REGISTRO DE ACTIVIDADES Y CATEGORÍAS DE ACTIVIDADES DE TRATAMIENTO

Reglamento General Europeo 679/2016 de
Protección de Datos de Carácter Personal
Ley Orgánica 3/2018, de Protección de Datos Personales
y Garantía de los Derechos Digitales.

Safetroop Technologies, S.L.

Datos del Responsable

SAFETROOP TECHNOLOGIES S.L.
B44925204
C/ Carrer Espinoi 8/10 Local 1
08024 - Barcelona
BARCELONA
ESPAÑA

Datos de Contacto

Teléfono: +34 685378085

Email: info@safetroop.com

Delegado de Protección de Datos

CARLOS TORTAJADA MONTUENGA
ABOGADO ICAM 92637
Auditor RGPD
C. SANTA ENGRACIA, 17 - 6º PLANTA
28010 - MADRID
MADRID
ESPAÑA
Tfno. 914456569
Email: equaldpo@equalprotecciondedatos.com

TRATAMIENTOS DE DATOS PERSONALES

1. INTRODUCCIÓN

El presente documento integra el Registro de Actividades de Tratamiento efectuadas por Safetroop Technologies, S.L. en calidad de Responsable del Tratamiento, así como el Registro de Categorías de Actividades realizadas en calidad de Encargado del Tratamiento, dado que actúa en determinados tratamientos como Responsable del Tratamiento y, en otros, como Encargado del Tratamiento por cuenta de Administraciones Públicas, todo ello de conformidad con el artículo 30 del Reglamento (UE) 2016/679 (RGPD).

Asimismo, el presente Registro se encuentra alineado con el sistema de gestión de seguridad implantado por la entidad y con los requisitos derivados del Esquema Nacional de Seguridad (ENS), constituyendo una herramienta de gobierno del dato, trazabilidad y gestión de riesgos.

Las medidas de seguridad reflejadas en este documento tienen carácter informativo y complementario a las evidencias, políticas, procedimientos y controles específicos documentados en la Declaración de Aplicabilidad (SoA), análisis de riesgos y resto de documentación ENS de la entidad.

1.1. MEDIDAS DE SEGURIDAD GENERALES APLICABLES A TODOS LOS TRATAMIENTOS

SAFETROOP TECHNOLOGIES, S.L. dispone de un sistema de gestión de seguridad de la información alineado con el Esquema Nacional de Seguridad (ENS), que incorpora medidas organizativas, operativas y técnicas destinadas a garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada.

Sin perjuicio de las medidas que de forma extensa están contempladas y auditadas en los procedimientos de certificación del ENS, las medidas fundamentales que Aplican a todos los tratamientos anteriores son las siguientes:

a) Gobierno y organización de la seguridad

El Responsable del Tratamiento dispone de:

- Política de Seguridad de la Información formalmente aprobada.
- Procedimientos de seguridad documentados.
- Sistema de gestión de riesgos.
- Inventario de activos.
- Procesos de revisión y mejora continua.
- Gestión documental de evidencias de cumplimiento.

b) Gestión de identidades y control de accesos

Se aplican medidas destinadas a garantizar que únicamente accedan a la información las personas autorizadas para ello, incluyendo:

- Identificación individual de usuarios.
- Autenticación robusta.
- Gestión formal de altas, modificaciones y bajas.
- Segregación de funciones.
- Principio de mínimo privilegio.
- Revisión periódica de permisos.

c) Protección de sistemas y servicios

El Responsable del Tratamiento dispone de:

- Configuración segura de sistemas.
- Gestión de vulnerabilidades.
- Actualización y parcheado.
- Protección frente a código malicioso.
- Control de cambios.
- Inventario de activos tecnológicos.

d) Registro de actividad y trazabilidad

Se mantienen mecanismos de:

- Registro de accesos.
- Registro de actividad.
- Conservación de evidencias.
- Monitorización de eventos.
- Investigación de incidentes.
- Trazabilidad de actuaciones.

e) Protección criptográfica

La información es protegida mediante:

- Cifrado de comunicaciones.
- Protección de claves criptográficas.
- Protocolos seguros de transmisión.
- Medidas de protección de información almacenada.

f) Seguridad de proveedores y servicios cloud

El Responsable del Tratamiento mantiene procedimientos de evaluación y supervisión de proveedores, incluyendo:

- Contratos de encargo del tratamiento.
- Acuerdos de nivel de servicio.
- Evaluación de garantías de seguridad.
- Control de interconexiones.
- Supervisión y evaluación continua de proveedores críticos.

g) Continuidad y recuperación

Se dispone de:

- Copias de seguridad periódicas.
- Procedimientos de restauración.
- Medidas de continuidad de negocio.
- Procedimientos de recuperación ante incidentes.

