DOCUMENTO DE SEGURIDAD

AUDITORÍA SEGÚN RGPD 2016/679 Y LEY 03/2018 DE PROTECCIÓN DE DATOS Y GARANTÍAS Y DERECHOS DIGITALES (LOPDGDD)

REISPORT DEPORTIVA INTEGRAL S.L.

Fecha del documento: 22 / 05 / 2024

Adaptación realizada por:

CONSULTORÍA EMPRESARIAL
VALEGAL ESPAÑA

DOCUMENTO DE SEGURIDAD DE:

REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.

Para el cumplimiento del Reglamento General de Protección de Datos (RGPD) (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Adaptación realizada por:

VALEGAL ESPAÑA S.L.U.

Versión: 1 **Fecha: 15 / 05 / 2024**

INTRODUCCIÓN

El objeto del presente documento es recoger las medidas de seguridad establecidas por el responsable del tratamiento para todo el personal con acceso a los datos de carácter personal que se mantienen automatizados, así como para los sistemas de información.

Debido a la continua evolución y cambios intrínsecos de los sistemas de información y a la propia complejidad de la organización, el documento intentará ser un marco estable, y a su vez, flexible, en lugar de una descripción estática, en cuyo caso se vería sometido a continuas actualizaciones.

El presente documento se mantendrá en todo momento actualizado por el Responsable del Tratamiento y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

De igual forma, el Documento de Seguridad se adecuará, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

DOCUMENTO DE SEGURIDAD

El documento deberá contener, como mínimo:
-Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
-Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar la seguridad de los datos personales.
-Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal.
-Estructura de los tratamientos de datos de carácter personal y descripción de los sistemas de información que los tratan.
-Procedimiento de notificación, gestión y respuesta ante las incidencias o violaciones de seguridad.
-Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
-Las medidas que sea necesario adoptar para el transporte de soportes, así como para su destrucción y reutilización.
-Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los tratamientos que se traten en concepto de encargado y se deberá firmar un contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

INDICE GENERAL

3) DOCUMENTO DE SEGURIDAD

1. Ámbito de aplicación del documento.
2. Funciones / obligaciones del personal.
3. Medidas, normas y procedimientos.
4. Violaciones de Seguridad y Gestión de Incidencias.
5. Contraseñas y copias de seguridad.
6. Gestión de soportes y documentos.
7. Tratamientos.
8. Controles periódicos / auditorías.
9. Encargados de tratamiento.

1) ÁMBITO DE APLICACIÓN DEL DOCUMENTO

REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L., como consecuencia de las actividades desarrolladas dentro de su actividad, necesariamente trata información y datos de carácter personal.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los datos de carácter personal sometidos a tratamiento por REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L., y las aplicaciones, herramientas de actualización y consulta, y sistemas que tratan los datos de carácter personal, los equipos informáticos que las soportan, los dispositivos de archivo y los locales donde estos se ubican.

En los anexos del presente Documento se recoge:

- Información de los tratamientos llevados a cabo por el responsable y su entorno.

- Descripción de las instalaciones y estructura informática.

- Descripción de las políticas de acceso a los datos, medidas de seguridad implantadas en los sistemas y definición de los procedimientos de copias de seguridad.

Este documento ha sido elaborado bajo la responsabilidad de REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L., quien, como Responsable del Tratamiento, se compromete a implantar y actualizar la normativa de Seguridad que de él se desprende. Dicha normativa será de obligado cumplimiento para todo el personal que tenga acceso a los datos de carácter personal y/o a los sistemas de información que permiten el acceso a los mismos.

Los datos de identificación del RESPONSABLE DEL TRATAMIENTO son los siguientes:

• **RAZÓN SOCIAL**: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
• **NIF/CIF:** B73843211
• **DOMICILIO:** CTRA. DE LA ESTACIÓN, 180 I - 30540 - BLANCA - MURCIA
• **DIRECCIÓN DONDE SE REALIZAN LOS TRATAMIENTOS:** La especificada en el ANEXO D (Locales)
• **ACTIVIDAD:** GESTIÃ“N DEPORTIVA

En concreto, los tratamientos sujetos a las medidas de seguridad establecidas en este documento son los detallados en el ANEXO A.

Como recursos protegidos de la entidad se han tenido en cuenta los siguientes componentes:

• Los tratamientos
• Aplicaciones Informáticas con acceso a datos personales
• Soportes informáticos y papel
• Equipos de almacenamiento
• Equipos de tratamiento
• Comunicaciones y sistemas de acceso remoto
• Oficinas y edificios
• Sistemas de Validación
• Personas

2) FUNCIONES / OBLIGACIONES DEL PERSONAL

Todas las personas que tengan acceso a los datos personales, a través del sistema informático o a través de cualquier otro medio automatizado de acceso, están obligadas a cumplir lo establecido en este documento, y por lo tanto, sujetas a las consecuencias que puedan derivar en caso de incumplimiento. El incumplimiento de las políticas, prácticas y procedimientos de seguridad estará sujeto a una acción disciplinaria, pudiendo conllevar una acción civil y/o penal.

Sin embargo, una eventual vulneración de la normativa de seguridad por parte de algún usuario, no eximirá de responsabilidad al Responsable del Tratamiento, sin perjuicio de las acciones que pueda éste ejercitar contra dicho usuario por el incumplimiento de sus obligaciones con respecto al mismo.

Las medidas de índole organizativas afectan en primera instancia a la actividad propia de la organización y a la asignación de funciones relacionadas con la seguridad. Por tanto, el responsable del tratamiento debe asegurar la implantación de las medidas técnicas y organizativas en sus sistemas de información y delimitar el acceso a los datos de carácter personal mediante la asignación de perfiles entre su personal. Dicha división conlleva a su vez una imposición de responsabilidades directamente relacionadas con la función a desempeñar dentro de la entidad. Los perfiles son básicamente los siguientes:

• **Responsable del tratamiento:** persona física o jurídica que decide sobre la finalidad y medios del tratamiento.

• **Delegado de Protección de Datos (si procede):** persona o personas físicas, designadas por el responsable del tratamiento, con las siguientes funciones:

Informar y asesorar al responsable o encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.

Cooperar con la autoridad de control.

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

El DPD será obligatorio en:
- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.
- Los colegios profesionales y sus consejos generales.
- Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

- Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- Los establecimientos financieros de crédito.
- Las entidades aseguradoras y reaseguradoras.
- Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.
- Las empresas de seguridad privada.
- Las federaciones deportivas cuando traten datos de menores de edad.

Aunque esta figura no siempre sea obligatoria, es muy recomendable como elemento clave para garantizar el cumplimiento de las medidas de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Tratamiento.

Las funciones principales del DPD respecto al Documento serán:

- Coordinar la actualización del documento.
- Coordinar y controlar la implantación y aplicación de las medidas definidas en el Documento de Seguridad.
- Poner en conocimiento de los usuarios de los datos las medidas y procedimientos de seguridad que les afectan.
- Realizar controles periódicos para verificar el cumplimiento de las medidas.
- Analizar los informes de auditoría y elevar las conclusiones al responsable adecuado.

