados. La identificación de soportes y documentos que contengan datos de carácter personal que la organización considerase especialmente sensibles, se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de las personas. Los soportes afectados, así como los criterios de etiquetado para ellos se especifican en el presente documento.

Los usuarios que traten los soportes o documentos con datos de carácter personal, son los encargados de custodiarlos y vigilar para que personas no autorizadas no accedan al soporte físico o documentos a su cargo.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o añejos a un correo electrónico, fuera de los locales bajo el control del responsable fichero o tratamiento, deberá ser autorizada por el responsable del fichero (o aquel en que se hubiera delegado), o encontrarse debidamente autorizada. En el presente documento se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

ANEXO III

FIGURA DELEGADO DE PROTECCIÓN DE DATOS (DPO) Y RESPONSIBLE DE SEGURIDAD

El nuevo Reglamento Europeo de Protección de datos introduce la figura del Delegado de Protección de Datos o Data Protection Officer (DPO)

Esta figura, conocida popularmente como DPO (en inglés, Data Protection Officer), constituye uno de los elementos claves del RGPD, y un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control.

Es decir, al Delegado de Protección de Datos, que deberá contar con conocimientos especializados del Derecho, y obviamente en protección de datos, que actuará de forma independiente, se le atribuyen una serie de funciones reguladas en el artículo 39 del RGPD, entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte del responsable o encargado.

No obstante, lo anterior, conviene precisar dos cuestiones al respecto:

• El RGPD no exige que deba ser un jurista, pero sí que cuente con ese conocimiento en Derecho anteriormente citado;

• El DPO podrá ser interno o externo, persona física o persona jurídica especializada en esta materia.

El Responsable de seguridad será el encargado de coordinar las medidas de seguridad definidas en la política de protección de datos diseñada por la empresa

ANEXO IV

AUTORIZACIÓN DE SALIDA FUERA DE LAS INSTALACIONES

Será necesario cumplimentar la autorización de salida de soportes de todos los usuarios que realicen trabajo fuera de las instalaciones, aun cuando dicha autorización sea permanente.

ANEXO V

FUNCIONES Y OBLIGACIONES DE USUARIOS

La entidad vela por la confidencialidad de los datos de los cuales es responsable por lo que desarrolla un exhaustivo plan de confidencialidad para que todos los usuarios que en el desarrollo de su actividad tienen acceso a datos personales, dentro del cual se engloba:

* Diferenciación de accesos según los perfiles y roles dentro de la entidad.
* Firma contratos de confidencialidad regulando los deberes de los usuarios en materia de protección de datos.
* Comunicado interno de lectura obligatoria con las normas sobre la política de privacidad.
* Plan de formación dando cumplimiento al deber de información a usuarios /empleados.

FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Usuario es todo el personal autorizado que accede a los datos de carácter personal para el desempeño de las funciones propias de su puesto de trabajo.

Todos los usuarios tienen la obligación de colaborar con el Responsable del Fichero para velar por el cumplimiento de la legislación vigente sobre Protección de Datos de Carácter Personal.

Los usuarios deben respetar los procedimientos definidos para gestionar la seguridad de la información que se detallan a continuación.

OBLIGACIONES GENERALES

* Guardar secreto y confidencialidad de la información tratada. Quienes intervienen en cualquier fase del tratamiento de los datos de carácter personal, está obligado al secreto profesional respecto a los datos y al deber de guardarlos, obligaciones que continúan incluso después de finalizar las relaciones con el Responsable del Fichero.
* La vulneración del deber de secreto respecto a los datos personales tratados, será considerado una falta leve, grave o muy grave, conforme a lo previsto en el artículo 44 de la LOPD, lo cual dará lugar al inicio de acciones disciplinarias, si proceden.
* Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.
* Los sistemas de información, recursos, y la información personal a la que se accede, sólo se debe utilizar para las labores estrictamente profesionales que el usuario tiene asignadas.
* Facilitar el derecho de acceso, rectificación y cancelación a los titulares de los datos. Para ello se informará al Responsable del Fichero, Responsable de Seguridad o Encargado del tratamiento y se recogerá siempre en solicitud escrita.

PUESTOS DE TRABAJO

Cada usuario es responsable de la confidencialidad de la contraseña que tiene para acceder a los sistemas de información. En caso que de forma accidental o intencionada esta contraseña sea conocida por personas no autorizadas, deberá registrarlo como incidencia y proceder al cambio de la misma.

El usuario deberá cambiar la contraseña inicial asignada en el primer acceso que realice al sistema, o tras el desbloqueo de su contraseña cuando haya sido necesaria la intervención de una tercera persona para realizar el proceso. Las contraseñas deberán ser lo suficientemente complejas para no ser adivinadas de forma sencilla por un tercero. Para ello, se deberán seguir las siguientes normas para elegir la contraseña:

* Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
* No deberán coincidir, ni siquiera en parte, con el código de usuario.
* No deberán estar basados en cadenas de caracteres que sean fácilmente asociadas al usuario nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).
* El usuario deberá aplicar las reglas nemotécnicas para poder construir una contraseña lo suficientemente compleja como para que no pueda ser adivinada por terceros y a la vez sean muy fáciles de recordar por él.

Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible a personas no autorizadas.

Los puestos de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad, así como las pantallas, impresoras y cualquier otro dispositivo conectado al puesto de trabajo y desde el que sea posible tener acceso a datos de carácter personal.

