DOCUMENTO DE PRIVACIDAD

APLICACIÓN CORRESPONDIENTE AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS
(Reglamento 679/2016 UE)

RALARSA HOLDING S.L.

ELABORADO para	REVISADO	APROBADO
AULA TECNOMEDIA, S.L.U.	RALARSA HOLDING S.L.	04/10/2018

ÍNDICE

1.- OBJETIVO Y PRINCIPIOS DE ESTE DOCUMENTO

El objetivo de este documento de Privacidad es el de describir las medidas, normas, procedimientos, reglas y estándares de seguridad que la Entidad acomete sobre el ámbito de aplicación de cualquier tipo de soporte, tanto si es informatizado como si no, para garantizar la seguridad de los datos de carácter personal evitando su alteración, pérdida, tratamiento o acceso no autorizado.

El personal afectado por este Documento de Privacidad conoce y debe cumplir la parte del mismo que afecta al desarrollo de sus funciones.

El personal afectado por este Documento de Privacidad debe ser consciente de la necesidad de preservar la información y de las consecuencias de acciones inapropiadas, en este sentido, pueden ocasionar a la Entidad.

La Entidad ha efectuado un análisis de riesgo de los tratamientos que lleva a cabo con afectación a datos personales, y ha aplicado las medidas de seguridad correspondientes con el objeto de minimizar los riesgos del tratamiento. En este documento se plasman y establecen las medidas de seguridad y procedimientos que afectan a los tratamientos que contienen datos personales en cualquier tipo de soporte.

El objetivo es proporcionar los controles eficaces que aseguren que los datos de la entidad no están sujetos a pérdida, difusión o modificación no autorizada. Para ello se han definido las medidas, normas, reglas y procedimientos de seguridad que permiten obtener y mantener el nivel de seguridad de la información adecuado a la criticidad de los datos y procesos que se almacenan y gestionan en la Entidad.

El Documento de Privacidad deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El Responsable del tratamiento deberá de ser el encargado de mantener actualizado el Documento de Privacidad, así como de comunicar las modificaciones en las que personal de la entidad pueda verse afectado.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a las sanciones disciplinarias que contemple la normativa laboral en cada momento y a salvo de derecho de repetición de daños y perjuicios generados a la entidad tanto por lucro cesante como por daño emergente.

2.- ÁMBITO DE APLICACIÓN DEL DOCUMENTO DE PRIVACIDAD.

2.1. Ámbito Jurídico.

Este documento se aplica a:

RALARSA HOLDING S.L.

B65467490

En adelante la Entidad.

2.2. Ámbito Personal.

Este Documento de Privacidad es de obligado cumplimiento para todo el personal de la entidad o personal externo que tenga acceso a los datos de carácter personal que son responsabilidad de la entidad. Las normas internas contenidas en los puntos 3 y 4 del presente documento se han puesto en conocimiento de todo el personal con acceso a datos de carácter personal y se incluyen en la documentación a entregar al personal en el momento de la contratación, con el objeto de dar debido cumplimiento al Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016.

2.3. Ámbito Material.

Las presentes normas de seguridad son de aplicación a los recursos protegidos. Un recurso es cualquier parte componente de un sistema de información. Se pueden identificar como recursos protegidos los siguientes componentes:

- Tratamientos automatizados.
- Aplicaciones informáticas, bases de datos y sistemas operativos.
- Plataformas, equipos, sistemas de soporte y tratamiento de datos.
- Equipos y sistemas de comunicaciones.
- Edificios.
- Expedientes y repositorios de información en soporte papel.

El ámbito de aplicación abarca los sistemas y/o soportes que de alguna forma participan en el almacenamiento o tratamiento de los tratamientos que contienen datos de carácter personal de la entidad.

La descripción detallada de las aplicaciones informáticas, bases de datos, sistemas operativos, sistemas de soporte, servidores, equipos, sistemas de comunicaciones y usuarios que componen la infraestructura de la informática de la Entidad, se encuentra descrita en el ANEXO 1 “Descripción de los Sistemas de Información”.

La descripción detallada de los soportes y repositorios en soporte papel, se encuentran descritos en el ANEXO 1.