• **Administrador/es de Sistemas:** personas físicas encargadas de implantar y mantener las medidas técnicas de seguridad, una vez autorizadas por el DPD o el Responsable del Tratamiento.

• **Usuarios de los datos:** Aquellos que, en ejercicio de sus funciones contractuales, tratan datos de carácter personal bajo el criterio de "necesidad de saber" establecido por el responsable del tratamiento. Los usuarios, así como el resto de personal con acceso y tratamiento de datos de carácter personal, deberán conocer sus responsabilidades, siendo para ello necesario que se articulen mecanismos para garantizar un conocimiento comprensible de dichas normas.

En este Documento aparecen las normas que afectaran básicamente al DPD y al Administrador de Sistemas pero es muy importante que los usuarios de los datos conozcan toda la normativa que les pueda afectar. Es por ello, que junto con el Documento de Seguridad formando parte del proyecto se entrega una

normativa específica para usuarios donde figuran todas las normas referentes al RGPD que afectan a todos los empleados que puedan tratar datos.

Esta normativa debe difundirse a todos los empleados ya sea entregándola en la incorporación de un empleado o publicándola en algún sitio público como la intranet o similar.

En la empresa, se procede a entregar la normativa en forma de recomendaciones a todo el personal implicado, a través del Documento (Usos y Recomendaciones) que se entregará a los diferentes perfiles de usuarios y responsables.

A los nuevos trabajadores se les haría entrega de la documentación, en el momento de la firma del contrato de trabajo.

3) MEDIDAS, NORMAS Y PROCEDIMIENTOS

En este apartado reflejamos todas las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar y poder demostrar que el tratamiento es conforme al reglamento RGPD.

Al margen del cumplimiento de esta normativa, el Responsable del Tratamiento deberá adoptar en cada momento aquellas medidas de índole técnica y organizativa que crea necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información.

Cabe decir que, si el cumplimiento estricto de alguna de las normas expuestas supusiera un coste desproporcionado para el Responsable del Tratamiento, éste podrá modular su cumplimiento, sin que en ningún caso pueda verse afectada la protección de datos de carácter personal.

Control de Acceso a los datos personales

El control de acceso es aquella medida destinada a garantizar la identidad de cada persona que accede a los sistemas de información (identificación/autenticación), así como a asegurar que el acceso de cada usuario corresponda exclusivamente al perfil y permisos asignados por el responsable del tratamiento, con el objeto de evitar accesos no autorizados al sistema que contiene datos personales.

Exclusivamente el personal responsable de sistemas podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del tratamiento.

Las aplicaciones deberán estar hechas de tal forma que se garantice que los usuarios sólo tendrán acceso a los datos que precisen para el desarrollo de sus funciones. El administrador de sistemas establecerá mecanismos para evitar que un usuario pueda acceder a datos sin estar debidamente autorizado.

En caso de que exista personal ajeno al responsable del tratamiento que tenga acceso puntual a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal interno. Es recomendable crear cuentas de usuario específicas en los sistemas de información para este tipo de usuarios.

Identificación y autenticación

El responsable del tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

Será obligatorio establecer 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.

Si el mecanismo de autenticación se basa en contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Estas contraseñas se deberán almacenar de forma ininteligible y tendrán que cambiarse con una periodicidad no superior al año.

Además, se establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Control de acceso físico

Las instalaciones donde se traten datos personales deberán contar con los medios mínimos de seguridad, que garanticen que los datos protegidos están a salvo de riesgos por incidencias fortuitas o intencionadas.

La estancia donde se ubiquen los servidores será objeto de especial protección, garantizándose en todo momento que están a salvo la disponibilidad, la integridad y confidencialidad de los datos.

El acceso a la ubicación donde se encuentra el Servidor, deberá estar restringido exclusivamente al personal autorizado, y a aquel que deba realizar labores de mantenimiento del mismo.

Telecomunicaciones

La transmisión de datos de carácter personal especialmente protegidos que se realicen a través de redes públicas o redes inalámbricas de comunicaciones electrónicas deberá realizarse cifrando dicha información o utilizando cualquier otro medio que garantice que la información no sea inteligible ni manipulada por terceros. Las medidas habituales consisten en la existencia de redes VPN (IPSEC o SSL) que garantizan la confidencialidad de la información transmitida normalmente mediante protocolos seguros, así como otras tecnologías para la securización de los accesos vía web a las aplicaciones de intranet o internet. Otras opciones consisten en el cifrado de origen a extremo llevado a cabo por los propios usuarios mediante el uso de software específico, certificados digitales, etc.

Puestos de trabajo

Los puestos de trabajo están bajo la responsabilidad de las personas autorizadas, que deberá garantizar que la información que puede mostrarse desde dicho puesto no podrá ser vista por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras y otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Configuración de las Aplicaciones

Los puestos de trabajo desde los que se tenga acceso a los datos personales tendrán una configuración fija en sus aplicaciones y sistemas operativos, que sólo podrá ser cambiada bajo la autorización del Administrador del sistema. Ningún usuario podrá instalar una aplicación sin autorización del Administrador del sistema, quien analizará si dicha aplicación puede perjudicar otras que traten datos de carácter personal.

Todos los ordenadores deberán tener instalados programas antivirus que deberán, asimismo, estar actualizados diariamente, para así garantizar la protección y detección inmediata de la entrada de virus informáticos en el sistema. Además, los sistemas operativos deberán mantenerse actualizados.

Medidas específicas de los soportes no automatizados:

Procedimiento de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos deberán garantizar la correcta conservación de los mismos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de los interesados.
En aquellos casos que no exista norma aplicable, el responsable del tratamiento establecerá los criterios y procedimientos de actuación que deban seguirse para el archivo.

Procedimiento para dispositivos de almacenamiento y acceso a la documentación

El responsable del tratamiento o, en su defecto, un tercero autorizado, deberá establecer mecanismos que obstaculicen la apertura de dispositivos o medios de almacenamiento. Asimismo, en caso de que la naturaleza de los mismos impida su aplicación, se deberían fijar medidas que impidan el acceso a personas no autorizadas al lugar de almacenamiento, en la medida de lo posible. Habitualmente, estos procedimientos podrán llevarse a cabo mediante la aplicación de controles de acceso físico (llaves, tarjetas de entrada, biometría, etc.).

Procedimiento de custodia de soportes

En los casos en los que la documentación no se encuentra en dispositivos debidamente protegidos sea con motivo de procesos de revisión, tramitación, previo o posterior a su archivo, el responsable a cargo de la misma deberá custodiarla impidiendo el acceso a terceros no autorizados.

Para ello, entre otras, se deberán tener en cuenta las siguientes recomendaciones:

- Se almacenará de forma protegida la información sensible en papel especialmente cuando se abandone el puesto de trabajo.
- Los puntos de correo, fotocopiadoras, escáner, etc. Deberán estar protegidos para evitar un uso no autorizado.
- Se deben recoger inmediatamente los documentos impresos o enviados a una impresora o fotocopiadora con datos de carácter personal.

Procedimiento de copia o reproducción de documentos

Para los datos especialmente protegidos, se indicarán, asimismo, las personas autorizadas para la realización de copias o reproducción de los mismos, además de garantizar la destrucción de dicha información para evitar así el acceso no autorizado o su recuperación posterior.