Cuando el responsable del puesto de trabajo lo abandone, bien temporalmente, o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. Para reanudar el trabajo será necesaria la introducción de una contraseña que desactive el protector de pantalla. Deberá retirar también cualquier soporte, como documentos, fichas, discos, u otros que contengan datos del fichero, y proceder a guardarlos en su ubicación protegida habitual.

En el caso de las impresoras, deberá asegurarse que no quedan documentos con datos personales en la bandeja de salida. Si las impresoras son compartidas, el usuario que ha mandado la impresión deberá retirar los documentos conforme vayan siendo impresos.

Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a sistemas o redes exteriores, que no esté autorizada previamente por el Responsable del Fichero.

Se deberá evitar el guardar copias de los datos personales en ficheros temporales. En caso de que el tratamiento haga imprescindible realizar dichas copias, se deberán adoptar las siguientes precauciones:

* Realizar siempre las copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por el disco duro, y siempre sea posible conocer dónde están los datos temporales.
* Tras realizar el tratamiento que ha requerido estos datos temporales, proceder a su inmediata eliminación.

Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda en función de los datos que contienen.

El trabajo fuera de los locales del Responsable del Fichero, solo se podrá realizar cuando exista una autorización previa del Responsable del Fichero o del encargado del tratamiento, en todo caso, deberá garantizarse el nivel de seguridad.

No deberá copiarse, ni transportar información en portátiles, o equipos que se encuentren fuera de las oficinas sin la correspondiente autorización del Responsable del Fichero. Especial consideración deberán tener los puestos de trabajo portátiles, como ordenadores portátiles o PDA. Estos dispositivos portátiles, cuando puedan almacenar datos personales, deberán contar con una autorización especial por parte del Responsable del Fichero.

GESTIÓN DE SOPORTES

Se entiende por soporte todo objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos. Ejemplos de soportes: disquetes, CD-ROM, DVD-ROM, memoria USB, disco duro, etc.

Los Usuarios deben observar las siguientes medidas de seguridad en relación con los soportes que contengan datos de carácter personal:

* Los usuarios que traten los soportes o documentos con datos de carácter personal, son los encargados de custodiarlos y vigilar para que personas no autorizadas no accedan al soporte físico o documentos a su cargo.
* Cuando un usuario gestione o produzca soportes que contengan datos de carácter personal, estos deberán estar claramente identificados con una etiqueta externa e inventariados.
* Los soportes que contengan datos de carácter personal, deberán ser almacenados en lugares a los que no tenga acceso el personal no autorizado.
* La salida de soportes que contengan datos de carácter personal de las instalaciones bajo control del Responsable del Fichero, deberá ser autorizada por el Responsable del Fichero o estar debidamente autorizada en el Documento de Seguridad.
* La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o añejos a un correo electrónico, fuera de los locales bajo el control del responsable fichero o tratamiento, deberá ser autorizada por el responsable del fichero (o aquel en que se hubiera delegado), o encontrarse debidamente autorizada en el Documento de Seguridad.
* El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.
* Cuando deban ser enviados datos personales fuera de las ubicaciones del Responsable del Fichero, ya sea mediante soporte físico de grabación de datos o bien a través de correo electrónico o FTP, deberán ir cifrados o utilizar cualquier otro mecanismo que asegure que la información no es accesible ni manipulada durante su transporte.

DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados. Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento.

* Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.
* Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.
* Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al Responsable del Fichero.
* Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al Responsable del Fichero para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los ficheros 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 hayan dejado de ser necesarios para los fines que motivaron su creación.

DOCUMENTACIÓN EN PAPEL (NO AUTOMATIZADA)

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 de personas no autorizadas.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las medidas que impidan el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma. Dichas medidas son:

* El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.
* En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.
* DESTRUCCIÓN DE DOCUMENTACIÓN
* Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.
* Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:
* Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.
* Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.
* En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.
* El Responsable del Fichero deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

GESTIÓN DE INCIDENCIAS

Se considerarán como “incidencias de seguridad”, entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos de carácter personal en sus tres vertientes de confidencialidad, integridad y disponibilidad.

Se deberán tener en cuenta, entre otras, las siguientes incidencias:

* Pérdida de información de algún fichero de datos de carácter personal.
* Modificación de datos personales por personal no autorizado o desconocido.
* Existencia de sistemas de información sin las debidas medidas de seguridad.
* Los intentos de acceso no autorizados a ficheros de carácter personal.
* El conocimiento por terceros de la clave de acceso al sistema.
* El intento no autorizado de salida de un soporte.
* La existencia de soportes sin inventariar y que contengan datos personales.
* La destrucción total o parcial de un soporte que contenga datos de carácter personal.
* La caída del sistema de seguridad informática, que posibilite el acceso a datos personales por personas no autorizadas.
* El cambio de la ubicación física de ficheros con datos de carácter personal.
* Cualquier incidencia que pueda afectar a la confidencialidad, integridad y/o disponibilidad de los datos de carácter personal.

Todos los usuarios, administradores, responsables, así como cualquier persona que tenga acceso a datos de carácter personal, deben tener conocimiento de este procedimiento para actuar en caso de incidencia que se detalla a continuación:

Cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad o integridad de los datos contenidos en los ficheros de la organización, deberá comunicarla inmediatamente al responsable del registro de incidencias a través del formulario GESTIÓN DE INCIDENCIAS, del que se le ha hecho entrega a cada trabajador. Deberá especificar el tipo de incidencia producida y su descripción detallada, indicando las intervenciones de las personas que hayan podido tener relación con la producción de la incidencia, así como la fecha y hora en que se ha producido o detectado, la persona que realiza la notificación, a quién se comunica y los efectos que se pueden haber derivado de la incidencia.