2.2. Criterios generales de conservación de datos

Sin perjuicio de los plazos de conservación que de forma específica sea necesario contemplar en supuestos de tratamientos concretos, con carácter general, los datos personales serán conservados durante el tiempo estrictamente necesario para cumplir la finalidad para la que fueron recabados.

Una vez finalizada dicha finalidad, los datos podrán permanecer bloqueados durante los plazos legalmente exigibles para atender posibles responsabilidades administrativas, tributarias, mercantiles, civiles, laborales o derivadas de la normativa de protección de datos y seguridad de la información.

El bloqueo de datos se realizará de conformidad con el artículo 32 de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

Finalizados los plazos de conservación y bloqueo aplicables, los datos serán suprimidos o anonimizados de forma segura.

Tratamiento	Conservación activa	Bloqueo / Conservación posterior	Base jurídica y normativa
Clientes	Durante la vigencia de la relación contractual	Hasta 6 años (mercantil), 4 años (fiscal) y 5 años para acciones contractuales	Art. 30 Código de Comercio; Arts. 66 a 70 Ley General Tributaria; Art. 1964 Código Civil
Contactos web y solicitudes de información	Hasta la resolución de la consulta o solicitud	Hasta el plazo de prescripción de posibles reclamaciones	Art. 1964 Código Civil; Art. 32 LOPDGDD
Contabilidad	Durante la gestión económica y fiscal	6 años desde el último asiento contable y, en su caso, 4 años a efectos tributarios	Art. 30 Código de Comercio; Ley General Tributaria
Proveedores	Durante la vigencia de la relación contractual	6 años mercantil, 4 años fiscal y 5 años contractual	Art. 30 Código de Comercio; Arts. 66 a 70 Ley General Tributaria; Art. 1964 Código Civil
Usuarios Agentes Autorizados	Durante la vigencia del servicio contratado por la entidad responsable	Conforme a las instrucciones documentadas del Responsable del Tratamiento y a las obligaciones derivadas del contrato de encargo	Art. 28 RGPD; Contrato de Encargo del Tratamiento
Alertas e incidencias operativas	Durante la prestación del servicio	Mientras resulte necesario para garantizar trazabilidad, auditoría, investigación de incidentes o defensa jurídica	ENS; Art. 32 RGPD; Art. 32 LOPDGDD
Administración	Durante la prestación	Mientras sea necesario para	Art. 1964 Código Civil;

técnica y soporte	del servicio	acreditar actuaciones técnicas, incidencias o responsabilidades derivadas del soporte prestado	ENS
Logs de acceso y seguridad	Conforme a la política de gestión de logs y seguridad de la información	Mientras resulte necesario para auditorías, investigación de incidentes, cumplimiento ENS y defensa jurídica	ENS; Art. 32 RGPD; Art. 32 LOPDGDD
Monitorización y eventos de seguridad	Conforme a la política de monitorización y seguridad	Mientras resulte necesario para investigación y trazabilidad de incidentes	ENS; Seguridad de la Información
Copias de seguridad	Según política de backup y continuidad	Conforme a los ciclos de rotación definidos y hasta la destrucción segura de los soportes	ENS; Plan de Continuidad y Recuperación
Registros relacionados con incidentes de seguridad	Durante la gestión activa del incidente	Hasta la prescripción de posibles responsabilidades administrativas, civiles o contractuales	RGPD; LOPDGDD; Código Civil

Conservación derivada de la normativa de protección de datos

En aquellos supuestos en los que puedan derivarse responsabilidades por incumplimiento de la normativa de protección de datos, la organización podrá conservar determinada información bloqueada durante los plazos necesarios para atender posibles procedimientos administrativos, reclamaciones o actuaciones de la autoridad de control competente.

