# NORMATIVA INTERNA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE

## AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-

| | |
|---|---|
| Fecha versión | **01.12.2023** |
| Versión | **X.** |

# ÍNDICE

PARTEGENERAL
……..……..3

1. INTRODUCCIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS ……....4

2. ÁMBITO DE APLICACIÓN DE LA NORMATIVA INTERNA DE PROTECCIÓN DE DATOS …….5

3. NORMAS Y PROCEDIMIENTOS PARA GARANTIZAR LOS NIVELES DE SEGURIDAD …..……14

4. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL……25

5. FUNCIONES Y OBLIGACIONES DEL PERSONAL ……..….26

6. ENCARGADOS DEL TRATAMIENTO ……..28

7. NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS …..30

8. REVISIÓN ……32

9. INCUMPLIMIENTO DE LA NORMATIVA INTERNA DE PROTECCIÓN DE DATOS ……..33

10. CUÁNDO DEBE CONTACTAR CON NOSOTROS ……..34

11. APROBACIÓN DE LA NORMATIVA ……35

**ANEXOS A LAS MEDIDAS DE SEGURIDAD ……36**

ANEXO I- Copias de Seguridad ……37
ANEXO II- Ejercicio de los derechos ……...40
ANEXO III- Nombramientos ……54
ANEXO IV- Autorizaciones ……57
ANEXO V- Obligaciones y funciones del personal ……..64
ANEXO VI- Cláusulas y circulares ……77
ANEXO VII- Brecha de Seguridad ……90
ANEXO VIII- Registro de Incidencias ……94
ANEXO IX- Documentación adicional ……..97
ANEXO X- Videovigilancia ……100
ANEXO XI- Descripción de los sistemas de información ……...102
ANEXO XII- Enfoque de aproximación al riesgo ……108
ANEXO XIII- Registro de Actividades ……115
ANEXO XIV- Usuarios con acceso al registro de actividades ……..123
ANEXO XV- Aplicaciones de acceso a los ficheros ……..127
ANEXO XVI- Encargados del Tratamiento ……..……129

# PARTE GENERAL

# 1. INTRODUCCIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El 14 de abril de 2016, el Parlamento Europeo aprobó la normativa de protección de datos europea, tras un largo proceso legislativo de más de cuatro años. Con la aprobación del RGPD se reforma la normativa de protección de datos europea, estableciendo nuevas reglas que sustituyen el antiguo marco regulatorio de la Unión Europea en materia de protección de datos.

La técnica legislativa del Reglamento utilizada por la UE para regular la protección de datos supone que el mismo será de aplicación directa a todos los Estados Miembros de la Unión Europea sin necesidad de que sea transpuesto por las normas nacionales de los Estados.

Por tanto, el RGPD deroga y sustituye a la Directiva 95/46/CE reforzando el derecho de la protección de datos de la Unión Europea, que se constituye como un pilar básico de las garantías y libertades en Europa.

A través del RGPD se consigue armonizar en todos los Estados miembros de la UE la dispersión normativa existente hasta entonces en materia de protección de datos. El RGPD es una norma única de aplicación directa a todos los Estados cuyo objetivo principal es otorgar un mayor control a los ciudadanos europeos sobre su información privada, y permitir una aplicación uniforme en toda la Unión Europea con el objetivo de alcanzar un nivel de protección de datos razonable en todo el territorio de la UE que evite la aplicación las diferentes normativas existentes hasta entonces en cada Estado Miembro de la UE.

Conforme el art. 99 del RGPD el mismo entra en vigor a los 20 días de su publicación en el Diario Oficial de la Unión Europea, es decir el 24 de mayo de 2016, sin embargo es directamente aplicable y obligatorio en todos sus elementos en cada Estado Miembro **a partir del 25 de mayo de 2018,** disponiendo por tanto los Estados Miembros y sus respectivas Autoridades de Control de un periodo de 2 años para su aplicación e interpretación de los distintos derechos y obligaciones que establece.

Esta normativa interna es de obligado cumplimiento para todos los responsables del tratamiento y en su caso, para los encargados del tratamiento.

El artículo 24 y 28 del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), establecen que *"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable y, en su caso, el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario*

# 2. ÁMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD

Esta normativa interna es única y será de aplicación a todos los ficheros o tratamientos recogidos en el registro de actividades que se hallan bajo la responsabilidad de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Debe **mantenerse en todo momento actualizado** y debe ser revisado siempre que se produzcan cambios que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, como son cambios relevantes en:

- enfoque de aproximación al riesgo

- el registro de actividad

- el sistema de tratamiento empleado

- los sistemas de información

- la evaluación de impacto

Debe mantenerse adecuado a las disposiciones vigentes en materia de protección de los datos de carácter personal.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, son los relacionados en el apartado 2.2.

Todas las personas que tengan acceso a los datos de los ficheros, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento con la parte que le afecte será entregada, para su conocimiento, a cada persona autorizada a acceder a los datos de los Ficheros, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

## 2.1. RESPONSABLE DEL TRATAMIENTO

**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**
C/ Serrano, 93, 3º E,
28006,Madrid
A28709319
info@ausmar.es
www.ausmar.com

## 2.2. MEDIDAS DE SEGURIDAD- PRINCIPIO DE RESPONSABILIDAD PROACTIVA.

Las medidas de seguridad se regirán por el principio de "Accountability" o de**"Responsabilidad Proactiva"**, este principio consiste, para los responsables y encargados del tratamiento, una obligación "proactiva y sistemática" del cumplimiento de la normativa de protección de datos desde el diseño y por defecto en aquellas áreas de la organización donde sean necesarias.

Constituye un principio fundamental en la normativa de protección de datos (incluido dentro de los principios fundamentales de tratamiento del art. 5 del RGPD) que no es otro que la obligación de los responsables y encargados de implantar un sistema interno de cumplimiento en materia de protección de datos. Sistema que estará integrado por distintas políticas o procesos internos de privacidad que deberán ser actualizados y auditados periódicamente de manera que permitan demostrar el cumplimiento del RGPD.

El objetivo final de la implantación de esas medidas de protección de datos no es otro que garantizar que las actividades de tratamiento realizadas cumplen con lo establecido en el Reglamento.

Las medidas de seguridad que tendrá que aplicar el responsable y el encargado del tratamiento a las que hace referencia el RGPD se podría resumir en las siguientes:

- Enfoque de aproximación al riesgo
- Registro de Actividades.
- Medidas de Protección de Datos desde el Diseño.
- Medidas de Protección de Datos por Defecto.
- Medidas de Seguridad Adecuadas.
- Evaluaciones de Impacto.
- Autorización previa o Consultas previas con la Autoridad de Control.
- Delegado de Protección de Datos.
- Notificación de Violación de Seguridad.

## 2.3. ENFOQUE DE APROXIMACIÓN AL RIESGO

Para el cumplimiento del principio de "Responsabilidad Proactiva" el responsable y encargado de tratamiento deberán previamente realizar un análisis **y estudio del cumplimiento en materia de protección de datos basado en el riesgo**. Es decir, deberán analizar qué medidas de protección de datos son necesarias implantar para garantizar el cumplimiento del RGPD, en función de naturaleza, alcance, contexto y finalidades del tratamiento de datos que realicen, así como de los riesgos o probabilidades de intromisión en los Derechos y libertades de los interesados.

De esta manera cuanto más probable y grave sea el riesgo del tratamiento, más medidas de protección de datos serán necesarias implantar para contrarrestarlos.

## 2.4. REGISTRO DE ACTIVIDADES

El Registro de Actividades se encuentra recogido en el art. 30 del RGPD y establece que es obligatorio para aquellas empresas con empleados superiores a 250 trabajadores o que teniendo menos trabajadores sus tratamientos supongan un mayor riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1.

No obstante, junto con el enfoque de aproximación al riesgo, esta medida es clave para identificar y organizar el cumplimiento de las medidas en función del tipo de tratamiento o actividades identificadas.

Por último, el Registro de Actividades vendría en cierta medida a cubrir la obligación establecida por la normativa anterior respecto de la notificación de ficheros ante la Agencia Española de Protección de Datos.

La información que debe contener dichos registros, difiere en función de si se trata de un responsable de tratamiento o un encargado.

En el caso de los responsables de tratamiento, los registros de actividades deberán incluir la siguiente información:

El Nombre y los datos de contacto del responsable, y, en su caso, del corresponsable, del representante del responsable, y del Delegado de Protección de Datos:

- Los fines del tratamiento;
- Las categorías de interesados;
- Las categorías de datos personales
- Las categorías de destinatarios;
- Las transferencias internacionales de datos y la documentación de las garantías adecuadas adoptadas;
- Los plazos previstos para la supresión de las diferentes categorías de datos;
- Descripción general de las medidas técnicas y organizativas de seguridad.

Por otro lado, en el caso de los encargados de tratamiento el Registro de Actividades deberá incluir la siguiente información:

- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del Delegado de Protección de Datos;
- Las categorías de datos personales efectuadas por cuenta de cada responsable;
- Las transferencias internacionales de datos y la documentación de las garantías adecuadas adoptadas;
- Descripción general de las medidas técnicas y organizativas de seguridad.

Por último, se establece que dichos Registros de Actividades deberán constar por escrito y quedara disposición de la Agencia Española de Protección de Datos.

## 2.5. MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS

Las medidas de seguridades técnicas y organizativas vienen recogidas en el art. 32 del RGPD.

Las medidas de seguridades técnicas y organizativas se deberán implantar en función del nivel adecuado al riesgo de los distintos tratamientos. En consecuencia, será fundamental identificar los niveles de riesgo existentes en cada tratamiento de datos para poder determinar las medidas de seguridad técnicas que deberán ser implantadas por el responsable o encargado de tratamiento.

De igual forma a la privacidad por defecto y desde el diseño, se deberá tener en cuenta en la implantación de dichas medidas de seguridad:

- El estado de la técnica.
- El coste de aplicación.
- La naturaleza del tratamiento.
- El ámbito de aplicación o alcance.
- El contexto.
- Las finalidades del tratamiento.
- Los riesgos de diversa probabilidad y gravedad (no sólo riesgo alto) que entrañe para los derechos y libertades de los interesados.

Será, por tanto, un estudio y análisis específico basado en el enfoque al riesgo que deberán realizar los responsables y encargados del tratamiento a fin de mantener la seguridad en el tratamiento de datos. Para dicha evaluación de riesgo, se deberán tener en cuenta los riesgos derivados del tratamiento que sean susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales como son:

- La destrucción.
- Pérdida o alteración accidental o ilícita de los datos personales en la transmisión, conservación o tratamiento.
- La comunicación o accesos no autorizados a los datos.

A diferencia de la Ley Orgánica de Protección de Datos, el Reglamento General de Protección de Datos no establece un listado de medidas de seguridad que deben de ser aplicables a los tratamientos de datos, sí se establece que en todo caso entre otras medidas se deberá garantizar:

- La seudonimización y el cifrado de datos personales;
- La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Para evaluar las medidas de seguridad a aplicar al tratamiento de datos personales se tendrá en cuenta los riesgos que presente el tratamiento como consecuencia de:

a) la destrucción, pérdida o alteración accidental o ilícita de datos personal es transmitidos, conservados o tratados de otra forma.
b) la comunicación o acceso no autorizados a dichos datos.

La adhesión a un código de conducta o certificación podrá servir de elemento para demostrar el cumplimiento de los requisitos de seguridad.

## 2.6. MEDIDAS DE SEGURIDAD ADECUADAS

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Atendiendo a la naturaleza de la información tratada, el RGPD diferencia entre los datos especialmente protegidos y los que no lo son. A los datos especialmente protegidos, el RGPD les da una nueva mención y ahora pasan a llamarse **"categorías especiales de datos"** e incluye dos nuevas categorías: Datos genéticos y Datos biométricos.