Las medidas de seguridad se aplican según el análisis de los riesgos y atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información:

- *Nivel ordinario: Se aplicarán a todos los tratamientos con datos de carácter personal.*
- *Nivel avanzado: Se aplicará a los tratamientos que contengan datos personales de especial protección.*

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

DATOS Y TRATAMIENTOS.

TRATAMIENTO	OBJETO	CATEGORÍAS	CÓDIGO
TRATAMIENTO DE RECURSOS HUMANOS	Gestión de la selección y prestación de servicios del personal	C1, C3, C4, C5, C6, C7, C8, C11	1
TRATAMIENTO DE PROVEEDORES	Gestión de las obligaciones contractuales	C1, C3, C7, C8	2
TRATAMIENTO DE CLIENTES	Gestión de las obligaciones contractuales, atención al cliente y envío de comunicaciones comerciales	C1, C3, C5, C7, C8, C11	3
TRATAMIENTO DE ASEGURADOS	Gestión de las obligaciones contractuales	C1, C2, C3,	4
TRATAMIENTO DE AGENTES	Gestión de las obligaciones contractuales	C1, C3 C5, C6, C7, C8, C11	5
TRATAMIENTO PÁGINA WEB	Gestión de las solicitudes de cita previa	C1, C2, C3	6
TRATAMIENTO CANDIDATOS	Gestión de la selección de personal	C1, C5, C6, C7	7

FLUJOS DE DATOS

ÁREAS DE ACTIVIDAD	DESCRIPCIÓN	TRATAMIENTOS
Gerencia	Supervisión de las acciones y buen uso.	1,2,3,4,5,6,7
Trabajadores	Ejercicio de funciones	2,3,4,5,6
Sistemas	Gestión, soporte y/ mantenimiento de los sistemas de información obrantes en la organización.	1,2,3,4,5,6,7
Ventas/Comercial	Ejercicio de funciones	2,3,4,5
Contabilidad / Dirección financiera	Gestión de la contabilidad mercantil de la entidad	2,3
Márquetin	Gestión de la página web, blog, redes sociales, emailing, auditorías internas, etc.	6
Atención al cliente	Gestión directa con las necesidades del cliente asociadas al servicio	3,4
Recursos humanos	Gestión del personal actual y de los candidatos	1,2,3,4,5,6,7

IDENTIFICACIÓN DE LA EMPRESA O INSTITUCIÓN:

Razón Social o Nombre de la Empresa		**CIF**
RALARSA HOLDING S.L.		B65467490
Dirección:		
Ctra. Terrassa a Rubí, Km. 19,3		
Población:		**Código Postal:**
Sant Quirze del Vallès		08192
Provincia:	**Estado / País:**	
Barcelona	España	
Tel/e-mail:	**Fax:**	
902222722	_	
Actividad económica:	**Código CNAE:**	
mantenimiento y reparación de vehículos de motor	4520	
Persona responsable	**Cargo.**	
Joan Jordi Arsalaguet	Director General	
DNI		
38138354-F		

IDENTIFICACIÓN EMPRESA ASESORA

Razón Social o Nombre de la Empresa		**CIF**
AULA TECNOMEDIA, S.L.U.		B64064991
Dirección:		
Av. Meridiana, 358 P.4 Ptas. A y B		
Población:		**Código Postal:**
Barcelona		08027
Provincia:	**Estado / País:**	
Barcelona	España	
Tel/e-mail:	**Fax:**	
933453395	933453395	
Actividad económica:	**Código CNAE:**	
Consultoría empresarial y otros	8299	
Persona responsable	**Cargo.**	
Lic. Jorge Ortega	Director técnico	
DNI / N.º identificación profesional		
26546		

3.- MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES DE SEGURIDAD.

Con el objeto de dar debido cumplimiento al Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016, la Entidad ha establecido las siguientes medidas de seguridad, que deben ser conocidas, aceptadas, cumplidas y respetadas por todo el personal.

3.1. Registro y autorización de tratamientos con datos de carácter personal.

Los procedimientos que la Entidad sigue en el registro y autorización de los tratamientos con datos de carácter personal se describen en el ANEXO 9 “Procedimiento de Registro y Autorización de Tratamientos”.