A estos efectos se tendrán en consideración, entre otras disposiciones:

- Reglamento (UE) 2016/679 (RGPD).
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de Régimen Jurídico del Sector Público.

Conservación de evidencias de seguridad y cumplimiento ENS

Los registros, evidencias, logs, trazas, auditorías y demás información necesaria para garantizar la seguridad, trazabilidad, investigación de incidentes y cumplimiento del Esquema Nacional de Seguridad podrán conservarse durante los plazos necesarios para:

- La investigación de incidentes de seguridad.
- La realización de auditorías internas o externas.
- La acreditación del cumplimiento normativo.
- La defensa jurídica de la organización.
- La atención de requerimientos de organismos públicos competentes.

La conservación de dichas evidencias se realizará aplicando medidas adecuadas de acceso restringido, integridad, trazabilidad y protección frente a alteración o destrucción no autorizada.

Supresión definitiva

Una vez transcurridos los plazos de conservación y bloqueo indicados, los datos personales serán eliminados de forma segura o anonimizados, aplicando procedimientos que impidan su recuperación posterior, salvo que exista una obligación legal específica que justifique su mantenimiento.

ACTIVIDADES COMO RESPONSABLE DEL TRATAMIENTO

1.- CLIENTES

Finalidad del Tratamiento

La finalidad es la gestión de la relación mercantil, tanto desde un punto de vista administrativo y de cumplimiento de obligaciones fiscales, como desde un punto de vista comercial y de marketing.

Base jurídica de legitimación

El tratamiento de datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica (clientes o proveedores) estarán legitimados bajo la base jurídica del artículo 6.1.f.) del RGPD, es decir, el interés legítimo del Responsable del tratamiento. De acuerdo con el artículo 19.1.a) de la LOPD 3/2018 únicamente serán tratados los datos personales necesarios para la localización profesional. Por otro lado, para los clientes considerados personas físicas o usuarios domésticos, el tratamiento de sus datos está legitimado por el artículo 6.1.b y 6.1.c, es decir, la ejecución de un contrato y el cumplimiento de obligaciones legales.

Plazo de conservación

Una vez finalizada la relación contractual, o prestación de servicio, los datos se conservarán bloqueados exclusivamente para atender posibles responsabilidades legales durante los siguientes plazos:

- 6 años: artículo 30 Código de Comercio.
- 4 años: artículos 66 a 70 Ley General Tributaria.
- 5 años: artículo 1964 Código Civil.

Categorías de interesados

Clientes y personas de contacto.

Categorías de datos personales

Datos identificativos, profesionales, datos de contacto, facturación y relación contractual.

Categorías de destinatarios de cesiones

Administración tributaria, otros órganos de la administración pública, bancos.

Encargados de tratamiento

DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa con la que se mantiene suscrito un contrato de Encargado del Tratamiento con los requisitos contemplados en el artículo 28 del RGPD.

Transferencias internacionales de datos

No se realizan transferencias internacionales.

Medidas de seguridad

Sin perjuicio de las medidas generales de conformidad con la certificación del ENS indicadas al inicio del presente documento, de acuerdo con el Art. 32 del RGPD 679/2016 el responsable ha realizado una evaluación de los riesgos desde el punto de vista RGPD para poder garantizar los derechos de los interesados. En base a dicha evaluación se han adoptado las medidas técnicas y organizativas necesarias, que se han reflejado en el informe de análisis de riesgos correspondiente.

MEDIDAS PARA LA SEUDONIMIZACIÓN Y EL CIFRADO:

Se utilizarán contraseñas únicas e intransferibles para acceder a los datos, que no podrán ser reveladas a terceras personas, ni siquiera a compañeros de trabajo:

- Generación y distribución de contraseñas

La generación de contraseñas la realiza el Administrador del sistema, que las comunica al usuario que va a utilizarlas.

Los sistemas que realicen la identificación del usuario garantizarán que la introducción de la contraseña y su representación en pantalla, en el momento de la autenticación, se efectúan en un formato no legible para el resto de los usuarios.