### 2.6.1. RECURSOS PROTEGIDOS

La protección de los datos de los Ficheros, incluidos en el registro de actividades, frente a accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los recursos que, por servir de medio directo o indirecto para acceder a los Ficheros, deberán ser controlados por esta normativa son:

1. Los centros de tratamiento, unidades y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan, tanto para el procesamiento, uso, utilización, depósito o almacén de los datos personales que contengan.
2. Los puestos de trabajo, locales o remotos, desde los que se acceda a los Ficheros.
3. Los servidores, si los hubiese, y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado e los Ficheros.
4. Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos, ordenadores y otros dispositivos portátiles o de almacenamiento o proceso de datos.
5. Las redes de comunicaciones de datos ya sean externas o locales y sus sistemas de interconexión.

## 2.7. EVALUCACIÓN DE IMPACTO

La evaluación de impacto viene recogida en el art. 35 del RGPD.

El Responsable de Tratamiento, antes del tratamiento, en aquellos supuestos en los que el tratamiento entrañe un alto riesgo para los derechos y libertades de los titulares de los datos o interesados, realizará una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. En determinados supuestos dicha evaluación de impacto será obligatoria para los Responsables y deberá contener al menos:

a) una descripción sistemática de las operaciones de tratamiento previstas.
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de Tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados.
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Si el resultado de la evaluación entraña un alto riesgo para los derechos y libertades de las personas físicas, deberá ser consultarse previamente a la Autoridad de Control.

## 2.8. AUTORIZACIÓN PREVIA O CONSULTAS PREVIAS CON LA AUTORIDAD DE CONTROL

La consulta previa a la Autoridad de control en supuestos de Evaluación de Impacto viene recogida en el art. 36 del RGPD.

La Consulta previa de la Autoridad de control se producirá cuando en aquellos supuestos en los que el responsable de tratamiento considera que en la Evaluación de Impacto el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación.

Recibida la consulta la Autoridad de control podrá:

- Asesorar por escrito al responsable o encargado.
- Utilizar cualquiera de sus poderes para prohibir el tratamiento.

Por último, además de la consulta o autorización identificada en los supuestos de Evaluaciones de Impacto el RGPD señala que el Derecho Nacional de los Estados miembros podrá establecer consulta y petición de autorización previa en relación con los tratamientos derivados de una misión realizada en interés público por parte del responsable.

## 2.9. EL DELEGADO DE PROTECCIÓN DE DATOS

La figura del Delegado de Protección de Datos viene recogida en los art. 37 a 39 del RGPD y establece que el Responsable y el Encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) Las actividades principales consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual o seguimiento regular de los titulares de datos o interesados a gran escala, o
c) Las actividades principales se realicen sobre categorías especiales de datos a gran escala.

El Delegado de Protección de Datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 del RGPD. Así mismo podrá ser externalizado o formar parte de la plantilla del responsable o encargado. Sus datos de contacto deberán ser publicados y comunicados a la Autoridad de Control competente. A este respecto conviene señalar que no necesariamente se deben publicar el nombre y apellidos del Delegado de Protección de Datos bastando identificar los datos de contacto del mismo.

### 2.9.1. POSICIÓN Y FUNCIONES DEL DPD O DPO

La posición del DPD o DPO se encuentran recogidos en el art.38 del RGPD:

- Debe participar de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
- Se le deberán facilitar los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.
- No puede recibir instrucciones en lo que respecta al desempeño de dichas funciones.
- No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.
- Rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.
- Los interesados podrán ponerse en contacto con el Delegado de Protección de Datos para cualesquiera cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.
- Estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.
- Podrá desempeñar otras funciones y cometidos, debiendo garantizarse que las mismas no den lugar a un conflicto de intereses.

Respecto a las funciones del Delegado de Protección de Datos el art. 39 del RGPD señala que las funciones mínimas serán:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les conforme al RGPD, así como de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
- Supervisar el cumplimiento de lo dispuesto en RGPD y de otras disposiciones o 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 del RGPD.
- 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.

## 2.10. VIOLACIONES DE SEGURIDAD

Las notificaciones sobre violaciones de seguridad o quiebras vienen recogidas en los arts. 33 y 34 del RGPD.

El responsable de tratamiento deberá notificar a la Autoridad de Control tan pronto como tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales. **Dicha notificación deberá realizarse sin dilación indebida y a más tardar en el plazo de 72 horas después de que haya tenido constancia de la misma**, salvo que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañar sede una indicación de los motivos de la dilación, pudiendo facilitarse información por fases.

La violación de seguridad deberá quedar registrada y documentada por el responsable de tratamiento identificando los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

Así mismo, se establece que el encargado del tratamiento estará obligado a notificar sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

Además de la comunicación a la Autoridad de Control el responsable tratamiento deberá comunicar al interesado sin dilación indebida, la violación de la seguridad de los datos personales cuando la misma entrañe un alto riesgo para los derechos y libertades de las personas físicas.

No será necesaria la comunicación al interesado, si el responsable cumple con alguna de las siguientes condiciones:

- El responsable del tratamiento ha adoptado con anterioridad a la violación de seguridad(ex-ante), medidas de protección técnicas y organizativas apropiadas sobre los datos que sufrieron dicha brecha o violación de seguridad, de manera que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como por ejemplo el cifrado;
- El responsable del tratamiento tras la violación de seguridad (ex-post) ha tomado medidas para garantizar que ya no se materializará un alto riesgo para los derechos y libertades del interesado;
- 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.

# 3. NORMAS Y PROCEDIMIENTOS PARA GARANTIZAR LOS NIVELES DE SEGURIDAD

## 3.1.1. CONTROL DE ACCESO

El personal sólo puede acceder a los datos y recursos necesarios para el desarrollo de sus funciones. El Responsable del Tratamiento establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

Para el caso de soportes informáticos, puede consistir en asignar contraseñas de acceso a los mismos, u otros dispositivos más sofisticados: biométricos, llaves USB, etc.; y para el caso de documentos en papel, en la entrega de llaves que faciliten la apertura de los dispositivos de almacenamiento donde se recopile la información.

Exclusivamente el Responsable del Tratamiento identificado en el aparatado 2.1 de éste documento, está autorizado para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el mismo.

Los procedimientos para efectuar el alta, modificación y baja de las autorizaciones de acceso a los datos, así como los controles de acceso a los sistemas de información, se encuentran descritos en el ANEXO IV.

En el ANEXO XIV se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos.

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

## 3.1.2. RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del Responsable del Tratamiento será preciso que exista su autorización previa, y en todo caso, garantizarse las medidas de seguridad correspondiente al tipo de fichero tratado.

En el ANEXO IV se recogen las autorizaciones para tratar datos fuera de las instalaciones del Responsable del Tratamiento, así como el periodo de validez de las mismas.

## 3.2. MEDIDAS DE SEGURIDAD PARA FICHEROS AUTOMATIZADOS

Las medidas de seguridad deben incluir entre otras las siguientes:

- La seudonimización y el cifrado de datos personales;
- La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

**La seudonimización**, tal y como la define el RGPD, consiste en el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

**El cifrado de datos personales** consiste en transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger.

Por su parte, **la resiliencia**, es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

### 3.2.1. IDENTIFICACIÓN Y AUTENTICACIÓN

El Responsable del Tratamiento establecerá medidas de seguridad en los sistemas informáticos para garantizar que únicamente accederá a los ficheros el personal autorizado para ello.

De la misma forma, establecerá un sistema que permita la identificación personalizada de todos los usuarios para acceder al sistema de información, y la debida autenticación para verificar su identidad.

Existen diferentes procedimientos de identificación como certificados electrónicos, datos biométricos o huellas dactilares. Las contraseñas personales, sin embargo, constituyen hoy todavía uno de los métodos más usados para proteger el acceso a los datos, y por tanto, deben estar especialmente protegidas, de modo que deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al Responsable del Tratamiento o al Delegado de Protección de Datos y subsanada en el menor plazo de tiempo posible.

Existirá un procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad de las contraseñas cuando el mecanismo de autenticación se base en este sistema.

La periodicidad máxima con la que tienen que ser cambiadas las contraseñas no debe ser superior a **tres meses** y se almacenarán de forma ininteligible mientras estén vigentes.

Las contraseñas han de ser suficientemente complejas y difícilmente adivinables por terceros. Para ello, **a modo de ejemplo**, pueden seguirse las siguientes pautas:

° Tener una longitud mínima de entre **4 y 6 caracteres alfanuméricos**; o

° No coincidir, ni siquiera en parte, con el código de usuario; o

° No estar basados en cadenas de caracteres fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).

Al acceso al sistema por primera vez: el administrador asignará una contraseña provisional al nuevo usuario, que deberá ser cambiada en su primer acceso al sistema por una que sólo conozca el usuario y en base a las características definidas anteriormente.

Se ha de limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información por parte de los usuarios, **por ejemplo, entre 3 y 5 veces.**

### 3.2.2. ACCESO A TRAVÉS DE REDES DE COMUNICACIONES

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

### 3.2.3. COPIAS DE RESPALDO Y RECUPERACIÓN (COPIAS DE SEGURIDAD)

La seguridad de los datos personales supone la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y de los servicios de tratamiento.

Para garantizar estos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y recuperación, de forma, que ante un fallo informático, permitan reconstruir el fichero en el estado que se encontraba antes de la pérdida.

Se realizarán copias de seguridad al menos **una vezal díacomo mínimo**, salvo que en este intervalo no se haya producido ninguna actualización de datos.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado que se encontraban al tiempo de producirse la pérdida o destrucción.

Si la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el

objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos.

El Responsable del Tratamiento verificará **semestralmente** los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información que traten con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en la normativa interna de protección de datos. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

**Se recomienda conservar** una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente a aquel en el que se encuentran los equipos informáticos que los tratan **(preferentemente mediante un sistema de "cloud")**, que deberá cumplir en todo caso las medidas de seguridad exigidas, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

En el ANEXO I se detallan los procedimientos de copia de seguridad de los ficheros.

### 3.2.4. TRASLADO DE SOPORTES

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

- El traslado del soporte fuera de las instalaciones debe realizarse siempre en un maletín o contenedor similar con mecanismo de apertura de llave o combinación.

- Cifrar siempre que sea posible la información que contiene o utilizar otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

### 3.2.5. DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

1. Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

2. Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

3. Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al Responsable de Seguridad o al Responsable del Tratamiento.

4. El Responsable del Tratamiento deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

## 3.3. MEDIDAS DE SEGURIDAD PARA FICHEROS NO AUTOMATIZADOS

### 3.3.1. CRITERIOS DE ARCHIVO

El archivo de soportes o documentos se realizará de acuerdo con determinados criterios.

Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación, cancelación, potabilidad y supresión.

En aquellos casos en que no exista normativa aplicable, el Responsable del Tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Los criterios y procedimientos de archivo se encuentran descritos en el ANEXO II.

### 3.3.2. ALMACENAMIENTO DE LA INFORMACIÓN

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal, deberán disponer de mecanismos que obstaculicen su apertura, mediante llaves u otros dispositivos análogos.

Cuando las características físicas no permitan adoptar esta medida, el Responsable del Tratamiento adoptará las medidas que impidan el acceso de personas no autorizadas.

Los dispositivos de almacenamiento utilizados para almacenar datos de carácter personal de nivel alto, deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los

documentos incluidos en el fichero. En el caso de que las características de los locales impidan cumplir lo anteriormente indicado se adoptarán medidas alternativas.

Los dispositivos utilizados para almacenar datos de carácter personal, se encuentran descritos en el ANEXO IV.

### 3.3.3. ACCESO A LOS DOCUMENTOS

El acceso a los documentos que contengan datos de carácter personal, se limitará de forma exclusiva al personal autorizado e identificado en el ANEXO IV.

### 3.3.4. CUSTODIA DE DOCUMENTOS

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

### 3.3.5. TRASLADO DE DOCUMENTACIÓN

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

- El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.

- En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

### 3.3.6. DESTRUCCIÓN DE DOCUMENTACIÓN

Uno de los mayores peligros para la confidencialidad de los datos son los documentos desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general, ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.

- Soportes en papel y no demasiado voluminosos, deberán ser destruidos en una destructora de papel.

- En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.

- El Responsable del Tratamiento deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

### 3.3.7. COPIA O REPRODUCCIÓN

La realización de copias o reproducción de los documentos con datos personales d, sólo se podrá realizar bajo el control del personal autorizado para ello.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida, según lo descrito en el punto 3.3.6.