3.2. Identificación y autenticación.

1. La entidad identifica y autentica a los usuarios que acceden a su Sistema de Información.

2. El Delegado de Protección de Datos supervisa para cada uno de los sistemas y de las aplicaciones, las altas, bajas y modificaciones de los accesos de los usuarios.

3. Dada la importancia de los accesos de los usuarios al Sistema de Información, el Responsable de Privacidad puede disponer en todo momento de una relación actualizada de los usuarios que tienen acceso autorizado a los Sistemas de Información.

4. Una vez realizada la creación de un usuario es necesario comunicar los datos de acceso (identificador de usuario y clave de acceso) al usuario solicitante.

5. Asimismo, es muy importante para asegurar la integridad y confidencialidad de la información, la existencia de una política de mantenimiento de claves de acceso. Para ello se detallan a continuación las siguientes normas:

    - No debe permitir la introducción de caracteres en blanco en la contraseña.
    - No debe permitir utilizar ninguna de las últimas 12 contraseñas anteriores.
    - No debe permitir que el código de usuario sea igual a la contraseña.
    - No debe permitir visualizar la contraseña al personal informático.
    - Las contraseñas deben caducar cada mes o cada 3 como máximo.
    - El usuario debe poder cambiarse la contraseña a voluntad.
    - Las contraseñas han de contener caracteres alfanuméricos.

3.3. Control de acceso y confidencialidad de la información.

1. Toda la información albergada en la red corporativa de la Entidad, de forma estática o circulando en forma de mensajes de correo electrónico, o en cualquier otro tipo de soporte físico, es propiedad de la entidad y tiene por tanto carácter de confidencial.

2. Exclusivamente el Delegado de Protección de Datos está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.

3. El Delegado de Protección de Datos identifica a sus usuarios y verifica que estos accedan, únicamente, a la información y a los recursos que precisen para su operativa diaria en función del puesto que ocupen. De esta forma existen procedimientos para asegurar que los distintos usuarios sólo accedan a la información confidencial indispensable para llevar a cabo sus funciones.

4. Adicionalmente los sistemas de la Entidad están configurados para limitar la posibilidad de intentar, reiteradamente, el acceso no autorizado a los mismos.

5. La/s persona/s destinada/s a seguridad se encargará/n de determinar, implantar, gestionar, autorizar, inspeccionar o revalidar, según los casos, el conjunto de medios y medidas de seguridad, así como las normas y procedimientos que aseguren el control de acceso físico a los locales.

6. Los espacios físicos que contengan soportes con datos de carácter personal estarán adecuadamente protegidos mediante las medidas de seguridad adecuadas.

3.4. Gestión de soportes.

En el ANEXO 4 “Gestión de Soportes” se describe el procedimiento de identificación, inventario y custodia de los soportes de la Entidad que contiene datos de carácter personal. Este procedimiento ha sido definido con el objetivo de permitir identificar el tipo de información que contienen dichos soportes. El ANEXO 4 “Gestión de Soportes”, especifica una relación de personas con acceso autorizado a dichos soportes.

Únicamente el Responsable del Tratamiento o el Delegado de Protección de Datos, en el caso de estar delegado esa función, puede autorizar la salida de soportes que contienen datos personales, fuera de los locales en los que esté ubicado el tratamiento.

3.5. Modificación de datos del Sistema de Información.

Se entiende por modificación de datos el cambio de cualquier dato de aplicación realizado de forma directa o indirecta, mediante cualquier herramienta de software, que no sea la aplicación propia para el tratamiento de los datos, por los usuarios de la misma y utilizando permisos o herramientas no habituales en la operativa diaria. Estos procedimientos se describen en el ANEXO 5 “Copias de Respaldo y Recuperación de Datos”.

3.6. Gestión de tratamientos temporales.

En el ANEXO 7 “Tratamientos Temporales” se describe el tratamiento que realiza la Entidad de los tratamientos temporales que contengan datos de carácter personal.

3.7. Portabilidad, acceso, rectificación, supresión, oposición y limitación al tratamiento.

En el ANEXO 8 “Procedimiento de Ejercicio de los Derechos” se describen los procedimientos para ejercer los derechos de portabilidad, acceso, rectificación, supresión, oposición y limitación al tratamiento sobre datos personales.