Una vez rellena la plantilla, se obtendrán 2 copias y se entregarán inmediatamente al Responsable del Fichero, o a la persona en quien haya delegado formalmente la gestión de las incidencias, solicitándole el acuse de recibo en una de las copias. Esta copia se guardará como resguardo de la notificación.

Una vez rellena la plantilla, se obtendrán 2 copias y se entregarán inmediatamente al Responsable del Fichero, o a la persona en quien haya delegado formalmente la gestión de las incidencias, solicitándole el acuse de recibo en una de las copias. Esta copia se guardará como resguardo de la notificación.)

El Responsable del fichero, o delegado, quedará encargado de la gestión, coordinación y resolución de la misma, así como al registro de la incidencia en el registro habilitado para ello.

El conocimiento y no notificación de una incidencia por parte de un usuario, será considerado como una falta de seguridad por parte de ese usuario.

ANEXO VI

ENCARGADOS DE TRATAMIENTO

¿QUE ES UN ENCARGADO DE TRATAMIENTO Y CUAL ES SU FUNCIÓN?

En el desarrollo de la actividad desarrollada, la entidad precisa de la externalización de servicios que suponen tratamiento de datos de carácter personal.

Encargados de tratamiento es aquella persona física o jurídica que, solo o conjuntamente con otros, trata los datos por cuenta del responsable de los datos personales.

Existe por tanto una relación jurídica que vincula al encargado con el responsable, y delimita el ámbito de actuación del encargado para la prestación del servicio de tratamiento de datos.

**¿QUE TRATAMIENTOS PUEDE LLEVAR A CABO UN ENCARGADO SOBRE LOS DATOS QUE LE HAN SIDO ENCOMENDADOS?**

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente. La definición de tratamiento nos permite concretarlos atendiendo al ciclo de vida de la información: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción; todos deben quedar claramente delimitados en el acuerdo que se adopte.

**¿QUE NIVEL DE DECISIÓN PUEDE ASUMIR UN ENCARGADO DE** **TRATAMIENTO?**

El encargado de tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades.

Todas las decisiones adoptadas deben respetar en todo caso las instrucciones otorgadas por el responsable de tratamiento.

La política de la entidad es siempre elegir encargados de tratamiento que ofrecen garantías suficientes en lo referente a la aplicación de medidas técnicas y organizativas para dar cumplimiento a los requisitos del Reglamento UE 2016/679. (RGPD)

ANEXO VII

PROCEDIMIENTO NOTIFICACION BRECHAS SEGURIDAD

El reglamento UE 2016/679 (RGPD) establece la obligación para todos los Responsables de tratamiento de notificar las violaciones de seguridad de los datos antes de 72 horas a la Agencia Española de Protección de Datos (AEPD)

Según indica el RGPD se denomina “Brecha de seguridad o violación de seguridad” como toda violación de la seguridad que ocasione la destrucción, perdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o a la comunicación o acceso no autorizado a dichos datos.

Cualquier Responsable del tratamiento que tenga conocimiento de cualquier violación de seguridad está obligado a notificar a la autoridad de control competente, sin dilación indebida y a más tardar 72 horas después de que se haya tenido constancia, la violación de la seguridad de los datos, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

El propio Reglamento indica el contenido mínimo que debe albergar dicha notificación, en concreto se refiere a:

* Naturaleza de la violación.
* Categorías de datos y de interesados afectados.
* Medidas adoptadas por el responsable para solventar la brecha.
* Las medidas aplicadas para paliar los efectos de la brecha.

Según indicación del RGPD será necesario documentar todas las violaciones de seguridad, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas y además en los casos en que sea probable que la violación de seguridad entrañe alto riesgo para los derechos y libertades de los interesados, será necesario realizar una notificación a los afectados.

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. ha implantado el siguiente protocolo de comunicación al DPO para que cualquier persona física o jurídica, relacionada con la empresa que detecte cualquier situación que pueda afectar al cumplimiento normativo pueda comunicárselo al DPO o Responsable de seguridad.

1. DETECCIÓN BRECHA DE SEGURIDAD
2. CUMPLIMENTACIÓN Y ENVÍO MODELO DE COMUNICACIÓN DPO / RESPONSABLE SEGURIDAD (Adjunto)
3. ANALISIS POR PARTE DEL DPO
4. DPO: SI FUERA BRECHA DE SEGURIDAD, NOTIFICACIÓN A LA AUTORIDAD DE CONTROL.
5. DPO: SI NO FUERA BRECHA DE SEGURIDAD, COMUNICACIÓN DE RESOLUCIÓN. (Adjunto)

ANEXO VIII

CLAUSULAS Y CIRCULARES

Este nuevo Reglamento está enfocado en ofrecer a los usuarios una información más exhaustiva, clara y sencilla sobre el tratamiento que se realiza de sus datos personales por lo que como comprobareis en la documentación incluida, hemos elaborado nuevas cláusulas de consentimiento que tanto clientes, como proveedores, empleados y cualquier interesado del cual tratemos datos personales, deben firmar.

Con la entrada en aplicación de esta nueva normativa, a las empresas se nos **EXIGE** poder demostrar que el interesado nos ha prestado el consentimiento para el tratamiento, por lo que es IMPORTANTE, modificar los consentimientos con los que actualmente trabajemos.