## 3.4. ENTORNO DE SEGURIDAD

### 3.4.1. CENTROS DE TRATAMIENTO Y LOCALES

Los locales donde se ubican los ficheros deben ser objeto especial de protección que garanticen la confidencialidad e integridad de los datos protegidos.

- Los locales deberán contar con los medios mínimos de seguridad que garanticen la confidencialidad e integridad de los datos protegidos, siendo conveniente que disponga de dispositivos extintores, alarmas, etc.

- Si el tratamiento de los datos del fichero se realiza en locales ajenos, debido a un contrato con un Encargado de tratamiento, el Encargado de tratamiento deberá elaborar una normativa interna de protección de datos en la que se describan las medidas de seguridad adoptadas para proteger el fichero o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación a dicho tratamiento.

## 3.4.2. PUESTOS DE TRABAJO

Son todas las estancias, despachos, mesas de trabajo, dispositivos desde los cuales se puede acceder a los datos del fichero (como por ejemplo, ordenadores personales o terminales de trabajo).

- Cada puesto de trabajo estará bajo la responsabilidad de una persona de las autorizadas en el ANEXO IV, que garantizará que la información no pueda ser vista por personas no autorizadas.

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

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

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

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

- El trabajo fuera de los locales del Responsable del Tratamiento sólo se podrá realizar cuando exista una autorización previa de él mismo o del Delegado de Protección de Datos garantizándose el nivel de seguridad.

- No deberá copiarse, ni transportar información en portátiles, o equipos que se encuentren fuera de las oficinas sin la correspondiente autorización del Responsable del Tratamiento. Especial consideración deberán tener los puestos de trabajo portátiles, como ordenadores portátiles o “smartphones”. Estos dispositivos deberán contar como mínimo con las mismas medidas de seguridad que los puestos de trabajo fijos, con una especial atención a los controles de acceso, que impidan acceder a los puestos de trabajo por parte de terceros en caso de pérdida o robo.

## 3.4.3. SISTEMA OPERATIVO Y COMUNICACIONES

Aunque las aplicaciones que acceden al fichero se encuentran descritas en el ANEXO VII, al estar el fichero ubicado en un ordenador con un sistema operativo determinado y poder contar con conexiones que le comunican con otros ordenadores, es posible, para personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación.

Se debe regular el uso y acceso a las partes del sistema operativo, herramientas o programas de utilidad, o del entorno de comunicaciones sean o no públicas, para impedir que personas no autorizadas con conocimientos tecnológicos avanzados en estos entornos puedan saltarse las barreras de seguridad de la aplicación o sistema de acceso al fichero.

- Cada fichero deberá tener un Administrador, que puede ser común para todos los ficheros o distinto en cada uno de ellos.

- El sistema operativo donde se ejecuta la aplicación, deberá tener su acceso restringido mediante código de usuario y contraseña. Ninguna herramienta o programa de utilidad que permita el acceso al Fichero deberá ser accesible a ningún usuario o administrador no autorizado.

- El Administrador del fichero deberá responsabilizarse de guardar en lugar protegido las copias de seguridad del Fichero, de forma que no tengan acceso a las mismas personas no autorizadas.

- Si la aplicación o sistema de acceso al Fichero utilizase usualmente ficheros temporales, o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, el administrador deberá asegurarse que estos datos no pueden ser accedidos posteriormente por personal no autorizado.

- Si el ordenador en el que está ubicado el Fichero forma parte de una red de comunicaciones, de forma que desde otros equipos conectados a esta red, sea posible acceder al Fichero, el administrador responsable del sistema, deberá asegurarse que no se permite el acceso a personas no autorizadas.

## 3.4.4. APLICACIONES DE ACCESO AL FICHERO

Son aquellos programas o aplicaciones con las que se puede acceder a los datos del Fichero, y que son utilizadas por los usuarios para acceder a ellos. Las aplicaciones que acceden a los ficheros están descritas en el ANEXO XV.

Estos programas pueden ser aplicaciones expresamente diseñadas para acceder al Fichero, o paquetes de uso general disponibles en el mercado.

- Las aplicaciones que acceden al Fichero deberán tener su acceso restringido mediante un código de usuario y una contraseña, o bien, mediante otros sistemas, como firma electrónica o control biométrico, por ejemplo.

- Si la aplicación informática que permite el acceso al Fichero no cuenta con un control de acceso, deberá ser al propio sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado mediante el citado nombre de usuario y contraseña.

### 3.4.5. BASES DE DATOS O ARCHIVOS OFIMÁTICOS

Los datos personales están ubicados físicamente en ficheros o en bases de datos, que deben ser protegidos.

Por otra parte, en la operativa diaria de tratamiento de los datos, pueden producirse copias de los datos protegidos sobre otros ficheros o archivos ofimáticos para tratamientos especiales. En estos casos deberá prestarse la adecuada protección a estos ficheros mientras existan.

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

- Realizar siempre las copias sobre un mismo directorio para que no queden dispersas por el disco duro, y siempre sea posible conocer donde están los datos temporales.

- Tras realizar el tratamiento requerido, proceder a su inmediata eliminación.

- Los ficheros temporales creados deberán cumplir el nivel de seguridad que les corresponda en función de los datos que contienen.

## 3.5. CONTROLES PERIÓDICOS DE VERIFICACIÓN

El cumplimiento de las normas que contiene este documento de seguridad deberá ser periódicamente comprobado, de forma que puedan detectarse y subsanarse anomalías.

- El Responsable del Tratamiento comprobará, con una periodicidad al menos **trimestral**, que la lista de usuarios autorizados para acceder al Ficheros, y que se encuentra en el ANEXO IV, corresponde con la lista de usuarios realmente autorizados en la aplicación de acceso al Fichero y perfiles.

- Se comprobará, al menos, de forma **semestral**, la existencia de copias de respaldo que permitan la recuperación del Fichero, realizando una prueba de restaurado que verifique la correcta definición de los procedimiento y proceso de recuperación, y enviando evidencias de esta comprobación al Responsable del Tratamiento.

- A su vez, también con periodicidad al menos **semestral**, los administradores del Fichero comunicarán al Responsable del Tratamiento o al Delegado de

Protección de Datos cualquier cambio que se haya realizado en los sistemas de información, como cambios en el hardware o software, bases de datos, aplicaciones de acceso al fichero, etc., procediendo a la actualización de dichos anexos.

- El Responsable del Tratamiento analizará, al menos con una periodicidad trimestral, la información registrada en el registro de incidencias para adoptar las medidas correctoras oportunas que prevengan la ocurrencia de las mismas en el futuro.

- El Responsable del Tratamiento comprobará en todo momento si se produce una brecha o violación de seguridad en la empresa y llevar a cabo el procedimiento correspondiente.

- Al menos **cada dos años** se realizará una auditoría en los términos que se recogen en el apartado 8.2 de esta Normativa Interna de Protección de Datos.

# 4. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el capítulo siguiente.

El Responsable del Tratamiento debe poner en conocimiento de personal las medidas y normas que les afectan en el desarrollo de sus funciones, así como de las consecuencias de no cumplirlas. Asimismo, deberá tener a disposición del personal la parte que les afecte de la presente normativa interna de protección de datos.

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

Se les dará una copia de las Funciones y Obligaciones del personal, y que se encuentran en el ANEXO V.

# 5. FUNCIONES Y OBLIGACIONES DEL PERSONAL

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

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

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

El Responsable del Tratamiento, y el personal a su cargo autorizado para el uso de los datos de carácter personal, están sujetos al cumplimiento de los siguientes deberes y obligaciones:

El **Responsable del Tratamiento** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Las obligaciones y funciones del Responsable del Tratamiento se encuentran recogidas en el art. 24 del RGPD:

- Aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme a la legislación vigente.
- Adoptar las políticas en materia de protección de datos.
- Garantizar que el Delegado de Protección de Datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
- Adherirse al Código de Conducta que pueda aprobarse por parte de la Comisión u organismo correspondiente.
- Llevar un registro de actividades de tratamiento en caso de tratar datos personales que supongan un riesgo para los derechos y libertades del interesado y/o de manera no ocasional, o que implique el tratamiento de categorías especiales de datos y/o datos relativos a condenas e infracciones.

Además del Responsable del Tratamiento, el personal afectado por esta normativa se puede clasificar en los siguientes perfiles:

1. **Delegado de Protección de Datos:** como ya hemos visto sus funciones en el punto 2.9 de éste documento, ésta figura se encargará de coordinar y supervisar las medidas de seguridad del Responsable del Tratamiento.

2. **Responsable de Seguridad:** será la persona designada por el DPO o en su defecto, por el Responsable del Tratamiento para coordinar todos los aspectos relacionados y definidos de las medidas de seguridad efectuadas.

3. **Administradores**, **encargados** de administrar o mantener el entorno operativo del Fichero, así como conceder, alterar o anular el acceso autorizado a los datos.

4. **Encargado del tratamiento**, es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o con otros, trate datos personales por cuenta del Responsable del Tratamiento, como consecuencia de una relación jurídica descrita en el ANEXO XVI, y cuyo ámbito se delimita en este documento. El tratamiento de los datos por un Encargado de tratamiento estará sometido en todo caso a las medidas de seguridad contempladas en este Documento.

5. **Usuarios del Fichero**, que es el personal de la empresa o entidad con acceso a datos de carácter personal. Sólo tendrán acceso a los recursos a los que estén autorizados en este documento de seguridad, Anexo IV.

6. **Comité de Protección de Datos**: El Responsable del Tratamiento, atendiendo a la complejidad de la gestión de la normativa interna de protección de datos, podrá constituir un comité en el que estén representados los diferentes perfiles mencionados.

7. **Otras personas**, de empresas ajenas que por motivo de su desempeño profesional, puedan potencialmente tener acceso a la información de carácter personal.

Este documento es de obligado cumplimiento para todos ellos.

Aquellas personas, ya sea de la propia organización, o de empresas ajenas, que realice trabajos que no impliquen el tratamiento de los datos personales, como por ejemplo, el personal de limpieza o vigilancia, etc., tendrán limitado el acceso a estos datos, a los soportes que los contengan y a los recursos del sistema de información.

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

# 6. ENCARGADOS DEL TRATAMIENTO

El Encargado del Tratamiento se encuentra recogido en el art. 28 del RGPD y la define como aquella persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos de carácter personal por cuenta del Responsable del Tratamiento o por el Delegado de Protección de Datos, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

El Encargado del Tratamiento garantizará al Responsable del Tratamiento de la aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con los requisitos del Reglamento y garantice los derechos de los interesados.

## 6.1. OBLIGACIONES

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

- Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público
- Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria
- Tomará todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento
- Respetará las condiciones para recurrir a otro Encargado de Tratamiento, según lo establecido en la normativa vigente en Protección de Datos de Carácter Personal
- Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados
- Ayudará al responsable a garantizar el cumplimiento de sus obligaciones, teniendo en cuenta la naturaleza del tratamiento y la información que está a su disposición
- A elección del responsable, suprimir o devolver todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimir las

copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros

- Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente apartado, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable
- Tratará los datos personales puestos a disposición del Encargado de Tratamiento de manera que garantice que el personal a su cargo sigue con las instrucciones del Responsable de Tratamiento
- Garantizará que el Delegado de Protección de Datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales
- Adherirse al Código de Conducta que pueda aprobarse por parte de la Comisión u organismo correspondiente
- Llevará un registro de actividades de tratamiento en caso de tratar datos personales que supongan un riesgo para los derechos y libertades del interesado y/o de manera no ocasional, o que implique el tratamiento de categorías especiales de datos y/o datos relativos a condenas e infracciones

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Responsable del Tratamiento o al Delegado de Protección de Datos.

Las prestaciones de servicios sin acceso a datos personales, (como por ejemplo, servicios de limpieza o vigilancia), también deben quedar reguladas por un contrato, que recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

# 7. NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "**incidencias de seguridad**", entre otras, cualquier incumplimiento de la normativa desarrollada en el presente documento, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos de carácter personal en sus tres vertientes de confidencialidad, integridad y disponibilidad.