3.8. 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 garantizan un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

3.9. Régimen de trabajo fuera de los locales de la ubicación del tratamiento.

La ejecución de tratamientos de datos de carácter personal fuera de los locales de la ubicación del tratamiento deberá ser autorizada expresamente por el responsable del tratamiento y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de tratamiento tratado.

Es preciso crear una operativa que especifique punto por punto los trámites realizados para garantizar la seguridad de los tratamientos fuera de la organización.

EJEMPLO:

Fecha y hora de la ejecución

Nombre del Usuario
Encargado del tratamiento
Duración del tratamiento fuera de la organización
Tratamientos
Fecha y hora de salida
Autorización

4.- FUNCIONES Y OBLIGACIONES DEL PERSONAL.

Con el objeto de dar cumplimiento a lo establecido en el Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016, la Entidad ha establecido una serie de obligaciones que deberán ser conocidas, aceptadas, cumplidas y respetadas por el 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, con acuse de recibo, de acuerdo con lo estipulado en el Documento "Comunicado Interno" disponible en el Anexo 14D del presente Documento de Privacidad.

Asimismo, la Entidad, mediante su Delegado de Protección de Datos, irá informando periódicamente al personal de las novedades sobre seguridad en el trato de los datos de carácter personal.

En el ANEXO 2 "Funciones y Obligaciones del Personal" se describen las funciones y obligaciones del personal referentes a la RGPD y se identifica a los diferentes responsables surgidos en materia PDP.

5.- ESTRUCTURA DE LOS TRATAMIENTOS DE LA COMPAÑÍA Y DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE LOS TRATAN.

Con el objeto de dar cumplimiento a lo establecido en el Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016, la Entidad declara la estructura de sus tratamientos y describe los Sistemas de Información que los tratan.

En el ANEXO 3 “Estructura de los Tratamientos de Datos” aparece la estructura y la descripción de datos personales incluidos en los tratamientos llevados a cabo por la Entidad.

La descripción de los Sistemas de Información que tratan dichos tratamientos aparece en el ANEXO 1 “Descripción de los Sistemas de Información”.

6.- NORMATIVA DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS.

Con el objeto de dar debido cumplimiento a lo establecido en el Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016, la Entidad dispone de la siguiente normativa de notificación, gestión y respuesta de las incidencias, entendiendo por "*incidencia*" cualquier anomalía que afecte o pueda afectar a la seguridad o integridad de los datos. El detalle del procedimiento se encuentra en el ANEXO 6 "Gestión de Incidencias".

6.1. Notificación.

Cualquier persona que forme parte de la plantilla de la Entidad o se halle prestando sus servicios temporalmente en la misma, debe notificar inmediatamente al Delegado de Protección de Datos cualquier anomalía que detecte y que afecte o pueda afectar a la seguridad de los datos. El retraso en la notificación de incidencias constituye un quebranto a la buena fe contractual, entre otras posibles infracciones, sancionable según las normas laborables y/o mercantiles de aplicación.

6.2. Gestión.

El Delegado de Protección de Datos debe registrar la incidencia en la aplicación correspondiente y dirigirla al responsable de su resolución.

6.3. Respuesta.

El Responsable de Resolución, debe dar respuesta a la incidencia en el menor tiempo posible, garantizando en todo momento que la seguridad e integridad de los datos no se vea comprometida. Una vez subsanada la incidencia se informará al Responsable del Tratamiento.

6.4. Registro.

Deberá crearse un registro en el cual se haga constar lo siguiente:

- Tipo de incidencia y momento en el cual se ha producido
- Persona que realiza y la que recibe la notificación
- Efectos derivados de dicha notificación

Es obligación del Responsable del Tratamiento velar por el mantenimiento actualizado del registro de incidencias.

7.- PROCEDIMIENTO DE REALIZACIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE DATOS.

Con el objeto de dar debido cumplimiento a lo establecido en el Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016, la Entidad dispone de un procedimiento de realización de copias de respaldo y recuperación de datos que garantiza su reconstrucción en el estado que se encontraban al tiempo de producirse la pérdida o destrucción.