Para ello es fundamental dotar de dispositivos de destrucción de documentos a todas las personas con acceso a la documentación y autorizadas para ello.

Procedimiento de acceso a la documentación

Además de la obligación de restricción de accesos a la información contenida en soportes no automatizados por personal no autorizado, en el caso de acceso a la documentación con datos especialmente protegidos se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

Traslado de la documentación

Siempre que se proceda al traslado físico de la documentación con datos especialmente protegidos, deberán anotarse medidas dirigidas a impedir el acceso o manipulación de la información objeto del traslado.

4) VIOLACIONES DE LA SEGURIDAD Y GESTIÓN DE INCIDENCIAS

Artículo 33 RGPD

Notificación de una violación de la seguridad de los datos personales a la autoridad de control

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

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

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

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

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

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

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

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

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34 RGPD

Comunicación de una violación de la seguridad de los datos personales al interesado

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

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

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

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

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

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

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

INCIDENCIAS DE SEGURIDAD

Se considerarán como incidencias de seguridad, entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del responsable del tratamiento.

Asimismo el responsable del tratamiento intentará contemplar el sentido más amplio del concepto de incidencia, entendiendo por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de los medios físicos y lógicos que pueda afectar a su disponibilidad y a la seguridad de la información que gestionan.

A continuación se presenta una lista de incidencias que serán inexcusablemente registradas. Esta lista no debe entenderse como limitativa, sino que podrá ser ampliada con cualquier otro tipo de incidencias que hubieran quedado omitidas:

Incidencias que afecten a la identificación y autenticación de los usuarios:
• Pérdida de confidencialidad de contraseñas.
• Asignación o modificación de derechos sobre herramientas de control de acceso y utilidades con accesos privilegiados.
• Períodos de desactivación de las herramientas de seguridad.

Incidencias que afecten a los derechos de acceso a los datos:
• Revisión de logs sobre intentos fallidos de accesos, accesos fuera de horas de oficina, etc.
• Comunicación de los usuarios de sospechas de que alguien ha suplantado su personalidad.
• Detección de puntos de acceso desatendidos y sin protección de pantalla activada.
• Detección de contraseñas escritas en los puestos de trabajo.
• Revisión de los informes de seguridad

Incidencias que afecten a la gestión de soportes:
• Comunicación de pérdida de soportes.
• Comunicación de localización de soportes en lugares inadecuados.
• Errores de contenido en soportes recibidos.

Incidencias que afecten a los procedimientos de copias de salvaguarda y recuperación:
• Errores en los procesos de realización de copias de salvaguarda.
• Recuperaciones de datos realizadas.

Cualquier otra de las observadas como consecuencia de la ejecución de los controles definidos para

garantizar el cumplimiento de lo dispuesto en el Documento de Seguridad.

La aplicación del presente Procedimiento se establece para todas las Áreas del responsable del tratamiento, empleados y colaboradores externos.

Responsabilidades

El Responsable se encargará de la redacción y mantenimiento de este procedimiento; así como de su custodia y archivo.

Todos los usuarios de la entidad deben informar de cualquier incidencia producida en materia de seguridad.

El Responsable debe ocuparse del seguimiento de las incidencias en materia de seguridad.

Los usuarios de los sistemas de información, empleados y colaboradores externos, deben participar en la implantación y seguimiento de la política de seguridad, aceptando formalmente sus obligaciones.

Comunicación de Incidencias de Seguridad por Usuarios

Cualquier usuario que tenga conocimiento directa o indirectamente de cualquier incidencia de seguridad, actual o posible, lo comunicará con la mayor brevedad tal incidencia y las acciones que se hubiesen tomado de urgencia.

En este momento se procede a incluirse en el registro y, si afecta a la seguridad de los datos de carácter personal, marcarla como tal.

Registro y Distribución de las Incidencias

Con el fin de poder mantener un registro de incidencias que permita su mantenimiento y posterior tratamiento y análisis se centralizará la recepción de las mismas en una misma persona designada por el responsable.

En el caso de incidencias sobre procesos o aplicaciones se comunicarán directamente al Responsable informático, quien se ocupará de informar al responsable sobre su resolución.

Registros

El registro de incidencias será mantenido en exclusiva por el responsable.
Se facilitará el acceso estrictamente a aquellos departamentos que lo necesiten, para su consulta o análisis encaminado al estudio de acciones a llevar a cabo para la resolución de las incidencias.

Se facilitarán los formularios necesarios para llevar a cabo el registro de las incidencias. El conocimiento y la no-notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del tratamiento por parte de ese usuario.

5) CONTRASEÑAS Y COPIAS DE SEGURIDAD

Autenticación

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales. Cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible. Este sistema de autenticación debe venir acompañado por una política de restricción de accesos, esto es, que exista una política en la empresa de controlar los accesos de información únicamente en lo estrictamente necesario al puesto de trabajo concreto y a las funciones que se deben desarrollar en él, siendo consecuente, que a mayor cargo y responsabilidad, mayor será el acceso que pueda obtenerse de la información del sistema, así como la restricción de acceso a la información por áreas o departamentos.

El sistema actual utilizado por el Responsable en el tratamiento en cuanto a la autenticación de las entradas en el sistema, es el que a continuación se describe:

En cuanto a las claves de acceso, el sistema operativo requiere usuario / contraseña para iniciar la sesión, éstas son dadas por el responsable de sistemas a los usuarios.

El procedimiento que se recomienda seguir para el cambio de contraseña entre los usuarios de el responsable del tratamiento es el siguiente:

1) Siempre que sea posible el sistema ha de pedir el cambio de contraseña no permitiendo volver a usar una contraseña ya utilizada anteriormente.

2) Si el punto 1 no es posible por limitaciones del sistema el administrador de sistemas pedirá personalmente a cada usuario la nueva contraseña. El usuario deberá comunicarla al administrador en un plazo máximo de 24 horas y esta comunicación se realizará por medios que garanticen la confidencialidad de la contraseña.

3) Una vez que el administrador de sistemas disponga de todas las contraseñas, validará que no sea una contraseña ya utilizada anteriormente. El administrador de sistemas cambiará la contraseña del usuario para todas las aplicaciones que la requieran junto con la contraseña del sistema operativo y red (recursos compartidos).

4) Se verificará que el cambio de las contraseñas se ha realizado correctamente.

5) Se comunicará a los usuarios el momento del cambio y cuando pueden empezar a utilizar la nuevas contraseñas haciendo hincapié en el tema de la confidencialidad. Para llevar a cabo correctamente este procedimiento será necesario disponer de una lista/fichero protegida/o con las aplicaciones y puntos del sistema informático que requieran contraseña.

A cada usuario del sistema informático de le será asignado un nombre de usuario, que asociado a una contraseña, lo identificará dentro de los sistemas de información y permitirá el acceso a las áreas relacionadas con su actividad profesional.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y solicitar el cambio al Responsable de protección de datos.