Las incidencias se registran en un libro de incidencias que contiene la información detallada en el cuadro anexado al final de este apartado.

Si la incidencia afecta a la integridad de los datos y deben realizarse procedimientos de recuperación de los datos se anota en el libro de incidencias.

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

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

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

Este procedimiento se ha dado a conocer a todo el personal que trata con datos de carácter personal del Responsable del Tratamiento y es el descrito en el ANEXO XIV.

## 7.1. REGISTRO DE INCIDENCIAS

El mantener un registro de las incidencias que comprometan la seguridad de un Fichero es una herramienta imprescindible para aplicar las medidas correctoras necesarias, así como posibilitar la prevención de posibles ataques a esa seguridad y la persecución de los responsables de los mismos.

Cualquier usuario que tenga conocimiento de una incidencia, es responsable del registro de la misma, si el registro de incidencias está automatizado, o de la notificación por escrito al Responsable del Tratamiento, al Delegado de Protección de Datos, o la persona en quien haya delegado formalmente la gestión de las incidencias, si el registro se realiza manualmente.

El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

En el ANEXO XIV, se establece la creación de un registro de incidencias, en el que se hará constar:

- Tipo de incidencia
- Momento en que se ha producido o detectado
- La persona que realiza la notificación
- Persona a la que se comunica
- Los efectos derivados de la incidencia
- Medidas correctoras aplicadas

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros cuyo nivel de seguridad sea medio y alto, identificando en el mismo, la persona que ejecutó el proceso de recuperación de los datos, así como los datos restaurados y, en su caso, los datos que ha sido necesario grabar manualmente en el proceso de recuperación.

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del Responsable del Tratamiento.

# 8. REVISIÓN

## 8.1. REVISIÓN DE LA NORMATIVA INTERNA

Según el Reglamento General de Protección de Datos, la normativa interna deberá mantenerse en todo momento actualizada y deberá ser revisada siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. 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.

Se realizará, al menos una vez al año, la revisión completa del presente documento, así como la validez y adecuación legal de todo su contenido.

## 8.2. AUDITORÍA

Los ficheros identificados en el registro de actividades del ANEXO XIII, deberán someterse, al menos cada dos años, a una auditoría interna o externa, que verifique el cumplimiento de las medidas de seguridad recogidas en esta normativa interna.

Esta auditoría afectará tanto a los ficheros automatizados como a los no automatizados y abarcará tanto los sistemas de información, como las instalaciones de tratamiento y almacenamiento de los datos contenidos en los ficheros.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones tales 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. Esta auditoría reinicia el cómputo **de dos años señalado**.

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

Los informes de auditoría han de ser analizados por el Delegado de Protección de Datos competente, que elevará las conclusiones al Responsable del Tratamiento para que adopte las medidas correctoras y quedará a disposición de la autoridad competente.

# 9. INCUMPLIMIENTO DE LA NORMATIVA INTERNA

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

## 10. CUÁNDO DEBE CONTACTAR CON NOSOTROS

- Cuando se recaben nuevos tipos de datos personales, se vayan a crear nuevos ficheros o cambie algo en los existentes (encargado del tratamiento, domicilio, etc.).

- Cuando tenga cualquier duda o consulta al respecto.

- Cuando algún nuevo trabajador u otra entidad vaya a tener acceso a datos personales de clientes, trabajadores, etc. **Recordar: nunca comunicar o ceder datos personales a ninguna entidad sin antes contactar con nosotros.**

- Cuando reciba alguna petición de acceso, rectificación, cancelación u oposición.

- **Siempre que haya cambios en los sistemas de información o en la organización**.

**Importante: la normativa interna debe estar en todo momentoactualizada, reflejando la situación real de la organización.**

## 11. APROBACIÓN DE LA NORMATIVA INTERNA

La adaptación de una empresa al Reglamento General de Protección de Datos (RGPD) no es simplemente una cuestión administrativa de cumplimentación de formularios, sino un proceso continuo de calidad en el tratamiento de la información y de mejora de la imagen empresarial ante el mercado.

**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**, como Responsable del Tratamiento, aprueba la presente normativa interna, aceptándola en su totalidad y ordenando su inmediato cumplimiento, tanto para el personal propio, como ajeno que tenga o pueda tener acceso a los datos de carácter personal que trata.

En Barcelona, a 1 de diciembre de 2023.

BUFETE ESCURA, S.L.P.

El presente documento se ha realizado en base a la información facilitada por **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**, único responsable de la veracidad de la misma, y BUFETE ESCURA, S.L. se exime de toda responsabilidad.

# ANEXOS

# ANEXO I

## COPIAS DE SEGURIDAD

# COPIAS DE RESPALDO Y RECUPERACIÓN PARA FICHEROS AUTOMATIZADOS

La seguridad de los datos personales supone la confidencialidad, integridad y disponibilidad de los mismos.

Para garantizar estos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y recuperación, de forma, que ante un fallo informático, permitan reconstruir el fichero en el estado que se encontraba antes de la pérdida.

Los procedimientos establecidos para las copias de respaldo y para su recuperación han de garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

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

El Responsable del Tratamiento y el responsable de seguridad verificarán **semestralmente** los procedimientos de copias de respaldo y recuperación de los datos.

**Se recomienda conservar** una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente a aquel en el que se encuentran los equipos informáticos que los tratan **(preferentemente mediante un sistema de "cloud")**, que deberá cumplir en todo caso las medidas de seguridad exigidas, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

## - Periodicidad de la Copia

La copia de seguridad se realiza como mínimo **diariamente**, empleando para realizar la copia varios juegos diferentes de soportes de copias.

El Responsable del Tratamiento y el responsable de seguridad verificarán **semestralmente** los procedimientos de copias de seguridad.

Las pruebas anteriores a la implantación o modificaciones de sistemas de información se realizarán con datos personales previa copia de seguridad**.**

Actualmente se utiliza el siguiente sistema de copias de seguridad:

| Campo | Descripción |
|---|---|
| Tipo de soporte | **CLOUD QUARTUP** |
| Procedimiento de realización de las copias | **Una copia diaria a través del cloud del programa de gestión integral de la empresa Quartup.** |
| Periodicidad de las copias | **Diaria** |
| Lugar donde se conservan las copias | **Las copias de seguridad se conservan en el servidor clud del programa de gestión Quartup.** |
| Observaciones | |

# ANEXO II

## EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, LIMITACIÓN, PORTABILIDAD Y OPOSICIÓN

# DERECHOS DE ACCESO, RECTIFICACIÓN, SUPRESIÓN, LIMITACIÓN, PORTABILIDAD Y OPOSICIÓN

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

| **NOMBRE DE LA EMPRESA** | **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-** |
|---|---|
| DIRECCIÓN SOCIAL | C/ Serrano, 93, 3º E, |
| CP POBLACIÓN | 28006,Madrid |
| TELÉFONO: | 936 37 48 48 |
| FAX: | |
| EMAIL: | info@ausmar.es |

# PROTOCOLOS DE ATENCIÓN DE LOS DERECHOS

Los derechos de los afectados son: **acceso, rectificación, supresión, limitación, portabilidad y oposición** que es preciso atender por la entidad en el adecuado plazo y forma.

Hay que tener especial cuidado y diligencia en la resolución satisfactoria del ejercicio de estos derechos, ya que su omisión puede acarrear cuantiosas sanciones.

El Responsable del Tratamiento deberá informar al personal que tiene acceso a datos de carácter personal del procedimiento a seguir para facilitar a los interesados o afectados el ejercicio de sus derechos.

El Responsable del Tratamiento facilitará respuesta al interesado **en el plazo de un mes** a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

## 1.1. QUIÉN PUEDE SOLICITAR LOS DERECHOS

Los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición son estrictamente personales y serán ejecutados por el afectado.

Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad.

b) Por su representante legal (acreditado), cuando el afectado se encuentre en situación de discapacidad o minoría de edad que el imposibilite el ejercicio personal de estos derechos.

c) Por un representante voluntario, expresamente designado para el ejercicio del derecho. En este caso, deberá constar claramente acreditada la identidad del representado, mediante DNI o documento equivalente, y la representación conferida por aquél.

Los derechos serán denegados cuando la solicitud sea formulada por una persona distinta del afectado y no se acredita que actúa en representación de aquél.

## 1.2. CONDICIONES PARA EL EJERCICIO DE LOS DERECHOS

Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición**.** El ejercicio de los derechos también será gratuito para el interesado.

No se considerarán conformes los supuestos siguientes:

• El envío de cartas certificadas o semejantes.

• La utilización de servicios de telecomunicaciones que impliquen tarificación adicional.

• Cualquier medio que implique un coste excesivo para el interesado.

## 1.3. PROCEDIMIENTO

Deberá dirigirse una comunicación dirigida al Responsable del Tratamiento en laque conste:

• Nombre y apellidos del interesado.

• Fotocopia del DNI/NIF del interesado, y en su caso, de la persona que lo representa así como el documento que acredita tal representación.

• Petición en que se concreta la solicitud.

• Dirección a efectos de notificaciones, fecha y firma del solicitante.

• Documentos acreditativos de la petición que formula, en su caso.

El Responsable del Tratamiento deberá contestar la solicitud que se le dirija en todocaso, teniendo en cuenta que:

• Deberá responder incluso si no figuran los datos personales del afectado en sus ficheros.

• En caso de que la solicitud no reúna los requisitos, solicitar la subsanación de los mismos.

• Deberá guardar prueba del cumplimiento del deber, conservando la acreditación del mismo.

• Deberá adoptar las medidas oportunas para garantizar que el personal que tenga acceso a datos, pueda informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

En el supuesto de no contestar dentro de los plazos establecidos, o hacerlo de forma incompleta, el afectado podrá ponerlo en conocimiento de la Autoridad Competente (Agencia Española de Protección de Datos), pudiendo abrir la misma un expediente sancionador y pudiendo derivarse del mismo una sanción.

## 1.4. LOS DERECHOS ANTE UN ENCARGADO DEL TRATAMIENTO

Cuando los afectados ejerciten sus derechos ante un encargado del tratamiento, el encargado deberá trasladar la solicitud al Responsable del Tratamiento para que proceda a su resolución, salvo que en el contrato de encargo se haya pactado que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio de derechos de los afectados.

## DERECHO DE ACCESO

El derecho de acceso se encuentra recogido en el art. 15 del RGPG y lo define como aquel derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como el origen de dichos datos y las cesiones previstas de los mismos, y concretamente, la siguiente información:

- Los fines del tratamiento;
- Las categorías de datos personales de que se trate;
- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
- De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
- El derecho a presentar una reclamación ante una autoridad de control;
- Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

## DERECHOS DE RECTIFICACIÓN

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. El derecho de rectificación se encuentra recogido en el art.16 del RGPD.

## DERECHO DE SUPRESIÓN "DERECHO AL OLVIDO"

El derecho de supresión o derecho al olvido está recogido en el art.17 del RGPD es la denominación que da el Reglamento al tradicional derecho de cancelación.

El Reglamento lo define como aquel derecho a impedir **la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa**. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima.

Como en este caso, es un ejercicio que se efectúa **directamente** a través de internet, los diferentes buscadores o redes sociales ya proporcionan formularios para ejercitar este derecho.

Los diferentes sitios de internet en donde el interesado puede ejercitar su derecho al olvido son:

- Google
- Yahoo
- Ask
- Bing
- Facebook
- Linkedin
- Instagram

Por último, si bien no hay una mención expresa al bloqueo de datos, se establece en el art. 17 una mención a la posible retención de los datos por parte del Responsable de Tratamiento o excepciones al derecho de supresión. Así se señala que, aunque los datos dejen de ser útiles o necesarios o el interesado retire el consentimiento para el tratamiento, cuando el tratamiento es necesario para:

- El ejercicio de las libertades de expresión e información
- El Cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros.