- Almacenamiento de las contraseñas

No está permitido a los usuarios apuntar los identificadores y contraseñas, ni en papel ni en soporte electrónico.

- Renovación periódica de contraseñas

Las contraseñas son renovadas por el propio usuario que va a utilizarlas, al menos una vez al año y, además, toda vez que se sospeche que su confidencialidad ha sido comprometida.

MEDIDAS PARA RESTAURAR LA DISPONIBILIDAD Y ACCESO A DATOS TRAS UN INCIDENTE:

- Copias de seguridad:

Las copias de seguridad se realizan de forma diaria, en los servidores de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa con la que se mantiene suscrito un contrato de Encargado del Tratamiento con los requisitos contemplados en el artículo 28 del RGPD. La recuperación de datos desde las copias de seguridad se efectuará por el encargado de tratamiento, o con su autorización y bajo su supervisión, cada vez que se produzca una alteración, perdida o destrucción, total o parcial, de los datos personales, debiendo reconstruirse al estado en que se encontraban antes de la incidencia.

Cuando los ficheros o tratamientos a los que haya afectado la incidencia estén parcialmente automatizados y la existencia de documentación en papel permita la óptima reconstrucción de los datos, estos se deben grabar manualmente y dejar constancia motivada de ello en la descripción de la incidencia.

2.- PROVEEDORES

Finalidad del Tratamiento

Gestión de las relaciones contractuales, administrativas, económicas y operativas con proveedores, suministradores, colaboradores y prestadores de servicios necesarios para el desarrollo de la actividad de la entidad.

Base jurídica de legitimación

- Artículo 6.1.b RGPD: ejecución de contrato.
- Artículo 6.1.c RGPD: cumplimiento de obligaciones legales.

Plazos de conservación

Los datos se conservarán durante la vigencia de la relación contractual.

Posteriormente permanecerán bloqueados durante los siguientes plazos:

- 6 años conforme al artículo 30 del Código de Comercio.
- 4 años conforme a la Ley General Tributaria.
- 5 años conforme al artículo 1964 del Código Civil para acciones derivadas de relaciones contractuales.

Categorías de interesados

- Proveedores personas físicas.
- Representantes de proveedores personas jurídicas.
- Colaboradores externos.
- Personal de contacto de empresas proveedoras.

Categorías de datos

- Datos identificativos.
- Datos profesionales.
- Datos de contacto.
- Datos económicos y bancarios.
- Información contractual.

Destinatarios

- Entidades financieras.
- Administraciones Públicas competentes.
- Asesorías fiscales y contables.
- Auditores.

Transferencias internacionales

No previstas, salvo utilización de proveedores tecnológicos debidamente regularizados.

Medidas de seguridad

Sin perjuicio de las medidas generales de conformidad con la certificación del ENS indicadas al inicio del presente documento, de acuerdo con el Art. 32 del RGPD 679/2016 el responsable ha realizado una evaluación de los riesgos desde el punto de vista RGPD para poder garantizar los derechos de los interesados. En base a dicha evaluación se han adoptado las medidas técnicas y organizativas necesarias, que se han reflejado en el informe de análisis de riesgos correspondiente.

MEDIDAS PARA LA SEUDONIMIZACIÓN Y EL CIFRADO:

Se utilizarán contraseñas únicas e intransferibles para acceder a los datos, que no podrán ser reveladas a terceras personas, ni siquiera a compañeros de trabajo:

- Generación y distribución de contraseñas

La generación de contraseñas la realiza el Administrador del sistema, que las comunica al usuario que va a utilizarlas.

Los sistemas que realicen la identificación del usuario garantizarán que la introducción de la contraseña y su representación en pantalla, en el momento de la autenticación, se efectúan en un formato no legible para el resto de los usuarios.

- Almacenamiento de las contraseñas

No está permitido a los usuarios apuntar los identificadores y contraseñas, ni en papel ni en soporte electrónico.

- Renovación periódica de contraseñas

Las contraseñas son renovadas por el propio usuario que va a utilizarlas, al menos una vez al año y, además, toda vez que se sospeche que su confidencialidad ha sido comprometida.