ANEXO I

REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS

NOMBRE DEL TRATAMIENTO

CLIENTES

FECHA DE ACTUALIZACIÓN DEL ANEXO

Actualizado a 22 de Abril de 2018

REGISTRO DEL TRATAMIENTO

Identificador y nombre del fichero en el Registro de Protección de Datos de la Agencia Española de Protección de Datos:

|  |  |
| --- | --- |
| **NOMBRE** | CLIENTES |
| **DESCRIPCIÓN** | Gestión comercial, administrativa, fiscal y contable de los clientes y potenciales clientes de la sociedad |

ESTRUCTURA DEL FICHERO PRINCIPAL Y TIPOS DE DATOS

|  |  |
| --- | --- |
| **Identificativos:** | NIF/DNI; Nombre y apellidos; Dirección; Teléfono; Firma; |
| **Especialmente protegidos:** |  |
| **Otros especialmente protegidos:** |  |
| **Otros datos tipificados:** | Información comercial; Económicos, financieros y de seguros; Transacciones de bienes y servicios; |
| **Otros tipos de datos:** | Correo electrónico |

INFORMACIÓN SOBRE EL TRATAMIENTO

|  |  |
| --- | --- |
| **Finalidad y usos previstos:** | Gestión de clientes contable, fiscal y administrativa; Publicidad y prospección comercial; |
| **Origen y procedencia de los datos:** | El propio interesado o su representante legal; |
| **Colectivos o categorías de interesados:** | Clientes y usuarios; Solicitantes; |
| **Cesiones previstas:** | Organizaciones o personas directamente relacionadas con el fichero; Administracion Tributaria; Bancos, cajas de ahorros y cajas rurales; |
| **Transferencias internacionales:** |  |

LOCALIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Los lugares donde se encuentran los sistemas de información, están ubicados en las siguientes direcciones:

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L.

C/ Chile Nº 10, oficina 119

Las Rozas (28290) MADRID

DERECHOS DE LOS INTERESADOS

El afectado podrá ejercitar sus derechos de acceso, rectificación, limitación, portabilidad cancelación u oposición en la siguiente dirección:

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L.

C/ Chile Nº 10, oficina 119

Las Rozas (28290) MADRID

Mail: comercial@gestinser.es

COPIAS DE RESPALDO Y PROCEDIMIENTO DE RECUPERACIÓN

Las copias de respaldo y recuperación de se realizan de acuerdo al siguiente procedimiento y con la periodicidad que se describe a continuación:

|  |  |
| --- | --- |
| **Periodicidad de la copia de seguridad:** | QUINCENAL |
| **Procedimiento para la realización de la copia de respaldo:** | SE REALIZA COPIA EN DISCO DURO EXTERNO |
| **Procedimiento de recuperación de los datos:** | SE RESTAURAN LOS FICHEROS DE LA COPIA DE SEGURIDAD A SU UBICACIÓN ORIGINAL |

CONEXIÓN CON OTROS SISTEMAS

No existen conexiones con otros sistemas.

FUNCIONES DEL PERSONAL CON ACCESO A LOS DATOS PERSONALES

Las diferentes funciones y obligaciones de cada perfil de usuarios que accede al fichero, así como el tipo de acceso que se realiza, se describen aquí:

|  |  |  |
| --- | --- | --- |
| **Perfil** | **Funciones asociadas al perfil** | **Tipo de acceso** |
| GERENCIA | GESTIÓN TOTAL DE LA SOCIEDAD | MIXTO |

APLICACIONES QUE ACCEDEN AL TRATAMIENTO

Las aplicaciones que acceden al fichero y los perfiles que las utilizan, así como los privilegios de que dispone dicho perfil son los siguientes:

|  |  |  |
| --- | --- | --- |
| **Perfil** | **Aplicación** | **Privilegios** |
| GERENCIA | PAQUETE OFFICE | L|A|B|M|I|E |

USUARIOS CON ACCESO AL TRATAMIENTO

La relación actualizada de usuarios con acceso autorizado al fichero es la siguiente:

|  |  |  |  |
| --- | --- | --- | --- |
| **Usuario** | **Perfil** | **F. Alta** | **F. Baja** |
| Julian Ramos Martín | GERENCIA | 01/01/2016 |  |

ANEXO I

REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS

NOMBRE DEL TRATAMIENTO

PROVEEDORES

FECHA DE ACTUALIZACIÓN DEL ANEXO

Actualizado a 22 de Abril de 2018

REGISTRO DEL TRATAMIENTO

Identificador y nombre del fichero en el Registro de Protección de Datos de la Agencia Española de Protección de Datos:

|  |  |
| --- | --- |
| **NOMBRE** | PROVEEDORES |
| **DESCRIPCIÓN** | Gestión comercial, administrativa, fiscal y contable de los proveedores y potenciales proveedores de la sociedad |

ESTRUCTURA DEL FICHERO PRINCIPAL Y TIPOS DE DATOS

|  |  |
| --- | --- |
| **Identificativos:** | NIF/DNI; Nombre y apellidos; Dirección; Teléfono; Firma; |
| **Especialmente protegidos:** |  |
| **Otros especialmente protegidos:** |  |
| **Otros datos tipificados:** | Información comercial; Económicos, financieros y de seguros; Transacciones de bienes y servicios; |
| **Otros tipos de datos:** | Correo electrónico |

INFORMACIÓN SOBRE EL TRATAMIENTO

|  |  |
| --- | --- |
| **Finalidad y usos previstos:** | Gestión de clientes contable, fiscal y administrativa; |
| **Origen y procedencia de los datos:** | El propio interesado o su representante legal; |
| **Colectivos o categorías de interesados:** | Proveedores; Solicitantes; |
| **Cesiones previstas:** | Organizaciones o personas directamente relacionadas con el fichero; Administracion Tributaria; Bancos, cajas de ahorros y cajas rurales; |
| **Transferencias internacionales:** |  |

LOCALIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Los lugares donde se encuentran los sistemas de información, están ubicados en las siguientes direcciones:

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L.