Cuando se incorpore un usuario nuevo el responsable de tratamiento se encargará de comunicarlo al departamento de sistemas para que se le dé de alta conforme a los permisos que le sean asignados. En esta alta se le asignará un nombre de usuario y una contraseña. No está permitida la divulgación de la clave por circunstancia alguna a otras personas integrantes de la plantilla o ajenas a la entidad.

Copias de Seguridad

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

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos de los ficheros con datos de carácter personal.

El responsable del tratamiento se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Procedimiento de respaldo

Debe fijarse y definirse un proceso de copia total de todos los archivos del sistema a través de cualquier medio válido que asegure la recuperación. El Responsable de realizarlas es el Responsable de Copias de Seguridad o el responsable de sistemas, por un medio automatizado. Se aconseja, especialmente, la copia en disco externo para almacenarla fuera del servidor de la empresa.

Procedimiento de recuperación

Cuando se produzca una pérdida total o parcial de datos de cualquiera de los servidores se deberán tener en cuenta los siguientes puntos:

• Dejar constancia en el libro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones rellenando el formulario con todos los datos requeridos.

• La recuperación deberá realizarse partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia que permita reconstruir los datos del fichero al estado en que se encontraban antes del momento del fallo o pérdida.

Soportes para los respaldos

Los soportes de las copias de seguridad se podrán reciclar. Aún así, si alguno dejará de ser fiable para su funcionamiento, deberá ser destruido físicamente de forma que sea imposible la recuperación de los datos. Antes de reciclar cualquier soporte el personal autorizado para realizar las copias deberá verificar si es o no óptimo para su funcionamiento. Se designará por el responsable un recinto donde se guardarán los soportes de las copias de seguridad, que se mantendrá constantemente cerrado con llave y protegido.

Para datos especialmente protegidos, se aconseja conservar una copia de seguridad en un lugar diferente a aquel que se encuentren los equipos que tratan los datos o utilizar elementos que garanticen la integridad y recuperación de la información.

6) GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes informáticos son todos aquellos medios físicos susceptibles de ser tratados en los sistemas de información, y sobre los que se pueden grabar y recuperar datos (equipos, discos, pendrives, etc.). El control de estos medios tiene una importancia fundamental, dada la facilidad para su transporte y reproducción.

Inventario

Los soportes o documentos que contengan datos de carácter personal deben estar claramente identificados con una etiqueta externa que permita identificar a través de algún identificador que tipo de datos contienen (salvo que las características físicas del soporte o documento lo impidan).

Dicho sistema debe permitir mantener un inventario de los soportes, donde se pueda registrar otra información adicional, como fecha de creación, fecha de baja, motivo de la baja, etc.

La identificación de los soportes para información especialmente sensible puede establecerse mediante una codificación que dificulte la identificación para usuarios no autorizados. Los soportes o documentos que contengan datos de carácter personal deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas.

Autorización salida o entrada de soportes

La salida de datos de carácter personal pertenecientes a los tratamientos definidos en el presente documento, sea cual sea el medio utilizado (incluye los comprendidos y/o anexos a un correo electrónico), sólo estará permitida cuando sea necesario para el desempeño de las funciones propias de la empresa, y cuando así lo autorice el Responsable del Tratamiento.

Los soportes o documentos que deban salir de las ubicaciones habituales deberán ser transportados con la debida protección frente a robos, sustracciones o accesos no autorizados, teniendo en cuenta la sensibilidad de la información. A ser posible el transporte se realizará de forma codificada o mediante otros mecanismos similares que puedan garantizar su protección durante su salida de la ubicación habitual. La tecnología de cifrado también es aplicable a los documentos como correo electrónico o equipos portátiles cuando se empleen fuera de las instalaciones.

Registro salida o entrada de soportes

La salida o entrada de soportes deberá registrarse expresamente mediante el formulario habilitado.
Este registro deberá contener el tipo de documentos o soportes, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción o entrega.

Si la salida de dichos soportes o documentos fuera periódica como el caso de portátil, PDA, etc. podrá hacerse un registro/autorización genérico especificándolo en la hoja de registro. El movimiento de soportes entre departamentos no se considerará a estos efectos.

Reutilización o desechado de soportes

Cuando un soporte que contenga datos de carácter personal vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario en caso que no se sustituya por otro soporte destinado a la misma función.

Entrada y Salida de Datos por Red

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

El envío de datos de los ficheros protegidos por correo electrónico sólo se realizará cuando sea necesario para el desempeño de las funciones propias de la empresa. En todo caso, el usuario que realice o pretenda realizar el envío de los datos deberá ser un usuario autorizado para el tratamiento de esos datos.

La obligación de dicho usuario será la de asegurarse de que la entrega o envío de esa información es legítima en virtud de lo establecido en la presente normativa aplicable y en el presente Documento de Seguridad.

El envío de información entre personal interno o entre departamentos, no se considerará entrada y salida de datos a los efectos de la presente normativa.

7) TRATAMIENTOS

Registro de Actividades de Tratamiento

Cada Responsable del tratamiento y Encargado llevará un registro (Anexo A) de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y categorías de datos personales tratados.
- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- Transferencias internacionales de datos.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

El registro (Anexo A) constará por escrito, inclusive en formato electrónico. El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de control que lo solicite.

8) CONTROLES PERIÓDICOS / AUDITORÍAS

El responsable llevará a cabo controles periódicos que verifiquen el cumplimiento de las normas establecidas en el reglamento europeo y de las medidas de seguridad y organizativas descritas en el documento de seguridad, así como controlar que documentalmente las modificaciones estén actualizadas: nuevos trabajadores que firman el documento de autorización del consentimiento, contratos con los posibles nuevos encargados del tratamiento, rutinas de registros, incidencias, entradas y salidas, etc.

Periódicamente los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, a una auditoría interna o externa que verifique el cumplimiento de las normas establecidas en el reglamento europeo y en el documento de seguridad.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con objeto de verificar la adaptación, adecuación y eficacia de las mismas.

Los informes de auditoría serán analizados por el Responsable del tratamiento para que adopte las medidas correctoras adecuadas.

9) ENCARGADOS DE TRATAMIENTO

El Reglamento Europeo establece que cuando exista un tratamiento de datos por cuenta de terceros, ya sea de forma parcial o de modo exclusivo, el documento de seguridad deberá contener la identificación de dichos tratamientos, así como un contrato que regule las condiciones del encargo.

Esta exigencia se cumple a través de los modelos de contrato de encargo de tratamiento que se facilitan a través de la implantación, ya que mediante la auto cumplimentación de datos, cada uno de los contratos de encargo de tratamiento identificarán además de la empresa con la que se ha contratado los servicios que llevan implícita la comunicación y cesión de datos, es decir, la identificación del Encargo de Tratamiento, así como el resto de información a la que viene referida el artículo 28 del reglamento europeo, se señalará qué datos quedan sujetos a las cesiones o accesos de datos que deba realizar el Encargado de tratamiento para poder prestar el servicio contratado.

En un régimen diferente, ya que no se produce un tratamiento de los datos, pero para salvaguardar el posible acceso y conocimiento de datos de carácter personal titularidad del Responsable del tratamiento, encontramos terceras personas, que por la naturaleza de sus servicios (mantenimiento, mensajería y auxiliar-administrativos) tienen acceso a determinada información del centro, convirtiéndose en cesionarios de la empresa. Normalmente, son autónomos colaboradores y prestadores de algún servicio profesional que acceden a la base de datos del Responsable del Tratamiento, por lo que se hace necesario firmar el oportuno documento de acceso de datos y confidencialidad.