- Tratamiento para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

## DERECHO DE LIMITACIÓN

El derecho de limitación se encuentra recogido en el art. 18 del RGPD y lo define como aquel derecho de limitar el tratamiento que realiza el Responsable del Tratamiento de los datos del interesado y por tanto que los mismos no sean tratados por el Responsable, siempre y cuando se haya impugnado la exactitud de los mismos por el titular, o el tratamiento sea ilícito, o el responsable no los necesite para los fines en los que fueron recogidos pero el titular del dato o interesado los necesita para la formulación ejercicio o defensa de reclamaciones.

## DERECHO DE PORTABILIDAD

El derecho a la portabilidad de los datos se encuentra recogido en el art. 20 del RGPD.

Es el derecho que tiene el titular o interesado del dato a que sus datos que hayan sido facilitados sean transmitidos a otro responsable del tratamiento en un formato estructurado de uso común y lectura mecánica siempre y cuando el tratamiento esté basado en el consentimiento o sea necesario para la ejecución de un contrato y el mismo se efectúe por medios automatizados.

Como excepción se establece aquellos supuestos en los que el tratamiento se funde en el cumplimiento de una misión de interés público o inherente al ejercicio del poder público.

## DERECHO DE OPOSICIÓN

El derecho de oposición se encuentra recogido en el art. 21 del RGPD.

Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.

Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

A diferencia de la antigua LOPD, **en la que era el interesado quién debía demostrar la situación particular para la oposición, en el RGPD se invierte dicha carga siendo obligación del responsable demostrar que existen motivos suficientes que prevalezcan sobre los derechos y libertades del interesado**. En caso contrario, dejará de tratar los datos personales del interesado.

## DERECHO A INDEMNIZACIÓN

Los interesados que, como consecuencia del incumplimiento del RGPD por parte del Responsable del Tratamiento sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados tal y como establece el artículo 82 del RGPD.

En el caso de ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

# GESTIÓN DE SOLICITUDES DE LOS DERECHOS

| GESTION DE SOLICITUDES | | | |
|---|---|---|---|
| FECHA | | HORA | |
| NOMBRE DEL SOLICITANTE | | | |
| APELLIDOS DEL SOLICITANTE | | | |
| NIF DEL SOLICITANTE | | | |
| DOMICILIO DEL SOLICITANTE | | | |
| PERSONA QUE RECIBE LA NOTIFICACIÓN | | | |
| DERECHO QUE DESEA EJERCER | | ☐ACCESO ☐ RECTIFICACIÓN<br>☐SUPRESIÓN ☐LIMITACIÓN<br>☐PORTABILIDAD ☐OPOSICIÓN | |
| OBSERVACIONES: | | | |
| ☐FOTOCOPIA DEL NIF INCLUIDA | | | |
| ☐OTROS DOCUMENTOS APORTADOS: | | | |
| PERSONA QUE RECIBE LA SOLICITUD | | | |

## EJERCICIO DEL DERECHO DE ACCESO

Petición de información sobre los datos personales incluidos en un fichero.

**DATOS DEL RESPONSABLE DEL TRATAMIENTO**

Nombre:**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**Dirección de la Oficina de Acceso: C/ Serrano, 93, 3º E, C.P 28006, Localidad: Madrid Provincia: Madrid.

**DATOS DEL SOLICITANTE**

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 15 del Reglamento General de Protección de Datos.

**SOLICITA.-**

1.- Que se le facilite gratuitamente el acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Autoridad Competente (Agencia de Protección de Datos) para iniciar el procedimiento de tutela de derechos, en virtud del artículo 77 del Reglamento General de Protección de Datos.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada.

3.- Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultantes de cualquier elaboración, proceso o tratamiento, de conformidad con lo establecido en el artículo 15 del RGPD.

En ..... a.....de.....de 202...

## EJERCICIO DE LOS DERECHOS DE RECTIFICACIÓN

Petición de corrección de datos personales inexactos o incorrectos objeto de tratamientos incluidos en un fichero.

### DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre:**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**Dirección de la Oficina de Acceso: C/ Serrano, 93, 3º E, C.P 28006, Localidad: Madrid Provincia: Madrid.

### DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 15 del Reglamento General de Protección de Datos.

### SOLICITA.-

1.- Que se proceda gratuitamente a la rectificación de sus datos personales en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de rectificación se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Autoridad Competente (Agencia de Protección de Datos) para iniciar el procedimiento de tutela de derechos, en virtud del artículo 77 del Reglamento General de Protección de Datos.

2.- Que si la solicitud del derecho de rectificación fuese estimada, se remita por correo la comunicación correspondiente al solicitante, de conformidad con lo establecido en el artículo 16 del RGPD.

En ..... a.....de.....de 202...

## EJERCICIO DEL DERECHO DE SUPRESIÓN (DERECHO AL OLVIDO)

Petición de supresión de los datos personales objeto de tratamiento incluido en un fichero.

### DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre:**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**Dirección de la Oficina de Acceso: C/ Serrano, 93, 3º E, C.P 28006, Localidad: Madrid Provincia: Madrid.

### DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 15 del Reglamento General de Protección de Datos.

### SOLICITA.-

1.- Que se le facilite gratuitamente la supresión de los datos personales que le conciernen, en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada. En este caso se interpondrá la oportuna reclamación ante la Autoridad Competente (Agencia de Protección de Datos) para iniciar el procedimiento de tutela de derechos, en virtud del artículo 77 del Reglamento General de Protección de Datos.

2.- Que si la solicitud del derecho de supresión fuese estimada, se remita por correo la información a la dirección arriba indicada, de conformidad con lo establecido en el artículo 17 del RGPD.

En ..... a.....de.....de 202...

## EJERCICIO DEL DERECHO DE LIMITACIÓN

Petición de limitación de los datos personales incluidos en un fichero.

**DATOS DEL RESPONSABLE DEL TRATAMIENTO**

Nombre:**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**Dirección de la Oficina de Acceso: C/ Serrano, 93, 3º E, C.P 28006, Localidad: Madrid Provincia: «Provincia»

**DATOS DEL SOLICITANTE**

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de portabilidad, de conformidad con el artículo 18 del Reglamento General de Protección de Datos.

**SOLICITA.-**

1.- Que se proceda a la limitación del tratamiento de mis datos por parte del Responsable del Tratamiento, debido a la concurrencia de un tratamiento ilícito o a la innecesaria conservación de los mismos debido a la finalidad por la que se recogieron. Si no se atiende a ésta petición el solicitante podrá interponer la oportuna reclamación ante la Autoridad Competente (Agencia de Protección de Datos) para iniciar el procedimiento de tutela de derechos, en virtud del artículo 77 del Reglamento General de Protección de Datos.

2. Que, en el caso de que el Responsable del Tratamiento considere que dicha limitación no proceda, lo comunique igualmente, de forma motivada, a fin de poder interponer la reclamación prevista en el artículo 77 del Reglamento General de Protección de Datos.

En ..... a.....de.....de 202...

## EJERCICIO DEL DERECHO DE PORTABILIDAD

Petición de portabilidad de los datos personales incluidos en un fichero.

**DATOS DEL RESPONSABLE DEL TRATAMIENTO**

Nombre:**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**Dirección de la Oficina de Acceso: C/ Serrano, 93, 3º E, C.P 28006, Localidad: Madrid Provincia: Madrid.

**DATOS DEL SOLICITANTE**

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia ..... C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de portabilidad, de conformidad con el artículo 20 del Reglamento General de Protección de Datos.

**DATOS DEL FUTURO RESPONSABLE DEL TRATAMIENTO (si procede)**

Nombre:**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**Dirección de la Oficina de Acceso: C/ Serrano, 93, 3º E, C.P 28006, Localidad: Madrid Provincia: «Provincia»

**SOLICITA.-**

1.- Que se le facilite gratuitamente la portabilidad de los datos contenidos en los ficheros automatizados (*a otro Responsable del Tratamiento / al solicitante de éste formulario)*. Si no se atiende a ésta petición el solicitante podrá interponer la oportuna reclamación ante la Autoridad Competente (Agencia de Protección de Datos) para iniciar el procedimiento de tutela de derechos, en virtud del artículo 77 del Reglamento General de Protección de Datos.

2.- Que si la solicitud del derecho de portabilidad fuese estimada, se remita por correo la información (*a la dirección arriba indicada / a la dirección del futuro Responsable del Tratamiento que también se indica en el presente formulario).*

En ..... a.....de.....de 202...

## EJERCICIO DEL DERECHO DE OPOSICIÓN

Petición de oposición al tratamiento de los datos personales incluidos en un fichero.

### DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre:**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**Dirección de la Oficina de Acceso: C/ Serrano, 93, 3º E, C.P 28006,Localidad:Madrid Provincia:«Provincia»

### DATOS DEL SOLICITANTE

D./ Dª ....., mayor de edad, con domicilio en la C/..... nº....., Localidad ..... Provincia .....C.P. ..... con D.N.I....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 21 del Reglamento General de Protección de Datos.

### SOLICITA.-

1. Que en el plazo de un mes desde la recepción de esta solicitud, se proceda a la efectiva cancelación de cualesquiera de los datos relativos a mi persona que se encuentren en sus ficheros, en los términos previstos en Reglamento General de Protección de Datos y me lo comuniquen de forma escrita a la dirección arriba indicada.

2. Que, en el caso de que el Responsable del Tratamiento considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada, a fin de poder interponer la reclamación prevista en el artículo 77 del Reglamento General de Protección de Datos.

En..... a..... de..... de 202...

# ANEXO III

## NOMBRAMIENTOS

# RESPONSABLES PARA AUTORIZAR

La seguridad del tratamiento que hace referencia el artículo 32.4 del Reglamento General de Protección de Datos establece se tomarán las medidas pertinentes para garantizar que cualquier persona que actúe bajo la autoridad del Responsable o del Encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del Responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Tratamiento.

Las autorizaciones recogidas en dicho Título son las siguientes:

- Autorización para conceder, alterar o anular el acceso a los datos y recursos.
- Autorización para acceder al lugar donde se almacenan los soportes y/o documentos.
- Autorización para salida de soportes y/o documentos (incluidos los adjuntos a un correo electrónico, por ftp o similar).
- Autorización para tratar datos fuera de los locales.
- Autorización para tratar datos en dispositivos portátiles fuera de los locales del responsable.
- Autorización para la recuperación de datos en los ficheros del registro de actividades.
- Autorización para entrega y recepción de soportes y/o documentos en los ficheros del registro de actividades.
- Autorización para el acceso a los lugares donde se hallen instalados los equipos físicos que dan soporte a los sistemas de información de los ficheros del registro de actividades.
- Autorización para la copia o reproducción de documentos que contengan datos especialmente protegidos.

La persona designada para otorgar las autorizaciones previstas es el Responsable del Tratamiento.

# RESPONSABLE DE SEGURIDAD

La persona designada como responsable de seguridad, y encargada de coordinar y controlar las medidas de seguridad recogidas en la normativa de protección de datos y los ficheros de los que son responsables es:

| **Concepto** | **Descripción** |
|---|---|
| Datos de la persona | **Juan Fargas Duarry** |
| Cargo que ocupa | **Representante Legal** |
| Fecha de alta | **26.04.2018** |
| Observaciones | |

# ANEXO IV

## AUTORIZACIONES

# AUTORIZACIÓN PARA ACCEDER A LOS LUGARES DONDE SE ALMACENAN SOPORTES CON DATOS DE CARÁCTER PERSONAL

En cumplimiento del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), se AUTORIZA expresamente en este documento el acceso al lugar donde se almacenan los soportes con datos de carácter personal responsabilidad de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-.**

La descripción detallada de estos dispositivos, así como las características que obstaculizan su apertura y la protección con que cuenta el acceso a los mismos, se encuentran detalladas en el ANEXO IV.

La presente autorización comenzará a regir en la fecha indicada para cada uno de los usuarios y permanecerá vigente mientras subsista la relación laboral, contractual o mercantil.

De la misma forma, la validez de la autorización finalizará en caso de que se acuerde derogación expresa de la misma o finalice la relación que la motivó.

# AUTORIZACIÓN PARA EL ACCESO A LOS LUGARES DONDE ESTÁN INSTALADOS LOS EQUIPOS FÍSICOS QUE DAN SOPORTE A LOS SISTEMAS DE INFORMACIÓN

En cumplimiento del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos),se AUTORIZA expresamente en este documento el acceso a los lugares donde se hallan instalados los equipos físicos que dan soporte a los sistemas de información.