Dicho procedimiento consiste en la realización de copias, con periodicidad diaria, semanal, mensual y anual.

Para más detalle sobre el procedimiento ver el ANEXO 5 “Copias de Respaldo y Recuperación de Datos”.

8.- MEDIDAS ADICIONALES DE NIVEL AVANZADO.

Las medidas que a continuación se describen, serán de aplicación a los tratamientos de nivel de seguridad avanzado indicados en el ANEXO 3 “Estructura de los Tratamientos de Datos”.

8.1. Identificación y autenticación.

El responsable del Tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

8.2. Control de acceso y confidencialidad de la información.

La posibilidad de intentar reiteradamente el acceso no autorizado al sistema estará limitada mediante un sistema que impedirá realizar múltiples intentos de acceso fallidos de forma consecutiva.

8.3. Control de acceso físico.

El acceso a los locales donde se encuentran ubicados los sistemas de información y/o los soportes no digitales que contienen datos de carácter personal, está limitado mediante un sistema de control de acceso físico que restringe la entrada al personal autorizado.

8.4 Relación del personal autorizado.

Únicamente el personal autorizado tiene acceso a las dependencias donde se albergan los sistemas de información y/o los soportes no digitales que contienen datos de carácter personal. La relación de dicho personal autorizado se encuentra en el Anexo 2 del presente Documento de Privacidad.

Cuando personal ajeno a la Entidad deba de entrar por motivos profesionales en los locales donde se encuentran ubicados los sistemas de información y/o los soportes que contienen datos de carácter personal, deberá de ser acompañado por un responsable designado por el responsable del tratamiento. Asimismo, dichos profesionales deberán de firmar un contrato de confidencialidad con la entidad para mantener la privacidad de los datos personales a los que pudieran acceder.

8.5 Gestión de soportes.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los tratamientos como consecuencia de operaciones de mantenimiento, se adoptarán las medidas descritas en el ANEXO 4 “Gestión de Soportes”, para impedir cualquier recuperación indebida de la información almacenada en ellos.

8.6 Control interno y auditoría.

1. Control Interno. De forma continuada y con una frecuencia mínima de una vez al año, el Delegado de Protección de Datos llevará a cabo un seguimiento para verificar el cumplimiento de lo dispuesto en el presente Documento de Privacidad.

2. Auditoria. De forma periódica, y según lo establecido en el Análisis del Riesgo, el Plan de Evaluación de Impacto, y el Plan de Acción Ejecutivo, se realizarán los controles internos y externos de los sistemas de información e instalaciones de tratamiento de datos para verificar el cumplimiento del Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016

El informe de auditoría dictaminará sobre la adecuación de las medidas y controles, identificando deficiencias y proponiendo las medidas correctoras o complementarias necesarias.

Los informes de auditoría serán analizados por quien se determine en cada momento, siendo supervisados por el Delegado de Protección de Datos que elevará las conclusiones al

Responsable del Tratamiento, para que adopte las medidas correctoras necesarias y quedarán a disposición de la Agencia de Protección de Datos.

8.7 Funciones del Responsable del Tratamiento.

Las Funciones del Responsable del Tratamiento de aplicación a los tratamientos aparecen en el ANEXO 2 “Funciones y Obligaciones del Personal”.

8.8 Funciones del Delegado de Protección de Datos.

Las Funciones del Delegado de Protección de Datos, aparecen en el ANEXO 2 “Funciones y Obligaciones del Personal”, y en el Acta de Designación del mismo.

8.9 Procedimiento de notificación, gestión y respuesta ante las incidencias.

Para la ejecución de los procedimientos de recuperación se precisará la autorización por escrito del responsable del tratamiento.

8.10 Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten tratamientos con datos de carácter personal, no se realizarás con datos reales, salvo que se asegure la aplicación de medidas de seguridad que permitan asegurar la falta de riesgo o la minimización del mismo de forma similar al tratamiento homónimo de producción.

9.- MEDIDAS ADICIONALES EN TRATAMIENTOS DE DATOS ESPECIALES.