ANÁLISIS DE NECESIDAD

Análisis

No existen Análisis de necesidad realizados

4) ANEXOS (MEDIDAS PROACTIVAS)

1. Anexo A
 Registro de actividades de tratamiento y relación de encargados de tratamiento.
2. Anexo B
 Descripción de la estructura del sistema informático.
3. Anexo C
 Riesgos, Medidas de Seguridad y Políticas de Acceso.
4. Anexo D
 Locales: Sede principal y delegaciones.
5. Anexo E
 Nombramientos y autorizaciones:
 1. Lista de responsables.
 2. Lista de autorizaciones.
6. Anexo F
 Registro de incidencias.
7. Anexo G
 Procedimientos de control y seguridad:
 G.1. Procedimiento de respaldo y recuperación.
 G.2. Autorización para el uso de ordenadores portátiles y trabajo fuera de locales.
8. Anexo H
 1. Programas y aplicaciones
 2. Equipamientos
 3. Soportes

ANEXO A Registro de actividades de tratamiento

Este anexo contiene la relación de tratamientos llevados a cabo por el responsable, y además una relación de los encargados del tratamiento.

Listado de tratamientos propios

Relación de tratamientos propios del responsable REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L..

Tratamiento PROPIO	Código: 1

Fecha: 15/05/2024
Nombre: CLIENTES
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO PARA LA GESTIÓN ADMINISTRATIVA Y COMERCIAL DE LA CARTERA DE CLIENTES DE LA EMPRESA.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: CLIENTES Y USUARIOS, SOLICITANTES.
Categorías de datos: DATOS IDENTIFICATIVOS: CIF/NIF, NOMBRE Y APELLIDOS, RAZÓN SOCIAL, DIRECCIÓN POSTAL O ELECTRÓNICA, TELÉFONO, DATOS BANCARIOS.
Cesiones: ADMINISTRACIÓN TRIBUTARIA Y OTROS ORGANISMOS DE LA ADMINISTRACIÓN PÚBLICA.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Tratamiento PROPIO	Código: 2

Fecha: 15/05/2024
Nombre: PROVEEDORES
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO PARA LA GESTIÓN ADMINISTRATIVA Y COMERCIAL DE LA CARTERA DE PROVEEDORES DE LA EMPRESA.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: PROVEEDORES.
Categorías de datos: DATOS IDENTIFICATIVOS: CIF/NIF, NOMBRE Y APELLIDOS, RAZÓN SOCIAL, DIRECCIÓN POSTAL O ELECTRÓNICA, TELÉFONO, DATOS BANCARIOS.
Cesiones: ADMINISTRACIÓN TRIBUTARIA Y OTROS ORGANISMOS DE LA ADMINISTRACIÓN PÚBLICA.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Tratamiento PROPIO	Código: 3

Fecha: 15/05/2024
Nombre: EMPLEADOS
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO PARA LA CONFECCIÓN DE NÓMINAS Y GESTIÓN LABORAL DE LOS TRABAJADORES DE LA EMPRESA.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: EMPLEADOS, SOLICITANTES.
Categorías de datos: DATOS IDENTIFICATIVOS: NOMBRE Y APELLIDOS, NIF/NIE, Nº SEGURIDAD SOCIAL, DIRECCIÓN POSTAL O ELECTRÓNICA,TELÉFONO, FIRMA MANUAL, MANUSCRITA O DIGITALIZADA.OTROS DATOS TIPIFICADOS: CARACTERÍSTICAS PERSONALES, ACADÉMICOS Y PROFESIONALES, OTROS DATOS BIOMÉTRICOS.
Cesiones: ORGANISMOS DE LA SEGURIDAD SOCIAL, ADMINISTRACIÓN TRIBUTARIA Y OTROS ORGANISMOS DE LA ADMINISTRACIÓN PÚBLICA.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Tratamiento PROPIO	Código: 4

Fecha: 15/05/2024
Nombre: PREVENCIÓN DE RIESGOS LABORALES
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO PARA LA GESTIÓN DE LA PREVENCIÓN DE RIESGOS LABORALES DE LA EMPRESA.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: EMPLEADOS.
Categorías de datos: DATOS IDENTIFICATIVOS: NOMBRE Y APELLIDOS, NIF/NIE, Nº SEGURIDAD SOCIAL, DIRECCIÓN POSTAL O ELECTRÓNICA,TELÉFONO, FIRMA MANUAL, MANUSCRITA O DIGITALIZADA.OTROS DATOS TIPIFICADOS: CARACTERÍSTICAS PERSONALES, ACADÉMICOS Y PROFESIONALES, OTROS DATOS BIOMÉTRICOS. OTROS DATOS ESPECIALMENTE PROTEGIDOS: SALUD.
Cesiones: SERVICIO AJENO DE PREVENCIÓN DE RIESGOS LABORALES.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Tratamiento PROPIO	Código: 5

Fecha: 15/05/2024
Nombre: VIDEOVIGILANCIA
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO UTILIZADO PARA ALMACENAR LAS GRABACIONES DE VIDEOVIGILANCIA DEL SISTEMA DE SEGURIDAD PROPIO DE LA ENTIDAD, CON LA FINALIDAD DE PRESERVAR LA SEGURIDAD PERSONAL Y MATERIAL, ASÍ COMO EL CONTROL EMPRESARIAL EN LAS INSTALACIONES.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: CLIENTES, PROVEEDORES, EMPLEADOS, SOLICITANTES.
Categorías de datos: IMAGEN Y VOZ.
Cesiones: FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO, ADMINISTRACIÓN COMPETENTE EN LA MATERIA.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Tratamiento PROPIO	Código: 6

Fecha: 15/05/2024
Nombre: USUARIOS WEB
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO PARA REALIZAR ACCIONES DE MARKETING OFERTAS Y PUBLICIDAD DE LOS PRODUCTOS Y SERVICIOS DE LA EMPRESA.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: CLIENTES, USUARIOS Y SOLICITANTES.
Categorías de datos: DATOS IDENTIFICATIVOS: NOMBRE Y APELLIDOS, NIF/NIE, Nº SEGURIDAD SOCIAL, DIRECCIÓN POSTAL O ELECTRÓNICA,TELÉFONO, FIRMA MANUAL, MANUSCRITA O DIGITALIZADA.
Cesiones: REGISTROS PÚBLICOS.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Tratamiento PROPIO	Código: 7

Fecha: 15/05/2024
Nombre: USUARIOS REDES SOCIALES
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO PARA REALIZAR ACCIONES DE MARKETING OFERTAS Y PUBLICIDAD DE LOS PRODUCTOS Y SERVICIOS DE LA EMPRESA.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: CLIENTES, USUARIOS Y SOLICITANTES.
Categorías de datos: DATOS IDENTIFICATIVOS: NOMBRE Y APELLIDOS, NIF/NIE, Nº SEGURIDAD SOCIAL, DIRECCIÓN POSTAL O ELECTRÓNICA,TELÉFONO, FIRMA MANUAL, MANUSCRITA O DIGITALIZADA.
Cesiones: REGISTROS PÚBLICOS.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Tratamiento PROPIO	Código: 8