C/ Chile Nº 10, oficina 119

Las Rozas (28290) MADRID

DERECHOS DE LOS INTERESADOS

El afectado podrá ejercitar sus derechos de acceso, rectificación, limitación, portabilidad cancelación u oposición en la siguiente dirección:

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L.

C/ Chile Nº 10, oficina 119

Las Rozas (28290) MADRID

Mail: comercial@gestinser.es

COPIAS DE RESPALDO Y PROCEDIMIENTO DE RECUPERACIÓN

Las copias de respaldo y recuperación de se realizan de acuerdo al siguiente procedimiento y con la periodicidad que se describe a continuación:

|  |  |
| --- | --- |
| **Periodicidad de la copia de seguridad:** | QUINCENAL |
| **Procedimiento para la realización de la copia de respaldo:** | SE REALIZA COPIA EN DISCO DURO EXTERNO |
| **Procedimiento de recuperación de los datos:** | SE RESTAURAN LOS FICHEROS DE LA COPIA DE SEGURIDAD A SU UBICACIÓN ORIGINAL |

CONEXIÓN CON OTROS SISTEMAS

No existen conexiones con otros sistemas.

FUNCIONES DEL PERSONAL CON ACCESO A LOS DATOS PERSONALES

Las diferentes funciones y obligaciones de cada perfil de usuarios que accede al fichero, así como el tipo de acceso que se realiza, se describen aquí:

|  |  |  |
| --- | --- | --- |
| **Perfil** | **Funciones asociadas al perfil** | **Tipo de acceso** |
| GERENCIA | GESTIÓN TOTAL DE LA SOCIEDAD | MIXTO |

APLICACIONES QUE ACCEDEN AL TRATAMIENTO

Las aplicaciones que acceden al fichero y los perfiles que las utilizan, así como los privilegios de que dispone dicho perfil son los siguientes:

|  |  |  |
| --- | --- | --- |
| **Perfil** | **Aplicación** | **Privilegios** |
| GERENCIA | PAQUETE OFFICE | L|A|B|M|I|E |

USUARIOS CON ACCESO AL TRATAMIENTO

La relación actualizada de usuarios con acceso autorizado al fichero es la siguiente:

|  |  |  |  |
| --- | --- | --- | --- |
| **Usuario** | **Perfil** | **F. Alta** | **F. Baja** |
| Julian Ramos Martín | GERENCIA | 01/01/2016 |  |

ANEXO II

MEDIDAS TÉCNICAS Y ORGANIZATIVAS

INVENTARIO DE SOPORTES

|  |  |
| --- | --- |
| **USUARIO** | **DISPOSITIVO** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

ANEXO III

NOMBRAMIENTO Y DELEGACIONES

NOMBRAMIENTO DELEGADO DE PROTECCIÓN DE DATOS

En……………………., a ..... de ...................... de 20...

Yo, Julian Ramos Martín, con DNI , como representante legal de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L., con CIF B81763484 de acuerdo con la normativa vigente de Protección de Datos, nombro como Delegado de Protección de Datos a LOCK4DATA CONSULTORES S.L. con CIF B86750668, haciéndose cargo de las tareas relacionadas a continuación:

* Asesorar e informar a PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. de las obligaciones que le incumben observancia de la normativa vigente en materia de protección datos
* Supervisar el cumplimiento normativo de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. en el tratamiento de datos personales
* Supervisar la implementación y aplicación de las políticas de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. en materia de protección de datos personales
* Supervisar el análisis de las operaciones de tratamiento de datos personales
* Supervisar el análisis de las categorías de datos que trata la Organización
* Supervisar el análisis de los riesgos que puedan derivarse de las operaciones de tratamiento llevadas a cabo por PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L.
* Facilitar el asesoramiento al Responsable de Privacidad o Seguridad en materia de protección de datos
* Impartir plan formativo al personal de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. que realice tratamiento de datos
* Intermediar entre PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L.y la Autoridad de Control
* Realizar las notificaciones requeridas por la Autoridad de Control, concretamente las referidas a la Evaluación de Impacto de Protección de Datos y a las incidencias y brechas de seguridad
* Supervisar la realización de la Evaluación de Impacto de protección de datos personales
* Supervisar la realización de las auditorías correspondientes
* Mantener el secreto y confidencialidad en el desempeño de sus funciones

Firma:

NOMBRAMIENTO RESPONSABLE DE SEGURIDAD

En……………………., a ..... de ...................... de 20...

Yo, Julian Ramos Martín, con DNI , como representante legal de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L., con CIF B81763484 de acuerdo con la normativa vigente de Protección de Datos, nombro como Responsable de Seguridad a Julian Ramos Martín con CIF , cuya figura tiene las siguientes responsabilidades:

* Mantener actualizada la documentación relacionada con la política de protección de datos de la entidad.
* Implantar el plan de formación en materia de protección de datos para los empleados
* Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias que pudieran incurrir en caso de incumplimiento
* Adoptar las medidas correctoras como consecuencia de las deficiencias detectadas en un proceso de auditoría y aprobadas por la entidad
* Mantener una relación del personal autorizado para conceder, anular o alterar los derechos de acceso, conforme con los criterios establecidos
* Mantener una relación del personal con acceso autorizado al lugar dónde se almacenan las copias de seguridad
* Mantener una relación del personal autorizado para acceder a los locales dónde se encuentren ubicados los sistemas de información
* Protocolos de comunicación con el Delegado de Protección de Datos por parte de los empleados
* Adoptar protocolos para el cumplimiento de las medidas de seguridad
* Realizar protocolos para el diseño de flujos de tratamiento de datos
* Informar de las consecuencias del incumplimiento del manual de Medidas y Procedimientos

En prueba de conformidad, firmo el presente documento en el lugar y fecha indicados en el encabezado.