La presente autorización comenzará a regir en la fecha indicada para cada uno de los usuarios y permanecerá vigente mientras subsista la relación laboral, contractual o mercantil.

De la misma forma, la validez de la autorización finalizará en caso de que se acuerde derogación expresa de la misma o finalice la relación que la motivó.

# AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES FUERA DE LOS LOCALES DEL RESPONSABLE DEL TRATAMIENTO

En cumplimiento del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos),se AUTORIZA expresamente el tratamiento de datos de carácter personal, responsabilidad de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**fuera de los local es donde se encuentran ubicados los ficheros, a los usuarios autorizados para ello y a los ficheros necesarios:

Los usuarios o perfiles de usuarios se han comprometido, a través del correspondiente Compromiso de confidencialidad y secreto a garantizar las medidas de seguridad correspondiente al fichero tratado.

La presente autorización comenzará a regir en la fecha indicada para cada uno de los usuarios y permanecerá vigente mientras subsista la relación laboral, contractual o mercantil.

De la misma forma, la validez de la autorización finalizará en caso de que se acuerde derogación expresa de la misma o finalice la relación que la motivó.

# AUTORIZACIÓN PARA EL ALMACENAMIENTO Y TRATAMIENTO DE DATOS PERSONALES EN DISPOSITIVOS PORTÁTILES FUERA DE LOS LOCALES DEL RESPONSABLE DEL TRATAMIENTO

En cumplimiento del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos),se AUTORIZA expresamente en este documento el almacenamiento y tratamiento de datos de carácter personal en equipos portátiles fuera de los locales del responsable del tratamiento.

Si los datos almacenados en el dispositivo portátil son de nivel alto, deberán ircifrados.

Los usuarios o perfiles de usuarios se han comprometido, a través del correspondiente Compromiso de confidencialidad y secreto a garantizar las medidas de seguridad correspondiente al fichero tratado.

La presente autorización comenzará a regir en la fecha indicada para cada uno de los usuarios y permanecerá vigente mientras subsista la relación laboral, contractual o mercantil.

De la misma forma, la validez de la autorización finalizará en caso de que se acuerde derogación expresa de la misma o finalice la relación que la motivó.

# AUTORIZACIÓN PARA LA ENTREGA DE SOPORTES Y/O DOCUMENTOS

En cumplimiento del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos),se AUTORIZA expresamente en este documento la entrega de soportes y documentos que contengan datos personales.

La presente autorización comenzará a regir en la fecha indicada para cada uno de los usuarios y permanecerá vigente mientras subsista la relación laboral, contractual o mercantil.

De la misma forma, la validez de la autorización finalizará en caso de que se acuerde derogación expresa de la misma o finalice la relación que la motivó.

# AUTORIZACIÓN PARA LA RECEPCIÓN DE SOPORTES Y/O DOCUMENTOS

En cumplimiento del Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos),se AUTORIZA expresamente en este documento la recepción de soportes y documentos que contengan datos personales.

La presente autorización comenzará a regir en la fecha indicada para cada uno de los usuarios y permanecerá vigente mientras subsista la relación laboral, contractual o mercantil.

De la misma forma, la validez de la autorización finalizará en caso de que se acuerde derogación expresa de la misma o finalice la relación que la motivó.

# ANEXO V

## OBLIGACIONES Y FUNCIONES DEL PERSONAL EN MATERIA DE PROTECCIÓN DE DATOS

# FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El Responsable del Tratamiento es la persona física o jurídica que decide sobre la finalidad, uso y contenido del fichero. Deberá:

- Elaborar la normativa interna de protección de datos.
- Implantar y hacer cumplir las medidas de seguridad técnicas y organizativas establecidas en este documento.
- Garantizar la difusión de esta normativa interna de protección de datos o los anexos que les afecten, entre todo el personal que trate con datos del fichero.
- Mantener actualizada la normativa interna de protección de datos siempre que se produzcan cambios relevantes en:
    - El sistema de información.
    - Es sistema de tratamiento.
    - La organización.
    - El contenido de la información incluida en los ficheros o en el registro de actividad.
    - Como consecuencia de los controles periódicos realizados.

Se considera que un cambio es relevante cuando pueda afectar al cumplimiento de las medidas de seguridad implantadas.

- Velará para que se cumplan las medidas de seguridad implantadas.
- Nombrará uno o varios Responsables delegados.
- Verificará, al menos semestralmente el correcto funcionamiento del sistema de copias de respaldo.
- Velará por la no concurrencia de brechas de seguridad y tomará las medidas correctivas por si se produjeran.
- Analizará las incidencias registradas e implantará las medidas correctivas necesarias para evitar ese tipo de incidencias en el futuro.

# FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

El responsable de seguridad es la persona designada por el Responsable del Tratamiento encargada de coordinar y controlar las medidas definidas la normativa interna de protección de datos.

Para ello, deberá:

- Coordinar la puesta en marcha de las medidas de seguridad, colaborar con el Responsable del Tratamiento en la difusión del documento de seguridad y cooperar con el controlando el cumplimiento de las mismas.

- Velará por la no concurrencia de brechas de seguridad y tomará las medidas correctivas por si se produjeran en colaboración con el Responsable del Tratamiento.

- Analizar las incidencias registradas, tomando las medidas oportunas en colaboración con el Responsable del Tratamiento.

- Comprobará, al menos, de forma semestral, la existencia de copias de respaldo que permitan la recuperación del Fichero, realizando una prueba de restaurado que verifique la correcta definición de los procedimiento y proceso de recuperación, y enviando evidencias de esta comprobación al Responsable del Tratamiento.

- A su vez, también con periodicidad al menos semestral, los administradores del Fichero comunicarán el Responsable del Tratamiento cualquier cambio que se haya realizado en los sistemas de información, como cambios en el hardware o software, bases de datos, aplicaciones de acceso al fichero, etc., procediendo a la actualización de dichos anexos.

- Tendrá el control directo de los mecanismos que permiten el registro de accesos, sin que se deba permitir, en ningún caso, la desactivación de los mismos.

- Al menos cada dos años se realizará una auditoría en los términos que se recogen en el apartado 8.2 de este documento de seguridad.

- Los resultados de los controles periódicos, así como de las auditorías, serán adjuntados a la normativa interna de protección de datos.

# FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

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

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

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

## 1. OBLIGACIONES GENERALES

- Guardar secreto y confidencialidad de la información tratada. Quienes intervienen en cualquier fase del tratamiento de los datos de carácter personal, está obligado al secreto profesional respecto a los datos y al deber de guardarlos, obligaciones que continúan incluso después de finalizar las relaciones con el Responsable del Tratamiento.

- La vulneración del deber de secreto respecto a los datos personales tratados, será considerado una falta leve, grave o muy grave, conforme a lo previsto en el artículo 83 del RGPD, lo cual dará lugar al inicio de acciones disciplinarias, si proceden.

- Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.

- Los sistemas de información, recursos, y la información personal a la que se accede, sólo se debe utilizar para las labores estrictamente profesionales que el usuario tiene asignadas.

- Facilitar los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición a los titulares de los datos. Para ello se informará al Responsable del Tratamiento, Responsable de Seguridad o Encargado del tratamiento y se recogerá siempre en solicitud escrita.

## 2. PUESTOS DE TRABAJO

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

El usuario deberá cambiar la contraseña inicial asignada en el primer acceso que realice al sistema, o tras el desbloqueo de su contraseña cuando haya sido necesaria la

intervención de una tercera persona para realizar el proceso. Las contraseñas deberán ser lo suficientemente complejas para no ser adivinadas de forma sencilla por un tercero.

Para ello, se deberán seguir las siguientes normas para elegir la contraseña:

- Deberán tener una longitud mínima **de entre 4 y 6 caracteres alfanuméricos**.
- No deberán coincidir, ni siquiera en parte, con el código de usuario.
- El usuario deberá aplicar las reglas nemotécnicas para poder construir una contraseña lo suficientemente compleja como para que no pueda ser adivinada por terceros y a la vez sean muy fáciles de recordar por él.

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

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

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

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

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

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

    - Realizar siempre las copias sobre un mismo directorio de nombre TEMP os imilar, de forma que no queden dispersas por el disco duro, y siempre sea posible conocer donde están los datos temporales.
    - Tras realizar el tratamiento que ha requerido estos datos temporales, proceder as u inmediata eliminación.
    - Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda en función de los datos que contienen.

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

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

## 3. GESTIÓN DE SOPORTES

Se entiende por soporte todo objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Ejemplos de soportes: cd-rom, dvd-rom,blu-ray, memoria usb, disco duro,smartphone etc. Los Usuarios deben observar las siguientes medidas de seguridad en relación con los soportes que contengan datos de carácter personal:

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

- Cuando un usuario gestione o produzca soportes que contengan datos de carácter personal, estos deberán estar claramente identificados con unas etiquetas externas e inventariadas.

- Los soportes que contengan datos de carácter personal, deberán ser almacenados en lugares a los que no tenga acceso el personal no autorizado.

- La salida de soportes que contengan datos de carácter personal de las instalaciones bajo control del Responsable del Tratamiento, deberá ser autorizada por el mismo o estar debidamente autorizada en el Documento de Seguridad.

- La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o añejos a un correo electrónico, fuera de los locales bajo el control del responsable fichero o tratamiento, deberá ser autorizada por el Responsable del Tratamiento (o aquel en que se hubiera delegado), o encontrarse debidamente autorizada en el Documento de Seguridad.

- El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.

- Cuando deban ser enviados datos personales fuera de las ubicaciones del Responsable del Tratamiento, ya sea mediante soporte físico de grabación de datos o bien a través de correo electrónico o FTP, deberán ir cifrados o utilizar cualquier otro mecanismo que asegure que la información no es accesible ni manipulada durante su transporte.

## 3.1. DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento.

- Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

- Aquellos CDs, cintas, discos removibles, que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

- Todos los soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al Responsable del Tratamiento.

- Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al Responsable del Tratamiento para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

# 4. FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

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

# 5. DOCUMENTACIÓN EN PAPEL

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

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

- El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.

- En todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

## 5.1. DESTRUCCIÓN DE DOCUMENTACIÓN

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.

- Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.

- En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.

- El Responsable del Tratamiento deberá exigir a la empresa encargada de la destrucción de los datos un contrato y un certificado en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

- El Responsable del Tratamiento podrá establecer un registro de destrucción de documentación con el fin de controlar que documentación se va a proceder a su destrucción.

## REGISTRO DE DESTRUCCIÓN

| REGISTRO DESTRUCCION DOCUMENTOS | Nº registro |
|---|---|
| **Departamento titular de la documentación**<br>**Datos de la documentación**<br>Referencia documental<br>Contenido documental | |
| **Datos de la destrucción**<br>Referencia documental<br>Fecha de destrucción<br>Certificado de destrucción | |
| En , a _____de _____ de<br><br>Firma responsable Departamento titular documentación  Firma responsable de destrucción | |

# 6. GESTIÓN DE INCIDENCIAS

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

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

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

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

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

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

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

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

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

# APÉNDICE I

| GESTION DE INCIDENCIAS | | | |
|---|---|---|---|
| FECHA | | HORA | |
| TIPO DE INCIDENCIA | | | |
| DESCRIPCIÓN: | | | |
| EFECTOS DERIVADOS: | | | |
| PERSONA QUE COMUNICA LA INCIDENCIA | | | |
| PERSONA QUE RECIBE LA NOTIFICACIÓN | | | |
| **ACUSE DE RECIBO** | | | |
| FECHA | | HORA | |
| FIRMA: | | | |

# APÉNDICE II

| GESTIÓN DE SOLICITUDES DE DERECHOS DE LOS INTERESADOS | | | |
|---|---|---|---|
| FECHA | | HORA | |
| NOMBRE DEL SOLICITANTE | | | |
| APELLIDOS DEL SOLICITANTE | | | |
| NIF DEL SOLICITANTE | | | |
| DOMICILIO DEL SOLICITANTE | | | |
| PERSONA QUE RECIBE LA NOTIFICACIÓN | | | |
| DERECHO QUE DESEA EJERCER | | ☐ACCESO ☐ RECTIFICACIÓN<br>☐SUPRESIÓN ☐LIMITACIÓN<br>☐PORTABILIDAD ☐OPOSICIÓN | |
| OBSERVACIONES: | | | |
| ☐FOTOCOPIA DEL NIF INCLUIDA | | | |
| ☐OTROS DOCUMENTOS APORTADOS: | | | |
| PERSONA QUE RECIBE LA SOLICITUD | | | |

# ANEXO VI

## CLAUSULAS Y CIRCULARES

# CLÁUSULAS PROTECCIÓN DE DATOS PARA FORMULARIOS DE RECOGIDA DE DATOS

**NOTA:** Los avisos legales que se proponen a continuación están redactados pensando en su inclusión en formularios donde se recaben datos de carácter personal. Sería necesaria la inclusión del presente aviso legal en todos aquellos formularios en los que la empresa obtiene los datos de carácter personal.