Fecha: 15/05/2024
Nombre: CURRÍCULUM VITAE
Responsable: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L.
Finalidad: FICHERO PARA LA GESTIÓN Y SELECCIÓN DE PERSONAL DE LA ENTIDAD.
Transferencias: NO EXISTEN TRANSFERENCIAS INTERNACIONALES DE LOS DATOS. EN CASO DE QUE TUVIERAN QUE SER REALIZADAS, EL RESPONSABLE DEL TRATAMIENTO DEBERÁ DE COMUNICAR AL ENCARGADO DEL TRATAMIENTO CON UNA ANTELACIÓN DE DIEZ DÍAS.
Medidas técnicas: LAS DETALLADAS EN EL DOCUMENTO DE SEGURIDAD.
Colectivos de interesados: SOLICITANTES, PADRES O TUTORES.
Categorías de datos: DATOS IDENTIFICATIVOS: NOMBRE Y APELLIDOS, NIF, DIRECCIÓN POSTAL O ELECTRÓNICA, TELÉFONO, Nº DE LA SEGURIDAD SOCIAL, IMAGEN / VOZ. OTROS DATOS TIPIFICADOS: CARACTERÍSTICAS PERSONALES, ACADÉMICOS Y PROFESIONALES.
Cesiones: ORGANIZACIONES O PERSONAS DIRECTAMENTE RELACIONADAS CON EL RESPONSABLE. EMPRESAS DE TRABAJO TEMPORAL QUE PRESTEN SERVICIO A LA ENTIDAD.
Duración: EL REQUERIDO POR LA LEGISLACIÓN VIGENTE. EN CASO DE NO EXISTIR LEGISLACIÓN EL PLAZO SERÁ DE UN AÑO.
Observaciones: NIVEL DE SEGURIDAD: BÁSICO

Listado de tratamientos de terceros

No existen datos para este anexo o documento.

Encargados con acceso

Listado de encargados con acceso a datos

Relación de empresas que prestan algún servicio al responsable del tratamiento, y dicho servicio implica tratamiento de datos personales.

Encargados con acceso	código: 1

Nombre del encargado: ÁREAS CONSULTORES S.L. **Nif:** B30161756
Dirección: C/ PRINCESA, 9, ENTRESUELO DCHA.
CP: 30002 **Localidad:** MURCIA
Teléfono: 968221350
Email: laua@areasconsultores.com
Servicio que prestará el encargado: SERVICIOS JURÍDICOS
Firmado: SI

Encargados con acceso	código: 2

Nombre del encargado: NOELIA PRIETO MARTÍNEZ (INFONET SOFTWARE) **Nif:** 34822960V
Dirección: APARTADO DE CORREOS 286
CP: 30110 **Localidad:** CABEZO DE TORRES
Teléfono: 901900060
Email: soporte@infonetsoftware.com
Descripción detallada del servicio prestado: INFORMATICA
Firmado: SI

Encargados con acceso	código: 3

Nombre del encargado: MUTUAL MIDAT CYCLOPS **Nif:** G64172513
Dirección: AV. JOSEP TARRADELLAS, Nº14,18
CP: 08029 **Localidad:** BARCELONA
Teléfono: 934447461
Email: info@mc-mutual.com
Descripción detallada del servicio prestado: MUTUA
Firmado: SI

Encargados con acceso	código: 4

Nombre del encargado: PRILANOR S.L.L. **Nif:** B73223547
Dirección: C/ MAHON, 18 BAJO
CP: 30100 **Localidad:** ESPINARDO
Teléfono: 968964144
Email: info@prilanor.com
Representante: FERNANDO PALAZON MARTINEZ **Nif:** 27477655S
Descripción detallada del servicio prestado: SERVICIO DE PREVENCION DE RIESGOS LABORALES
Firmado: SI

Encargados con acceso	código: 5

Nombre del encargado: VALEGAL ESPAÑA S.L.U. **Nif:** B54955760
Dirección: FELIX RODRIGUEZ DE LA FUENTE Nº 42
CP: 03650 **Localidad:** PINOSO
Teléfono: 965478703
Email: jose.herrero@valegalespaña.com
Representante: JOSE HERRERO MIRALLES **Nif:** 48475971K
Descripción detallada del servicio prestado: CONSULTORIA EMPRESARIAL.
Firmado: SI

Encargados sin acceso

No existen datos para este anexo o documento.

Relación de empresas que prestan algún servicio al responsable del tratamiento, y dicho servicio NO implica tratamiento de datos personales.

Responsables

No existen datos para este anexo o documento.

Relación de empresas a las cuales se les presta un servicio, y REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L. actúa como encargado.

ANEXO B Estructura informática

Este anexo contiene la descripción de la estructura del sistema informático, el tipo de red y el entorno de las comunicaciones.

Estructura informática	Código: 1
Descripción de la estructura informática: RED LOCAL CON UN (1) SERVIDOR DE FICHEROS, CUATRO (4) ORDENADORES SOBREMESA, CONECTADOS ENTRE SÍ POR UN SWICTH A TRAVÉS DE CABLE DE RED ETHERNET. ESTÁN CONECTADOS A INTERNET MEDIANTE UN ROUTER ADSL. HAY UNA (1) IMPRESORA MULTIFUNCIÓN COMPARTIDAS PARA GESTIÓN DOCUMENTAL. **Esta estructura pertenece al local o locales:** SEDE PRINCIPAL	

ANEXO C

No existen datos para este anexo o documento

En este anexo se describen las políticas de acceso a los datos así como los riesgos y sus medidas de seguridad aplicadas a los equipos y programas informáticos o cualquier medio o activo utilizado en el tratamiento de datos así como los métodos implementados.

ANEXO D Locales donde se tratan datos personales

Este anexo contiene una relación de los locales donde se tratan datos personales

Local	Código: 1

Nombre del local: SEDE PRINCIPAL
Dirección completa del local: CTRA. DE LA ESTACIÓN, 180 I, 30540, BLANCA, MURCIA
Descripción física del local: OFICINA DE 30 M2, UNA SOLA PLANTA, UN SOLO ACCESO POR LA PUERTA PRINCIPAL, CON UN PUESTO DE TRABAJO.
Control de acceso: PERSONAL DE LA EMPRESA AUTORIZADO CON LLAVE DE LA ENTRADA PRINCIPAL
Sistemas de seguridad: ALARMA DE INFRARROJOS Y SIRENA EXTERIOR, CÁMARAS DE VIDEOVIGILANCIA, CERRADURA DE SEGURIDAD.
Tratamientos: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

Observaciones:

ANEXO E Nombramientos

Este anexo contiene una relación de los diferentes representantes en materia de protección de datos, todos ellos nombrados o autorizados por el Responsable del Tratamiento: REISPORT GESTIÓN DEPORTIVA INTEGRAL S.L..