Las medidas que a continuación se describen, serán de aplicación a los tratamientos de datos especiales indicados en el ANEXO 3 “Estructura de los Tratamientos de Datos”, únicamente en el caso de que la Entidad llegue a tener tratamientos con esta calificación.

9.1. Control de acceso y confidencialidad de la información digital.

1. De cada acceso se guardarán, la identificación del usuario, fecha y hora, el tratamiento accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. Si ha sido autorizado, se guarda en el registro de accesos que permite identificar el registro accedido.

3. No se permite desactivar los mecanismos de registro de accesos, que controla el Delegado de Protección de Datos.

4. Los datos del registro de accesos se guardarán durante 2 años.

5. El Delegado de Protección de Datos se encargará de realizar revisiones, con periodicidad mensual, de la información de control registrada, elaborando un informe de las revisiones realizadas y los problemas detectados.

9.2. Gestión de soportes.

La distribución de los soportes que contienen datos personales, se realiza cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Estos soportes estarán identificados mediante algún sistema de etiquetado comprensible y con significado que permita a los usuarios con acceso autorizados a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas

Se evitará el tratamiento de datos de carácter personal en dispositivos portátiles que no permita su cifrado. En caso de que fuera estrictamente necesario se hará constar motivadamente en el presente Documento de Privacidad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

9.3. Control de los accesos físicos.

Exclusivamente el personal autorizado en el documento de Privacidad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información (Modelo en Anexo 2, página 26).

En caso de tratarse de soportes no digitales, el acceso a la documentación se limitará exclusivamente al personal autorizado (Modelo en Anexo 2, página 26).

Se establecerán mecanismos que permita identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

Cuando accedan personas no autorizadas a datos de nivel alto, deberá quedar adecuadamente registrado en el Documento de Privacidad (Modelo en ANEXO 1 "Descripción de los Sistemas de Información".

9.4. Telecomunicaciones.

La transmisión de datos de carácter personal de nivel alto a través de redes de telecomunicaciones, se realiza cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada por terceros.

9.4.1. Modelo de registro de transmisión de datos de carácter personal de nivel alto.

Datos transmitidos
Método de Cifrado
Fecha y hora de la transmisión

9.5. Funciones del Delegado de Protección de Datos.

Las Funciones del Delegado de Protección de Datos, aparecen en el ANEXO 2 "Funciones y Obligaciones del Personal".

9.6. Procedimiento de realización de copias de respaldo y recuperación de datos.

Se conserva una copia de respaldo y de los procedimientos de recuperación de los datos en lugar diferente de aquél en que se encuentran los equipos informáticos que los tratan, cumpliendo en todo caso las medidas de seguridad exigidas en el Reglamento General de Protección de Datos 2016/679 del Parlamento Europeo y del Consejo de 27 abril de 2016.

9.7. Modelo de registro mensual sobre "Log de accesos".

El acceso a datos de carácter personal de nivel alto, en caso de producirse, será registrado en un informe mensual en el que deberán constar los siguientes datos.

EJEMPLO:

Nombre del Tratamiento
Fecha y hora en que se realizó el acceso
Tratamiento accedido
Tipo de acceso y si ha obtenido autorización
Registro Accedido
Gestiones realizadas en el tratamiento
Autorización Delegado de Protección de Datos

10.- RELACIÓN DE ANEXOS

Anexo 1 Descripción de los Sistemas de Información.

Anexo 2 Funciones y Obligaciones del Personal. Procesos vinculados al DPD

Anexo 3 Estructura de los Tratamientos de Datos. Análisis de Riesgos y PEI.

Anexo 4 Gestión de Soportes.

Anexo 5 Copias de Respaldo y Recuperación de Datos.

Anexo 6 Gestión de Incidencias.

Anexo 7 Tratamientos Temporales.

Anexo 8 Procedimiento de Ejercicio de los Derechos PARSOL y otros.

Anexo 9 Registro de Actividades de Tratamientos.

Anexo 10 Inventario de Contratos.

Anexo 11 Procedimientos y Modelos.

Anexo 12 Documentación Oficial

Anexo 13 Circuito Cerrado de Televisión (CCTV)

Anexo 14 Misceláneos

Anexo 15 Entorno web