MEDIDAS PARA RESTAURAR LA DISPONIBILIDAD Y ACCESO A DATOS TRAS UN INCIDENTE:

-Copias de seguridad:

Las copias de seguridad se realizan de forma diaria, en los servidores de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa con la que se mantiene suscrito un contrato de Encargado del Tratamiento con los requisitos contemplados en el artículo 28 del RGPD. La recuperación de datos desde las copias de seguridad se efectuará por el encargado de tratamiento, o con su autorización y bajo su supervisión, cada vez que se produzca una alteración, perdida o destrucción, total o parcial, de los datos personales, debiendo reconstruirse al estado en que se encontraban antes de la incidencia.

Cuando los ficheros o tratamientos a los que haya afectado la incidencia estén parcialmente automatizados y la existencia de documentación en papel permita la óptima reconstrucción de los datos, estos se deben grabar manualmente y dejar constancia motivada de ello en la descripción de la incidencia.

3.- CONTABILIDAD

Finalidad del tratamiento

Gestión contable, fiscal, económica y administrativa de la entidad, incluyendo la emisión y recepción de facturas, gestión de cobros y pagos, cumplimiento de obligaciones tributarias y elaboración de documentación económico-financiera.

Base jurídica de legitimación

- Artículo 6.1.c RGPD: cumplimiento de obligaciones legales.

Artículo 6.1.b RGPD: ejecución de contratos.

Plazos de conservación

Los documentos contables y fiscales se conservarán conforme a las siguientes obligaciones legales:

- Artículo 30 del Código de Comercio: 6 años.
- Ley General Tributaria (arts. 66 a 70): 4 años.
- Ley 58/2003 General Tributaria.
- Normativa mercantil y fiscal aplicable.

Finalizados dichos plazos, los datos serán eliminados o anonimizados, salvo que resulte necesaria su conservación para la defensa de reclamaciones judiciales o administrativas.

Categorías de interesados

- Clientes.
- Proveedores.
- Profesionales colaboradores.
- Representantes de entidades contratantes.

Categorías de datos

- Datos identificativos.
- Datos fiscales.
- Datos económicos y financieros.
- Datos bancarios.
- Información relativa a operaciones comerciales y contables.

Destinatarios

- Agencia Estatal de Administración Tributaria.
- Entidades financieras.
- Auditores.
- Administraciones Públicas competentes.
- Asesorías fiscales y contables.

Transferencias internacionales

No previstas.

Medidas de seguridad

Sin perjuicio de las medidas generales de conformidad con la certificación del ENS indicadas al inicio del presente documento, de acuerdo con el Art. 32 del RGPD 679/2016 el responsable ha realizado una evaluación de los riesgos desde el punto de vista RGPD para poder garantizar los derechos de los interesados. En base a dicha evaluación se han adoptado las medidas técnicas y organizativas necesarias, que se han reflejado en el informe de análisis de riesgos correspondiente.

MEDIDAS PARA LA SEUDONIMIZACIÓN Y EL CIFRADO:

Se utilizarán contraseñas únicas e intransferibles para acceder a los datos, que no podrán ser reveladas a terceras personas, ni siquiera a compañeros de trabajo:

- Generación y distribución de contraseñas

La generación de contraseñas la realiza el Administrador del sistema, que las comunica al usuario que va a utilizarlas.

Los sistemas que realicen la identificación del usuario garantizarán que la introducción de la contraseña y su representación en pantalla, en el momento de la autenticación, se efectúan en un formato no legible para el resto de los usuarios.

- Almacenamiento de las contraseñas

No está permitido a los usuarios apuntar los identificadores y contraseñas, ni en papel ni en soporte electrónico.

- Renovación periódica de contraseñas

Las contraseñas son renovadas por el propio usuario que va a utilizarlas, al menos una vez al año y, además, toda vez que se sospeche que su confidencialidad ha sido comprometida.

MEDIDAS PARA RESTAURAR LA DISPONIBILIDAD Y ACCESO A DATOS TRAS UN INCIDENTE:

- - Copias de seguridad:

Las copias de seguridad se realizan de forma diaria, en los servidores de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa con la que se mantiene suscrito un contrato de Encargado del Tratamiento con los requisitos contemplados en el artículo 28 del RGPD. La recuperación de datos desde las copias de seguridad se efectuará por el encargado de tratamiento, o con su autorización y bajo su supervisión, cada vez que se produzca una alteración, perdida o destrucción, total o parcial, de los datos personales, debiendo reconstruirse al estado en que se encontraban antes de la incidencia.