## CASTELLANO

*"En cumplimiento al Reglamento General de Protección de Datos 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, le informamos que los datos personales que se solicitan en el presente formulario se incluirán en una base de datos informatizada titularidad de* ***AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-.*** *El titular de los datos dispone de los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición que podrá ejercitar mediante correo postal a la dirección de la empresa en* ***C/ Serrano, 93, 3º E, 28006,Madrid.*** *Le informamos que los datos obtenidos a través del presente formulario, responden a la finalidad, única y exclusiva de poder facilitar a los clientes los servicios solicitados. Para más información sobre nuestra empresa, puede consultar el Aviso Legal de nuestra web www.ausmar.com".*

## CATALÀ

*"En compliment al Reglament General de Protecció de Dades 2016/679 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals a la lliure circulació d'aquestes dades, l'informem que les dades personals que se sol·liciten en el present formulari s'inclouran en una base de dades informatitzada titularitat de* ***AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-****. El titular de les dades disposa dels drets d'accés, rectificació, supressió,limitació, portabilitat i oposició, que podrà exercitar mitjançant correu postal a l'adreça de l'empresa en* ***C/ Serrano, 93, 3º E, 28006,Madrid.*** *L'informem que les dades obtingudes a través del present formulari, responen a la finalitat, única i exclusiva de poder facilitar als clients els serveis sol·licitats. Per mes informació vosté pot consultar el nostre Avis Legal de la nostra pàgina web www.ausmar.com".*

# CLÁUSULAS PIE DE PAGINA E-MAILS TEMA CONFIDENCIALIDAD

**AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**
**C/ Serrano, 93, 3º E,**
**28006,,Madrid,**
**info@ausmar.es**

ADVERTÈNCIA DE CONFIDENCIALITAT: Aquest missatge i els documents que, en el seu cas, porti annexats, va dirigit exclusivament al seu(s) destinatari(s) i pot contenir informació privilegiada i confidencial. L'accés a aquesta informació per altres persones diferents a les designades no està autoritzat. Si vostè no es el destinatari indicat, queda notificat que l'ús, divulgació i/o còpia sense autorització està prohibida en virtut de la legislació vigent. Si ha rebut aquest missatge per error, per favor li preguem que ho comuniqui immediatament al remitent via fax o e-mail i procedeixi a la seva destrucció.

ADVERTENCIA DE CONFIDENCIALIDAD: Este mensaje y los documentos que, en su caso, lleve anexos, se dirige exclusivamente a su(s) destinatario(s) y puede contener información privilegiada o confidencial. El acceso a esta información por otras personas distintas a las designadas no está autorizado. Si usted no es el destinatario indicado, queda notificado que la utilización, divulgación y/o copia sin autorización está prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, por favor le rogamos que lo comunique inmediatamente al remitente vía fax o e-mail y proceda a su destrucción.

# CLAUSULA INFORMATIVA:
# INCORPORACIÓN DE LOS CURRÍCULOS VITAE A LAS BASES DE DATOS

De conformidad con el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos), le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de ***AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR*-(en adelante el Responsable del Tratamiento)** ***C/ Serrano, 93, 3º E, , 28006,,Madrid,*** con ***CIF*A-28709319**, con la finalidad de formar parte en los procesos de selección de personal que se lleven a cabo por nuestra parte.. En cumplimiento con la normativa vigente, Responsable del Tratamiento informa que los datos serán conservados durante el siguiente periodo: LEGALMENTE ESTABLECIDO.

A su vez, le informamos que puede contactar con el Responsable de Protección de Datos del Responsable del Tratamiento dirigiéndose por escrito a la dirección de correo **info@ausmar.es**

El Responsable del Tratamiento le solicita su consentimiento para el tratamiento de sus datos para analizar su perfil con la finalidad de evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

El Responsable del Tratamiento le informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada. Es por ello que el Responsable del Tratamiento se compromete a adoptar todas las medidas razonables para que estos se supriman o rectifiquen sin dilación cuando sean inexactos.

De acuerdo con los derechos que le confiere la normativa vigente en protección de Datos de Carácter Personal podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad y oposición, dirigiendo su petición a la dirección postal indicada más arriba o bien a través de correo electrónico **info@ausmar.es**En este sentido, el trabajador dispondrá del derecho a revocar el consentimiento prestado mediante la presente cláusula.

Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

En último lugar, Responsable del Tratamiento informa que con la firma del presente documento otorga el consentimiento explícito para el tratamiento de los datos mencionados anteriormente.

Nombre y apellidos
DNI:
Firma:

# CLÁUSULAS INFORMATIVAS:
# CONTRATOS LABORALES

De conformidad con el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos), le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de ***AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR*-(en adelante el Responsable del Tratamiento)*C/ Serrano, 93, 3º E, , 28006,,Madrid,*** con ***CIF*A-28709319**, con la finalidad de atender los compromisos derivados del contrato suscrito entre ambas partes. En cumplimiento con la normativa vigente, El Responsable del Tratamiento informa que los datos serán conservados durante 4 años en cumplimiento con el art. 21 de la Ley sobre Infracciones y Sanciones en el Orden Social.

Con la presente cláusula queda informado de que sus datos serán comunicados en caso de ser necesario a: Administraciones Públicas y a todas aquellas entidades con las que sea necesaria la comunicación con la finalidad de cumplir con la prestación del servicio anteriormente mencionado.

El hecho de no facilitar los datos a las entidades mencionadas implica que no se pueda cumplir con la prestación de los servicios objeto del presente contrato.

A su vez, le informamos que puede contactar con el Responsable de Protección de Datos del Responsable del Tratamiento dirigiéndose por escrito a la dirección de correo **info@ausmar.es**

El Responsable del Tratamiento le informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada. Es por ello que el Responsable del Tratamiento se compromete a adoptar todas las medidas razonables para que estos se supriman o rectifiquen sin dilación cuando sean inexactos.

De acuerdo con los derechos que le confiere la normativa vigente en protección de Datos de Carácter Personal podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad y oposición, dirigiendo su petición a la dirección postal indicada más arriba o bien a través de correo electrónico **info@ausmar.es**En este sentido, el trabajador dispondrá del derecho a revocar el consentimiento prestado mediante la presente cláusula.

Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

En último lugar, Responsable del Tratamiento informa que con la firma del presente documento otorga el consentimiento explícito para el tratamiento de los datos mencionados anteriormente.

Nombre y apellidos
DNI:
Firma:

# CLAUSULA INFORMATIVA:
# OBLIGACIÓN DE CONFIDENCIALIDAD Y DEBER DE GUARDAR SECRETO POR PARTE DEL PERSONAL

De conformidad con el Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), HAGO CONSTAR que doy **mi consentimiento expreso y explícito** a que mis datos sean incluidos en un fichero o en el registro de actividad propiedad de la empresa destinado al tratamiento de datos de carácter personal para la gestión de los Recursos Humanos, en su sentido más amplio, con la posibilidad de que los mismos sean cedidos en outsourcing a_____ , con la misma finalidad, pudiendo, en todo caso, ejercitar los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición a los datos facilitados, mediante contrato laboral.

Conforme al Reglamento (UE) 2016/679, el Responsable del Tratamiento y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al **secreto profesional de los mismos y al deber de guardarlos**, obligaciones que subsistirán aún después de finalizadas sus relaciones con el titular del fichero o, en su caso, con el Responsable del Tratamiento.

La infracción de este deber viene sancionada administrativamente conforme al Reglamento (UE) 2016/679, que configura las vulneraciones de esta obligación de guardar secreto respecto a los datos de carácter personal con multas administrativas.

Además, el incumplimiento del deber de secreto respecto a los datos de carácter personal puede dar lugar a la responsabilidad penal tipificada en el título X del Libro II del vigente Código Penal, artículos 197 y 199.

El que suscribe, cuyos datos personales y ocupación profesional en esta entidad se consignan a continuación, declara expresa y formalmente conocer:

**a)** La obligación de guardar secreto, no desvelar ni facilitar a terceros información a la que tenga acceso en el ejercicio de sus funciones (sobre proveedores, clientes, “know-how”, procedimientos comerciales e industriales y demás información sujeta a secreto profesional) y en especial en lo relativo a datos de carácter personal entendidos según lo que establece la normativa vigente (Reglamento (UE) 2016/679).

**b)** Las consecuencias sancionadoras de orden administrativo y penal que puede acarrear su incumplimiento, así como las eventuales indemnizaciones por responsabilidad de daños y perjuicios que la infracción puede llevar aparejadas.

c) **Y a estos efectos, declara expresa y formalmente su compromiso de cumplir con este deber de guardar secreto, aceptando y asumiendo, en otro caso, su responsabilidad personal frente al titular de los datos personales para resarcirle personalmente de los daños y perjuicios que se le pudieran irrogar al titular como consecuencia de su incumplimiento culpable, aceptando asimismo las consecuencias sancionadoras de orden laboral o profesional que se arbitren al efecto por los procedimientos legalmente procedentes.**

Nombre y Apellidos:

**Cargo, función, puesto de trabajo o equivalente:**

En ....., a .....
Firmado:

(Con la firma de este documento se reconoce haber recibido o recibir en este acto copia de las obligaciones y funciones de todo el personal establecidas en la normativa interna de protección de datos de la empresa o entidad para la protección de los datos de carácter personal).

# CIRCULAR INFORMATIVA:
# PARA CLIENTES

De conformidad con el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos), le informamos que sus datos serán incorporados al sistema de tratamiento titularidad de ***AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR*-(en adelante el Responsable del Tratamiento)*C/ Serrano, 93, 3º E, , 28006,,Madrid,*** con ***CIF*** **A-28709319**, con la finalidad de una relación comercial. En cumplimiento con la normativa vigente, El Responsable del Tratamiento informa que los datos serán conservados mientras dure la relación comercial a excepción de poder conservarlos más tiempo para ejercer acciones legales.

Con la presente cláusula queda informado de que sus datos serán comunicados en caso de ser necesario a: Administraciones Públicas y a todas aquellas entidades con las que sea necesaria la comunicación con la finalidad de cumplir con la prestación del servicio anteriormente mencionado.

El hecho de no facilitar los datos a las entidades mencionadas implica que no se pueda cumplir con la prestación de los servicios objeto del presente contrato.

A su vez, le informamos que puede contactar con el Responsable de Protección de Datos del Responsable del Tratamiento dirigiéndose por escrito a la dirección de correo **info@ausmar.es**

El Responsable del Tratamiento le informa que procederá a tratar los datos de manera lícita, leal, transparente, adecuada, pertinente, limitada, exacta y actualizada. Es por ello que el Responsable del Tratamiento se compromete a adoptar todas las medidas razonables para que estos se supriman o rectifiquen sin dilación cuando sean inexactos.

De acuerdo con los derechos que le confiere la normativa vigente en protección de Datos de Carácter Personal podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad y oposición, dirigiendo su petición a la dirección postal indicada más arriba o bien a través de correo electrónico **info@ausmar.es**En este sentido, el trabajador dispondrá del derecho a revocar el consentimiento prestado mediante la presente cláusula.

Podrá dirigirse a la Autoridad de Control competente para presentar la reclamación que considere oportuna.