Firma:

ANEXO IV

**AUTORIZACIONES**

AUTORIZACIÓN DE SALIDA FUERA DE LAS INSTALACIONES

|  |
| --- |
| FECHA (1): / /  |
| ENTREGA A (2): |
| Se autoriza a (3) D./Dña para realizar la entrega del soporte con datos personales que se describe a continuación a la empresa que se detalla arriba.La devolución del citado soporte deberá ser registrada cumplimentando el apartado correspondiente de este formulario. |
| RESPONSABLE DEL TRATAMIENTO O DELEGADO (4):Firma: | DATOS DEL RECEPTOR (OPERARIO/TÉCNICO) (5):Firma:Fecha: / /  |
| SOPORTE: |
| MOTIVO DE LA SALIDA: |
| PRECAUCIONES TOMADAS |

DEVOLUCIÓN DE SOPORTE

|  |
| --- |
| Sin devolución [ ] |
| FECHA (6): / / En la fecha señalada se confirma la devolución del soporte con Datos de Carácter Personal que se describe en el apartado anterior. |
| RESPONSABLE DE LA RECEPCIÓN (7):Firma: | RESPONSABLE DE LA ENTREGA (8):Firma: |
| RESPONSABLE DE LA RECEPCIÓN (9):Firma: |

1. Fecha de la autorización.
2. Empresa a la que se va a entregar el soporte.
3. Persona de nuestra empresa autorizada para realizar la entrega del soporte.
4. Nombre, apellidos y firma del Responsable del fichero o delegado para autorizar la salida de soportes y documentos.
5. Nombre y apellidos, firma y fecha de la persona de la otra empresa que recibe el soporte entregado.
6. Fecha de la devolución del soporte.
7. Nombre, apellidos y firma de la persona de nuestra empresa que recoge el soporte devuelto.
8. Nombre, apellidos y firma de la persona de la otra empresa que nos devuelve el soporte.

REGISTRO TRABAJO FUERA DE LOS LOCALES

Relación de los usuarios autorizados a tratar con soportes fuera de las instalaciones

|  |  |  |  |
| --- | --- | --- | --- |
| **USUARIO** | **DISPOSITIVO** | **SALIDA SOPORTE** | **CATEGORIA DE DATOS** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

ANEXO V

GESTIÓN DE USUARIOS

PLAN FORMACION USUARIOS

Resumen de las acciones formativas y previsión de realización

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DEPARTAMENTO** | **PARTICIPANTE** | **HORAS** | **FECHAS** | **ACCION** | **PRIORIDAD** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

ANEXO VI

GESTIÓN DE ENCARGADOS DE TRATAMIENTO

REGISTRO DE ENCARGADOS DE TRATAMIENTO

|  |  |  |  |
| --- | --- | --- | --- |
| **ENCARGADO TRATAMIENTO** | **CIF** | **FINALIDAD** | **CATEGORIAS DATOS** |
| LOCK4DATA CONSULTORES S.L. | B86750668 | SERVICIO DE CONSULTORÍA LOPD |  |

ANEXO VII

BRECHAS DE SEGURIDAD

MODELO NOTIFICACIÓN VIOLACIÓN DE SEGURIDAD

|  |
| --- |
| ***MODELO DE COMUNICACIÓN DELEGADO DE PROTECCIÓN DE DATOS*** |
|  |
| **ENTRADA:………….. DÍA:…… MES:………… AÑO:……… HORA:………** |
| **IDENTIFICACIÓN DEL EMPLEADO QUE REALIZA LA COMUNICACIÓN:**Nombre y Apellidos: DNI/NIE:Cargo:DESCRIPCIÓN DE DUDA, SUGERENCIA, COMUNICACIÓN:1. **COMUNICACIÓN DE VIOLACIÓN DE SEGURIDAD DE LOS DATOS PERSONALES**

2.1.-Descripción de la violación producida:2.2.- Describir las consecuencias probables de la violación de seguridad de los datos personales (en caso de conocerse):1. **RELACIÓN DE DOCUMENTACIÓN ADJUNTADA:**

1.-……………………………………………………………………………..2.-……………………………………………………………………………..3.-……………………………………………………………………………..1. **OTROS COMENTARIOS**
 |
| Fecha envío comunicación Firma comunicador:  |

MODELO RESOLUCIÓN VIOLACIÓN DE SEGURIDAD

|  |
| --- |
| MODELO DE RESOLUCIÓN BRECHA SEGURIDAD |
|  |
| ENTRADA:………….. DÍA:………… MES:……………….…… AÑO:……………… HORA:……… |
| Nº COMUNICACIÓN:DIRIGIDO A:Nombre y Apellidos:DNI/NIE:Cargo:1. DATOS DE REFERENCIA DE LA COMUNICACIÓN
2. CONCLUSIONES DEL ANÁLISIS DE LA OPERACIÓN
3. ACCIONES EFECTUADAS
 |
| Fecha envío resolución Firma DPO / R. Seguridad: |

ANEXO VIII

CLÁUSULAS Y CIRCULARES

CLÁUSULA PARA CONTRATOS

En cumplimiento de la normativa Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPR) y legislación vigente en materia de protección de datos, le informamos que sus datos serán incorporados al sistema de tratamiento de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. con CIF B81763484 y domicilio social en C/ Chile Nº 10, oficina 119 - Las Rozas (28290) con la finalidad de atender los compromisos derivados del presente contrato suscrito entre ambas partes.