Cuando los ficheros o tratamientos a los que haya afectado la incidencia estén parcialmente automatizados y la existencia de documentación en papel permita la óptima reconstrucción de los datos, estos se deben grabar manualmente y dejar constancia motivada de ello en la descripción de la incidencia.

4.- CONTACTOS WEB Y SOLICITUDES DE INFORMACIÓN

Finalidad del tratamiento

Gestión de las consultas, solicitudes de información, peticiones de contacto, solicitudes comerciales, incidencias y cualquier otra comunicación remitida por los usuarios a través de los

formularios habilitados en el sitio web corporativo, correo electrónico u otros canales de comunicación facilitados por SAFETROOP TECHNOLOGIES, S.L.

Asimismo, este tratamiento permite mantener comunicaciones posteriores relacionadas con la solicitud realizada, incluyendo la remisión de información adicional solicitada por el interesado y la realización de actuaciones precontractuales cuando estas resulten necesarias.

Base jurídica de legitimación

- Artículo 6.1.a RGPD: consentimiento del interesado.
- Artículo 6.1.b RGPD: aplicación de medidas precontractuales solicitadas por el interesado.

Plazo de conservación

Los datos se conservarán durante el tiempo necesario para atender la solicitud realizada por el interesado.

Cuando la consulta derive en una relación contractual o comercial, los datos pasarán a integrarse en el tratamiento correspondiente.

En caso contrario, los datos podrán conservarse durante un plazo máximo de un año desde la última interacción, salvo que resulte necesario conservarlos para atender posibles reclamaciones o responsabilidades legales.

Posteriormente permanecerán bloqueados durante el plazo necesario para atender posibles responsabilidades derivadas de la relación mantenida, de conformidad con el artículo 1964 del Código Civil.

Categorías de interesados

- Usuarios del sitio web.
- Personas interesadas en los productos o servicios de la entidad.
- Representantes de entidades públicas o privadas.
- Potenciales clientes.

Categorías de datos

- Nombre y apellidos.
- Dirección de correo electrónico.
- Teléfono de contacto.
- Entidad u organización a la que pertenece el interesado.
- Cargo profesional.
- Contenido de la consulta o solicitud.
- Dirección IP y datos técnicos asociados a la navegación cuando proceda.

Destinatarios

No se prevén cesiones de datos salvo obligación legal o cuando resulte necesario para la prestación de servicios tecnológicos asociados al funcionamiento de la página web o los sistemas de comunicación utilizados.

Transferencias internacionales

No se prevén transferencias internacionales de datos, sin perjuicio de la utilización de proveedores tecnológicos que puedan implicar transferencias debidamente regularizadas conforme al RGPD.

ACTIVIDADES COMO ENCARGADO DEL TRATAMIENTO

1.- GESTIÓN DE USUARIOS AGENTES AUTORIZADOS

Finalidad del tratamiento

Prestación de servicios tecnológicos de alerta, coordinación operativa y asistencia a usuarios autorizados pertenecientes a cuerpos y fuerzas de seguridad.

Base jurídica de legitimación

Prestación de un servicio, relación contractual con el Responsable del Tratamiento correspondiente.

Plazos de conservación

Los datos serán tratados durante la vigencia del servicio contratado y conforme a las instrucciones documentadas de la entidad responsable del tratamiento. Finalizada la prestación, los datos serán devueltos, suprimidos o bloqueados conforme al contrato de encargo y normativa aplicable.

Categorías de datos: TIP o placa profesional, identificadores de usuario, credenciales, logs de acceso, dirección IP, datos de dispositivo y geolocalización puntual asociada a eventos o alertas.

Geolocalización únicamente activa cuando se produce una alerta o evento de seguridad que requiere la localización del agente para su atención operativa.

Categorías de destinatarios de cesiones

Administración pública, Órgano financiador

Transferencias internacionales de datos

No se realizan transferencias internacionales.