Nombramientos	Código: 1

Administrador
Nombre y Apellidos: ROBERTO MONTESINOS SÁNCHEZ
Dni: 48494181S
Fecha de Alta: 15/05/2024
Cargo/función en la empresa: PERSONA DESIGNADA PARA CONCEDER ALTERAR O ANULAR EL ACCESO AUTORIZADO A LOS DATOS

Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

Fdo. Responsable del tratamiento:

Fdo. Administrador:

Nombramientos	Código: 2

Responsable de seguridad
Nombre y Apellidos: ROBERTO MONTESINOS SÁNCHEZ
Dni: 48494181S
Fecha de Alta: 15/05/2024
Cargo/función en la empresa:

Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

Fdo. Responsable del tratamiento:

Fdo. Responsable de seguridad:

Nombramientos	Código: 3

Responsable de copias de respaldo y recuperación
Nombre y Apellidos: ROBERTO MONTESINOS SÁNCHEZ
Dni: 48494181S
Fecha de Alta: 15/05/2024
Cargo/función en la empresa:

Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

Fdo. Responsable del tratamiento:

Fdo. Responsable de copias de respaldo y recuperación:

Nombramientos	Código: 4

Responsable de la gestión de incidencias
Nombre y Apellidos: ROBERTO MONTESINOS SÁNCHEZ
Dni: 48494181S
Fecha de Alta: 15/05/2024
Cargo/función en la empresa:

Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

Fdo. Responsable del tratamiento:

Fdo. Responsable de la gestión de incidencias:

Nombramientos	Código: 5

Responsable de atención a los afectados
Nombre y Apellidos: ROBERTO MONTESINOS SÁNCHEZ
Dni: 48494181S
Fecha de Alta: 15/05/2024
Cargo/función en la empresa:

Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

Fdo. Responsable del tratamiento:

Fdo. Responsable de atención a los afectados:

ANEXO E Autorizaciones con acceso

No existen datos para este anexo o documento.

ANEXO E Autorizaciones sin acceso a datos

No existen datos para este anexo o documento.

ANEXO F Notificación y gestión de incidencias

Cuando se produzca una incidencia, el usuario o el administrador deberán comunicarla al Responsable de seguridad o al Responsable del fichero o superior inmediato. Para ello emplearán el formulario aquí detallado. Una vez recibida la notificación el responsable correspondiente procederá a su registro y análisis, debiendo tomar las medidas correctoras necesarias. En ficheros de nivel medio y alto el responsable del fichero debe autorizar previamente las posibles recuperaciones de datos.

Se mantendrán las incidencias registradas de los 12 últimos meses.

ANEXO F

Registro automatizado de Incidencias

No existen datos para este anexo o documento.

ANEXO F **Notificación y gestión manual de incidencias**

Incidencia Nº: (Este número será rellenado por el Responsable de seguridad)
Fecha de la alerta:
Tipo de incidencia:
Descripción detallada de la incidencia:
Fecha y hora en que se produjo la incidencia:

Efectos que puede producir:
Medidas correctoras aplicadas:
Recuperación de Datos : (A rellenar sólo si la incidencia es de este tipo) Procedimiento realizado: Datos restaurados: Datos grabados manualmente: Persona que ejecutó el proceso:
Nombre del Responsable: Firma: El responsable autoriza las recuperaciones de datos mediante la firma de este formulario.

Persona que alertó la incidencia: Firma:	Persona a quién se comunica:

ANEXO G.1 Procedimiento de copias de seguridad y recuperación

Este anexo contiene la descripción del sistema de copias de seguridad y recuperación, así cómo la frecuencia.

Procedimiento de copias de seguridad y recuperación	Código: 1

Descripción del sistema de copias: LA EMPRESA TIENE ESTABLECIDO UN PROTOCOLO DE SEGURIDAD. PARA ELLO, UTILIZA UN DISCO DURO EXTERNO DE 1 TB. DE FORMA DIARIA ESTÁN PROGRAMADAS LAS COPIAS DE SEGURIDAD EN EL SERVIDOR EN DISCO ESPEJO. ADEMÁS CADA VIERNES SE CONECTA UNA DIFERENTE, SE EJECUTA EL PROGRAMA DE COPIAS COBIAN BACKUP O SIMILAR EL CUAL YA TIENE UNA SELECCIÓN DE CARPETAS ESTABLECIDAS. EL RESPONSABLE DE LAS COPIAS ESPERA LA FINALIZACIÓN, RETIRA LA UNIDAD Y LA GUARDA BAJO LLAVE.
Descripción del sistema de recuperación: SE CONECTA EL DISCO DURO EXTERNO QUE TENGA LA COPIA MÁS RECIENTE Y SE EJECUTA EL PROGRAMA COBIAN BACKUP O SIMILAR, A TRAVÉS DE ESTE SE SELECCIONAN LAS CARPETAS A RECUPERAR Y UNA VEZ COMPROBADO EL CONTENIDO RECUPERADO SE DEVUELVE LA UNIDAD A SU CAJÓN BAJO LLAVE.
Frecuencia de las copias: SEMANAL
Tratamientos afectados: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

ANEXO G2 Autorización para el uso de PC portátiles

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

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

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

Utilizar el siguiente formulario para ello.

ANEXO G2 Autorización para el uso de PC portátiles

Nombre y firma persona autorizada: **Nombre y firma del responsable que autoriza:**	**Identificación del equipo:**
Tratamiento que contiene:	**Fecha autorización:** **Periodo de validez:**

Detallar las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o pérdida del equipo:
Se cifrarán los datos que contengan los ordenadores portátiles cuando estos se encuentren fuera de las instalaciones que están bajo el control del responsable, si esto no es posible se hará constar las medidas alternativas que se adopten. **Medidas alternativas:**

ANEXO H Programas y aplicaciones

Lista de los programas Ofimáticos, Gestores de Facturación, Contabilidad, etc.. que traten datos personales.

Programa / Aplicación:	Código: 1

Nombre: MICROSOFT OFFICE
Cantidad: 1
Fabricante: MICROSOFT
Finalidad y descripción: BASE DE DATOS, HOJA DE CÁLCULO Y PROCESADOR DE TEXTOS.
Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE.
Equipos donde se ejecuta: ORDENADOR SERVIDOR (1), ORDENADOR SOBREMESA (4), IMPRESORA MULTIFUNCIÓN (1).
Registro de accesos: NO
Fecha de alta: 15/05/2024 **Fecha de baja:**

Programa / Aplicación:	Código: 2

Nombre: INFONET SOFTWARE
Cantidad: 1
Fabricante: INFONET
Finalidad y descripción: GESTIÓN, FACTURACIÓN Y CONTABILIDAD.
Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE.
Equipos donde se ejecuta: ORDENADOR SERVIDOR (1), ORDENADOR SOBREMESA (4), IMPRESORA MULTIFUNCIÓN (1).
Registro de accesos: SI
Fecha de alta: 15/05/2024 **Fecha de baja:**

Programa / Aplicación:	Código: 3

Nombre: WORDPRESS
Cantidad: 1
Fabricante: WORDPRESS FOUNDATION
Finalidad y descripción: SISTEMA DE GESTIÓN DE CONTENIDOS
Tratamientos que realiza: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE.
Equipos donde se ejecuta: ORDENADOR SERVIDOR (1), ORDENADOR SOBREMESA (4), IMPRESORA MULTIFUNCIÓN (1).
Registro de accesos: SI
Fecha de alta: 15/05/2024 **Fecha de baja:**

ANEXO H Equipamiento

Inventario de los equipos informáticos que tratan datos personales.