El tratamiento de los datos queda legitimado en ejecución del presente contrato. PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. no elaborará perfiles automatizados con los datos aportados. Sus datos serán tratados durante un periodo no superior a cinco años.

A su vez le informamos que puede contactar con el Delegado de Protección de Datos dirigiéndose por escrito a la dirección de correo electrónico dpo.gestinser@lock4data.es

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada comprometiéndose a adoptar las medidas de seguridad razonables para suprimir o rectificar estos cuando sean inexactos.

Sus datos podrán ser comunicados a administraciones públicas o a terceros, siempre que sea necesario para la prestación del servicio o bien exista alguna previsión legal.

Podrá revocar el consentimiento prestado en todo momento, dirigiéndose por escrito a C/ Chile Nº 10, oficina 119 - Las Rozas (28290) así como dirigirse a la Autoridad de control competente para presentar la reclamación que considere oportuna.

De acuerdo con los derechos que le confiere la normativa vigente en protección de datos de carácter personal, podrá revocar el consentimiento prestado así como ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición dirigiendo su petición a la dirección postal C/ Chile Nº 10, oficina 119 - Las Rozas (28290). También podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna. Puede ampliar la información sobre nuestra política de protección de datos en www.gestinser.es

CLAUSULA CONTESTACIÓN CURRICULUM VITAE

En cumplimiento de la normativa Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPR) y legislación vigente en materia de protección de datos, le informamos que sus datos serán incorporados al sistema de tratamiento de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. con CIF B81763484 y domicilio social en C/ Chile Nº 10, oficina 119 - Las Rozas (28290) con la finalidad de formar parte en los procesos de selección de personal llevados a cabo por la entidad.

El tratamiento de los datos queda legitimado en ejecución del consentimiento prestado y matriculación de acciones formativas. PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. no elaborará perfiles automatizados con los datos aportados. Sus datos serán conservados durante el periodo de tiempo que exista la candidatura para la cual se presenta, no siendo más de un año desde la última muestra de interés por su parte.

A su vez le informamos que puede contactar con el Delegado de Protección de Datos dirigiéndose por escrito a la dirección de correo electrónico dpo.gestinser@lock4data.es

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada comprometiéndose a adoptar las medidas de seguridad razonables para suprimir o rectificar estos cuando sean inexactos.

Podrá revocar el consentimiento prestado en todo momento, dirigiéndose por escrito a C/ Chile Nº 10, oficina 119 - Las Rozas (28290) así como dirigirse a la Autoridad de control competente para presentar la reclamación que considere oportuna.

De acuerdo con los derechos que le confiere la normativa vigente en protección de datos de carácter personal, podrá revocar el consentimiento prestado así como ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición dirigiendo su petición a la dirección postal C/ Chile Nº 10, oficina 119 - Las Rozas (28290). También podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna. Puede ampliar la información sobre nuestra política de protección de datos en www.gestinser.es

CLAUSULA CORREO ELECTRÓNICO

La información contenida en este mensaje y/o archivo(s) adjunto(s), enviada desde PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L., es confidencial/privilegiada y está destinada a ser leída sólo por la(s) persona(s) a la(s) que va dirigida.

Le recordamos que sus datos han sido incorporados en el sistema de tratamiento de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. y que siempre y cuando se cumplan los requisitos exigidos por la normativa, usted podrá ejercer sus derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición/revocación, en los términos que establece la normativa vigente en materia de protección de datos, dirigiendo su petición a la dirección postal C/ Chile Nº 10, oficina 119 - Las Rozas (28290) o bien a través de correo electrónico dpo.gestinser@lock4data.es

Si usted lee este mensaje y no es el destinatario señalado, el empleado o el agente responsable de entregar el mensaje al destinatario, o ha recibido esta comunicación por error, le informamos que está totalmente prohibida, y puede ser ilegal, cualquier divulgación, distribución o reproducción de esta comunicación, y le rogamos que nos lo notifique inmediatamente y nos devuelva el mensaje original a la dirección arriba mencionada. Gracias.

CLAUSULA FICHAS CLIENTES

En cumplimiento de la normativa Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPR) y legislación vigente en materia de protección de datos, le informamos que sus datos serán incorporados al sistema de tratamiento de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. con CIF B81763484 y domicilio social en C/ Chile Nº 10, oficina 119 - Las Rozas (28290) con la finalidad de realizar la gestión comercial, administrativa, fiscal y contable.

El tratamiento de los datos queda legitimado en ejecución del consentimiento prestado por usted con la firma del presente documento. PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. no elaborará perfiles automatizados con los datos aportados. Sus datos serán conservados durante un periodo máximo de 5 años desde la última muestra de interés por su parte

A su vez le informamos que puede contactar con el Delegado de Protección de Datos dirigiéndose por escrito a la dirección de correo electrónico dpo.gestinser@lock4data.es

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada comprometiéndose a adoptar las medidas de seguridad razonables para suprimir o rectificar estos cuando sean inexactos.