2.- GESTIÓN OPERATIVA DE ALERTAS E INCIDENCIAS

Finalidad

Tratamiento realizado por cuenta de las entidades responsables para permitir la gestión operativa de alertas de seguridad, incidencias, eventos y comunicaciones asociadas al uso de la plataforma tecnológica.

Base jurídica de legitimación

La determinada por la entidad responsable del tratamiento correspondiente, basada en relación contractual por prestación de servicios.

Plazos de conservación

Durante el tiempo necesario para la prestación del servicio y conforme a las instrucciones documentadas del responsable del tratamiento.

Los registros vinculados a incidentes de seguridad podrán conservarse durante los plazos necesarios para garantizar la investigación, trazabilidad y defensa jurídica de las actuaciones realizadas.

Categorías de interesados

- Agentes autorizados.
- Usuarios operativos autorizados por la entidad responsable.

Categorías de datos

- Identificadores profesionales.
- Registros de actividad.
- Geolocalización puntual asociada a eventos.
- Información relativa a alertas.
- Timestamps.
- Direcciones IP.

Categorías de destinatarios de cesiones

Administración pública, Órgano financiador

Transferencias internacionales de datos

No se realizan transferencias internacionales.

Medidas de seguridad

Sin perjuicio de las medidas generales de conformidad con la certificación del ENS indicadas al inicio del presente documento, de acuerdo con el Art. 32 del RGPD 679/2016 el responsable ha realizado una evaluación de los riesgos desde el punto de vista RGPD para poder garantizar los derechos de los interesados. En base a dicha evaluación se han adoptado las medidas técnicas y organizativas necesarias, que se han reflejado en el informe de análisis de riesgos correspondiente.

MEDIDAS PARA LA SEUDONIMIZACIÓN Y EL CIFRADO:

Se utilizarán contraseñas únicas e intransferibles para acceder a los datos, que no podrán ser reveladas a terceras personas, ni siquiera a compañeros de trabajo:

- Generación y distribución de contraseñas

La generación de contraseñas la realiza el Administrador del sistema, que las comunica al usuario que va a utilizarlas.

Los sistemas que realicen la identificación del usuario garantizarán que la introducción de la contraseña y su representación en pantalla, en el momento de la autenticación, se efectúan en un formato no legible para el resto de los usuarios.

- Almacenamiento de las contraseñas

No está permitido a los usuarios apuntar los identificadores y contraseñas, ni en papel ni en soporte electrónico.

- Renovación periódica de contraseñas

Las contraseñas son renovadas por el propio usuario que va a utilizarlas, al menos una vez al año y, además, toda vez que se sospeche que su confidencialidad ha sido comprometida.

MEDIDAS PARA RESTAURAR LA DISPONIBILIDAD Y ACCESO A DATOS TRAS UN INCIDENTE:

- - Copias de seguridad:

Las copias de seguridad se realizan de forma diaria, en los servidores de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa con la que se mantiene suscrito un contrato de Encargado del Tratamiento con los requisitos contemplados en el artículo 28 del RGPD. La recuperación de datos desde las copias de seguridad se efectuará por el encargado de tratamiento, o con su autorización y bajo su supervisión, cada vez que se produzca una alteración, perdida o destrucción, total o parcial, de los datos personales, debiendo reconstruirse al estado en que se encontraban antes de la incidencia.

Cuando los ficheros o tratamientos a los que haya afectado la incidencia estén parcialmente automatizados y la existencia de documentación en papel permita la óptima reconstrucción de los datos, estos se deben grabar manualmente y dejar constancia motivada de ello en la descripción de la incidencia.

Como se ha expuesto en el presente documento, las medidas organizativas, operativas y técnicas de las que dispone el Responsable del Tratamiento están alineadas con el Esquema Nacional de Seguridad (ENS), incluyendo control de accesos, autenticación, gestión de permisos, monitorización, trazabilidad, gestión de incidentes, protección cloud, protección de aplicaciones web, copias de seguridad, continuidad, control de cambios y desarrollo seguro.

Las restantes medidas descritas en el presente documento son complementarias a la Declaración de Aplicabilidad (SoA), políticas, procedimientos y resto de documentación ENS de la entidad.