Características del equipos/s	Código: 1
Tipo equipo: ORDENADOR SERVIDOR **Cantidad:** 1 **Tratamientos que realiza:** CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE. **Local donde se encuentra este equipo:** SEDE PRINCIPAL **Sistema operativo:** WINDOWS 10 **Antivirus:** AVAST **Fecha de alta:** 15/05/2024 **Fecha de baja:**	
Características del equipos/s	Código: 2
Tipo equipo: ORDENADOR SOBREMESA **Cantidad:** 4 **Tratamientos que realiza:** CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE. **Local donde se encuentra este equipo:** SEDE PRINCIPAL **Sistema operativo:** WINDOWS 10 **Antivirus:** AVAST **Fecha de alta:** 15/05/2024 **Fecha de baja:**	
Características del equipos/s	Código: 3
Tipo equipo: IMPRESORA MULTIFUNCIÓN **Cantidad:** 1 **Tratamientos que realiza:** CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE. **Local donde se encuentra este equipo:** SEDE PRINCIPAL **Fecha de alta:** 15/05/2024 **Fecha de baja:**	

Anexo H

Relación de soportes

Lista de soportes utilizados que contienen datos personales.

Soporte:	Código: 1
Referencia del soporte: 01 **Tipo de soporte:** ARCHIVADOR NO AUTOMATIZADO **Lugar de acceso restringido donde se deposita el soporte:** ARCHIVO **Datos que contiene:** CLIENTES **Local donde se encuentra:** SEDE PRINCIPAL	
Soporte:	Código: 2
Referencia del soporte: 02 **Tipo de soporte:** ARCHIVADOR NO AUTOMATIZADO **Lugar de acceso restringido donde se deposita el soporte:** ARCHIVO **Datos que contiene:** PROVEEDORES **Local donde se encuentra:** SEDE PRINCIPAL	
Soporte:	Código: 3
Referencia del soporte: 03 **Tipo de soporte:** ARCHIVADOR NO AUTOMATIZADO **Lugar de acceso restringido donde se deposita el soporte:** ARCHIVO **Datos que contiene:** EMPLEADOS **Local donde se encuentra:** SEDE PRINCIPAL	
Soporte:	Código: 4
Referencia del soporte: 04 **Tipo de soporte:** ARCHIVADOR NO AUTOMATIZADO **Lugar de acceso restringido donde se deposita el soporte:** ARCHIVO **Datos que contiene:** PREVENCIÓN DE RIESGOS LABORALES **Local donde se encuentra:** SEDE PRINCIPAL	
Soporte:	Código: 5
Referencia del soporte: 05 **Tipo de soporte:** ARCHIVADOR NO AUTOMATIZADO **Lugar de acceso restringido donde se deposita el soporte:** ARCHIVO **Datos que contiene:** USUARIOS WEB, USUARIOS REDES SOCIALES **Local donde se encuentra:** SEDE PRINCIPAL	
Soporte:	Código: 6
Referencia del soporte: 06 **Tipo de soporte:** ARCHIVADOR NO AUTOMATIZADO **Lugar de acceso restringido donde se deposita el soporte:** ARCHIVO **Datos que contiene:** VIDEOVIGILANCIA **Local donde se encuentra:** SEDE PRINCIPAL	

Soporte:	Código: 7

Referencia del soporte: 07
Tipo de soporte: ARCHIVADOR NO AUTOMATIZADO
Lugar de acceso restringido donde se deposita el soporte: ARCHIVO
Datos que contiene: CURRÍCULUM VITAE
Local donde se encuentra: SEDE PRINCIPAL

Soporte:	Código: 8

Referencia del soporte: 08
Tipo de soporte: DISCO DURO EXTERNO AUTOMATIZADO
Lugar de acceso restringido donde se deposita el soporte: LUGAR SEGURO FUERA DE LAS INSTALACIONES.
Datos que contiene: CLIENTES, PROVEEDORES, EMPLEADOS, PREVENCIÓN DE RIESGOS LABORALES, VIDEOVIGILANCIA, USUARIOS WEB, USUARIOS REDES SOCIALES, CURRÍCULUM VITAE

5) Post Adaptación

1. Solicitudes de derechos.
2. Modificaciones del Documento de Seguridad.
3. Auditorías y controles periódicos realizados.
4. Violaciones de Seguridad.
5. Relación de cesionarios.
6. Recomendaciones del consultor.

Derechos del Titular

Registro de peticiones

No existen datos para este documento.

REGISTRO DE MODIFICACIONES DEL DOCUMENTO DE SEGURIDAD Y ANEXOS

El responsable del tratamiento o la persona delegada, será el encargado de actualizar el documento de seguridad, los anexos y también de divulgar los cambios realizados. Cada vez que se actualice el documento de seguridad se anotará en el siguiente formulario.

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

MODIFICACIONES

Registro automatizado de Modificaciones

Lista de las modificaciones o actualizaciones realizadas en el documento de seguridad, anexos u otros documentos.

Modificación	Código: 1
Fecha: 15/05/2024 **Versión:** 1 **Documento o apartado:** Primera versión del doc. de seg. sin modificaciones	

MODIFICACIONES

Registro manual de Modificaciones

Lista de las modificaciones o actualizaciones realizadas en el documento de seguridad, anexos u otros documentos.

Código	Fecha	Versión	Documento o apartado modificado	Descripción de la modificación

REGISTRO DE AUDITORÍAS Y CONTROLES PERIÓDICOS

Este apartado contendrá los resultados de los controles periódicos y de las auditorías realizadas en la empresa.

CONTROLES

Registro automatizado de Auditorías y Controles periódicos realizados en la empresa

No existen datos para este documento.

CONTROLES

Registro manual de auditorías y controles periódicos

Tipo de Control:	Fecha:	Documento/s Revisado/s:	Resultado del Control:	Persona/s o Departamentos que han intervenido:

VIOLACIONES

Registro de violaciones de seguridad

Registro de violaciones de seguridad para comunicar si procede, a la autoridad de control, a los interesados o al responsable.

VIOLACIONES

Registro automatizado de violaciones de seguridad

No existen datos para este anexo o documento.

VIOLACIONES **Registro manual de violaciones de seguridad**

Registro manual de violaciones de seguridad para comunicar si procede, a la autoridad de control, a los interesados o al responsable.

Nº:	Fecha:

Naturaleza:
Categorías y número aproximado de interesados afectados:
Categorías y número aproximado de registros de datos personales afectados:
Nombre y los datos de contacto del DPD o de otro punto de contacto en el que pueda obtenerse más información:
Describir las posibles consecuencias de la violación de la seguridad de los datos personales:
Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos:
Nombre: Firma:

Listado de cesionarios

Cesionarios

No existen datos para este anexo o documento.

RECOMENDACIONES:

- FIN DEL DOCUMENTO DE SEGURIDAD -