Podrá revocar el consentimiento prestado en todo momento, dirigiéndose por escrito a C/ Chile Nº 10, oficina 119 - Las Rozas (28290) así como dirigirse a la Autoridad de control para presentar la reclamación que considere oportuna

De acuerdo con los derechos que le confiere la normativa vigente en protección de datos de carácter personal, podrá revocar el consentimiento prestado así como ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición dirigiendo su petición a la dirección postal C/ Chile Nº 10, oficina 119 - Las Rozas (28290). Puede ampliar la información sobre nuestra política de protección de datos en www.gestinser.es

En \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ a \_\_\_\_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_

Firma:

Nombre:

DNI:

CLAUSULA PARA FICHAS DE ALUMNOS

En cumplimiento de la normativa Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPR) y legislación vigente en materia de protección de datos, le informamos que sus datos serán incorporados al sistema de tratamiento de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. con CIF B81763484 y domicilio social en C/ Chile Nº 10, oficina 119 - Las Rozas (28290) con la finalidad de realizar los trámites necesarios para el desarrollo, seguimiento y gestión de las acciones formativas.

El tratamiento de los datos queda legitimado en ejecución del consentimiento prestado y matriculación de acciones formativas. PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. no elaborará perfiles automatizados con los datos aportados. Sus datos serán tratados durante un periodo no superior a cinco años desde la última muestra de interés por su parte.

A su vez le informamos que puede contactar con el Delegado de Protección de Datos dirigiéndose por escrito a la dirección de correo electrónico dpo.gestinser@lock4data.es

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada comprometiéndose a adoptar las medidas de seguridad razonables para suprimir o rectificar estos cuando sean inexactos.

Sus datos podrán ser comunicados a administraciones públicas o a terceros, siempre que sea necesario para la prestación del servicio o bien exista alguna previsión legal.

Podrá revocar el consentimiento prestado en todo momento, dirigiéndose por escrito a C/ Chile Nº 10, oficina 119 - Las Rozas (28290) así como dirigirse a la Autoridad de control competente para presentar la reclamación que considere oportuna.

De acuerdo con los derechos que le confiere la normativa vigente en protección de datos de carácter personal, podrá revocar el consentimiento prestado así como ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición dirigiendo su petición a la dirección postal C/ Chile Nº 10, oficina 119 - Las Rozas (28290). También podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna. Puede ampliar la información sobre nuestra política de protección de datos en www.gestinser.es

CLAUSULA PARA SOLICITANTES EMPLEO

En cumplimiento de la normativa Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPR) y legislación vigente en materia de protección de datos, le informamos que sus datos serán incorporados al sistema de tratamiento de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. con CIF B81763484 y domicilio social en C/ Chile Nº 10, oficina 119 - Las Rozas (28290) con la finalidad de realizar la selección de candidatos para los puestos laborales de la entidad.

El tratamiento de los datos queda legitimado en ejecución de la candidatura realizada por usted para optar a un puesto laboral en la entidad. PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. no elaborará perfiles automatizados con los datos aportados. Sus datos serán conservados durante el periodo de selección a la candidatura a la que se haya presentado

A su vez le informamos que puede contactar con el Delegado de Protección de Datos dirigiéndose por escrito a la dirección de correo electrónico dpo.gestinser@lock4data.es

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada comprometiéndose a adoptar las medidas de seguridad razonables para suprimir o rectificar estos cuando sean inexactos.

Podrá revocar el consentimiento prestado en todo momento, dirigiéndose por escrito a C/ Chile Nº 10, oficina 119 - Las Rozas (28290) así como dirigirse a la Autoridad de control para presentar la reclamación que considere oportuna

De acuerdo con los derechos que le confiere la normativa vigente en protección de datos de carácter personal, podrá revocar el consentimiento prestado así como ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición dirigiendo su petición a la dirección postal C/ Chile Nº 10, oficina 119 - Las Rozas (28290). Puede ampliar la información sobre nuestra política de protección de datos en www.gestinser.es

 Consiento la comunicación de mis datos a empresas del grupo para futuras selecciones.

En \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ a \_\_\_\_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_

Firma:

NOTA INFORMATIVA CLIENTES

Apreciado cliente:

En cumplimiento de la normativa Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPD) y legislación vigente en materia de protección de datos, le informamos que sus datos serán incorporados al sistema de tratamiento de PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. con CIF B81763484 y domicilio social en C/ Chile Nº 10, oficina 119 - Las Rozas (28290) con la finalidad de poder atender los compromisos generados por la relación comercial que mantenemos con usted.

El tratamiento de los datos queda legitimado en ejecución del contrato de prestación de servicios en vigor. PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. no elaborará perfiles automatizados con los datos aportados. Sus datos serán conservados durante el periodo legalmente establecido legalmente.

A su vez le informamos que puede contactar con el Delegado de Protección de Datos dirigiéndose por escrito a la dirección de correo electrónico dpo.gestinser@lock4data.es

PLATAFORMA GESTION INTEGRAL DE SERVICIOS S.L. informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada comprometiéndose a adoptar las medidas de seguridad razonables para suprimir o rectificar estos cuando sean inexactos.

Podrá revocar el consentimiento prestado en todo momento, dirigiéndose por escrito a C/ Chile Nº 10, oficina 119 - Las Rozas (28290) así como dirigirse a la Autoridad de control

De acuerdo con los derechos que le confiere la normativa vigente en protección de datos de carácter personal, podrá revocar el consentimiento prestado así como ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición dirigiendo su petición a la dirección postal C/ Chile Nº 10, oficina 119 - Las Rozas (28290). También podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna. Puede ampliar la información sobre nuestra política de protección de datos en www.gestinser.es