En último lugar, Responsable del Tratamiento informa que con la firma del presente documento otorga el consentimiento explícito para el tratamiento de los datos mencionados anteriormente.

Nombre y apellidos:
DNI:
Firma:

# COMUNICADO AL AFECTADO PARA INFORMARLE Y RECABAR SU CONSENTIMIENTO PARA LA CESIÓN DE SUS DATOS DE CARÁCTER PERSONAL

1º.- Mediante el presente comunicado se le informa y se le solicita el consentimiento para ceder sus datos de carácter personal a un tercero.

2º.- Los datos identificativos del Responsable del Tratamiento cedente son:

| |
|---|
| Denominación:<br>.....<br>Actividad:<br>.....<br>Dirección:<br>.....<br>Teléfono:<br>..... |

3º.- Los datos de carácter personal del afectado que obran en poder del Responsable del Tratamiento y cuya comunicación a un tercero se pretende autorizar son:

| |
|---|
| |

4º.- Las circunstancias en las que el Responsable del Tratamiento obtuvo sus datos que se pretende comunicar son:

| |
|---|
| |

*(Habrá que hacer mención de la información o el consentimiento prestados con ocasión de la recogida de los mismos).*

5º.- La finalidad a la que se destinarán los datos cuya comunicación se pretende autorizar es:

| |
|---|
| |

6º.- El tercero o cesionario queda sujeto, por el sólo hecho de la comunicación de sus datos de carácter personal, al Reglamento (UE) 2016/679.

☐Si, doy mi consentimiento expreso para ceder mis datos personales a un tercero.

☐No, no doy mi consentimiento expreso para ceder mis datos personales a un tercero

# NORMATIVA INTERNA DE USO: TELEFONÍA E INFORMÁTICA

## USO DE LA TELEFONÍA PROPIEDAD AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-

- Tanto la telefonía fija como la móvil son para uso exclusivo de los miembros de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**y corresponde a estos el buen uso de la misma.
- Se entiende que su uso se limita exclusivamente a temas relacionados con la empresa, recordando a los usuarios de móviles de empresa que se les podrá descontar de sus honorarios el importe correspondiente a aquellas llamadas que hayan realizado con usos particulares.
- Se recuerda también que los usuarios que dispongan de móvil de empresa (y no se encuentren en otra sede con teléfono fijo) y quieran llamar a los despachos desde el exterior, lo deberán hacer a las líneas móviles de centralita, no a las fijas.
- Desde los centros de trabajo donde haya línea de teléfono fijo se llamará a fijos y se evitará en lo posible llamar a móviles.

## USO DE LOS ELEMENTOS INFORMÁTICOS PROPIEDAD DEAUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-

- **Los recursos informáticos** de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR- ,** tanto los del servicio de informática como los del resto de sus instalaciones: sistemas centrales (servidor), estaciones de trabajo, ordenadores personales, redes internas y externas, cuentas de correo, conexión a Internet, etc., **son para uso exclusivo de los miembros de la empresa** o personas autorizadas. Asimismo son para **uso únicamente de temas relacionados con la empresa.** Se informa expresamente al empleado, que **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-,** por si misma o mediante terceros autorizados, puede acceder en cualquier momento a los recursos informáticos de la empresa proporcionados al empleado, obtener copias de su contenido, modificarlo, borrarlo, etc.
- Los sistemas informáticos de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**están conectados directa o indirectamente a la red. De ahí que **el mal uso o la falta de adecuados sistemas de seguridad en alguno de estos equipos pueda comprometer la seguridad** del resto de ellos.
- En consecuencia, esta normativa es de aplicación a toda persona que haga uso de los sistemas y/o recursos informáticos de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**o que disponga de sistemas o redes conectadas directa o indirectamente a la red general, como es el caso de las smartphones y agendas diversas.
- **Las cuentas de correo** son recursos proporcionados por **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**al empleado para facilitar las

labores administrativas a realizar, siendo su uso exclusivo para tal fin. Quedan por tanto excluidos los usos particulares de las mismas, tanto para mandar como para recibir mensajes. **No podrá utilizarse la cuenta de correo para fines o actividades ajenas a la empresa.** Se informa expresamente al empleado, que **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-**por si misma o mediante terceros autorizados, puede acceder en cualquier momento a las cuentas de correo electrónico de la empresa proporcionadas al empleado, obtener copias de correos, reenviar correos, borrar correos, etc.

- Los recursos proporcionados son **multiusuario** (o pudieran serlo en caso de ser necesario) y **abiertos**. Si alguno de ellos no lo fuera se informaría al resto de los componentes de la red de dicha exclusividad. (Por ejemplo la información referente al departamento de personal o similares).
- El responsable de informática es la persona encargada de velar por la gestión y el buen funcionamiento de los equipos. Cualquier sugerencia, incidencia o mal funcionamiento de los mismos **deberá serle informado**. Asimismo **cada usuario final será el responsable directo del buen o mal uso al que dedique su equipo y el único responsable de los usos que se deriven del mismo.**
- El Departamento de informática revisará periódicamente los equipos y podrá modificar el sistema para solventar cuantas irregularidades se encuentren en el equipo de los usuarios sin previo aviso.
- Los usuarios tendrán un gran cuidado a la hora de manipular y usar los equipos informáticos propiedad de la empresa y toda la infraestructura complementaria. Evitarán realizar cualquier acción, que de forma voluntaria o no, pudiera perjudicar la integridad física de la instalación.
- **No está permitida la instalación/desinstalación de ningún tipo de software sin la aprobación del Responsable de Informática**. En caso de ser necesario se hará demanda por escrito del mismo al responsable informático, especificando nombre del producto, fabricante y versión solicitada.
- No se podrán realizar **cambios de configuración**, cambios administrativos, importación/exportación de cuentas de correo de la empresa o particulares.
- Las **copias de seguridad** de la información contenida en los ordenadores personales se realiza periódicamente, si se trabaja desde la sede principal. Esta información debe estar **ordenada en carpetas** y siempre **dentro de la carpeta "Mis Documentos"** de la cuenta de usuario de Windows proporcionada para cada puesto. Todos los archivos que no se encuentren en esta ubicación no serán copiados necesariamente, a excepción de los correos electrónicos.
- La copia de seguridad de ordenadores que no dispongan de Servidor la realizará el usuario regularmente.
- **No se podrán crear carpetas** en el directorio raíz (**C:**) ni en ningún otro excepto las que estén dentro de "mis documentos", sin previo aviso.
- **Los usuarios que usen software exclusivo** (por ejemplo el departamento de rrhh, administración, etc**) harán sus propias copias de seguridad** que guardarán en una carpeta específica dentro de "mis documentos" para que se incluya dicha información en la copia general.
- **Nunca se deberá desactivar el antivirus** en ningún equipo.

- No está permitido bajo ningún concepto el uso de correo electrónico particular, ni su configuración dentro de ningún programa gestor de correo. Ni tampoco del uso de programas relacionados con la mensajería instantánea o Chat, como por ejemplo Windows Messenger o similares.
- Se recuerda a los usuarios que deben apagar sus ordenadores al finalizar su jornada laboral
- El incumplimiento reiterado de dicha normativa interna (tanto de telefonía como de informática)a podrá ser motivo de amonestación laboral.

En ……., a …… de ……. de 20…..

Fdo.: Fdo. Recibí:

# ANEXO VII

## BRECHA DE SEGURIDAD

# PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE UNA BRECHA DE SEGURIDAD

Cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad o integridad de los datos contenidos en el registro de actividades de la organización, deberá comunicarla inmediatamente al Responsable del Tratamiento quien deberá notificar en un plazo **no superior a 72 horas** a la Agencia Española de Protección de Datos. En los casos en que sea probable que la violación de seguridad suponga un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos.

El procedimiento habilitado por **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. - AUSMAR-**ante una brecha o violación de seguridad es el siguiente:

1- **Valoración del riesgo**: La valoración del riesgo de la quiebra es diferente del análisis de riesgos previo a todo tratamiento. Se pretende determinar hasta qué punto el incidente, por sus características, el tipo de datos a los que se refiere o el tipo de consecuencias que puede ocasionar a los afectados puede causar un daño en sus derechos o libertades.

2- **Daños materiales o inmateriales**: Los daños pueden ser materiales o inmateriales, e ir desde la posible discriminación de los afectados debido al uso de sus datos personales por quien ha accedido a ellos de forma no autorizada hasta la suplantación de identidad, pasando por daños económicos o la exposición pública de datos confidenciales.

3- **Alcance:** Se entiende que se tiene conocimiento de una violación de seguridad cuando hay una **certeza de que se ha producido** y se tiene un conocimiento suficiente de su naturaleza y alcance.

4- **Evidencia o incidente real**: En supuestos de quiebras que por sus características pudieran tener gran impacto, sí sería aconsejable ponerse en contacto con la autoridad de supervisión tan pronto como **existan indicios** de que se ha producido alguna situación irregular respecto a la seguridad de los datos. Sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

5- **Formulario y su contenido:** el formulario es el documento por el cual se notifica tanto a la autoridad competente como a los afectados ante una brecha o violación de seguridad y contendrá :

- La naturaleza de la vi a naturaleza de la violación, categorías de datos y de interesados afectados.
- Medidas impuestas por el responsable para resolver esa quiebra y,
- Si procede, las medidas adoptadas para reducir los posibles efectos negativos sobre los interesados.

6- **Registro de Incidencias**: El Responsable del Tratamiento deberá incluir la brecha o violación de seguridad en el Registro de Incidencias.

# MODELO DE NOTIFICACIÓN DE BRECHA O VIOLACIÓN DE SEGURIDAD

Este modelo será cumplimentado para la notificación ante la Agencia Española de Protección de Datos ante una brecha o violación de seguridad, también la propia autoridad establecerá un canal único y exclusivo para que el Responsable del Tratamiento pueda notificarlo:

| **NOTIFICACIÓN AEPD SOBRE UNA BRECHA DE SEGURIDAD** | **Nº notif.** |
|---|---|
| **Datos del Responsable del Tratamiento** | |
| Fecha, hora y detección de la violación de seguridad: | |
| Circunstancias en que se ha producido la violación de los datos (pérdida, robo, copia etc.): | |
| Naturaleza y contenido de los datos personales en cuestión: | |
| Medidas técnicas y organizativas que ha aplicado el Responsable del Tratamiento a los datos personales en cuestión: | |
| Resumen del incidente que ha causado la violación de datos personales (con indicación de la ubicación física de la violación y del soporte de almacenamiento): | |
| Número de afectados: | |
| Posibles consecuencias y efectos negativos a los afectados: | |
| Medios de comunicación utilizados: | |
| En , a _____de _____ de 202...<br><br>Firma Responsable del Tratamiento o Responsable de Seguridad | |

| NOTIFICACIÓN AL AFECTADO SOBRE UNA BRECHA DE SEGURIDAD | Nº notif. |
|---|---|
| **Datos del Responsable del Tratamiento** | |
| Fecha, hora y detección de la violación de seguridad: | |
| Resumen del incidente que ha causado la violación de datos personales: | |
| Naturaleza y contenido de los datos personales en cuestión: | |
| Posibles consecuencias y efectos negativos a los afectados: | |
| Circunstancias en que se ha producido la violación de los datos (pérdida, robo, copia etc.): | |
| Medidas adoptadas por el Responsable del Tratamiento para subsanar la violación de datos personales:: | |
| En , a _____de _____ de 202...<br><br>Firma Responsable del Tratamiento o Responsable de Seguridad | |

# ANEXO VIII

## REGISTRO DE INCIDENCIAS

# GESTIÓN Y REGISTRO DE INCIDENCIAS

## PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTAANTE LAS INCIDENCIAS

El procedimiento habilitado por **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. - AUSMAR-**para la notificación, gestión y respuesta ante las incidencias es el siguiente:

Cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad o integridad de los datos contenidos en los ficheros de la organización, deberá comunicarla inmediatamente al responsable del registro de incidencias a través del formulario GESTIÓN DE INCIDENCIAS, del que se le ha hecho entrega a cada trabajador.

Deberá especificar el tipo de incidencia producida y su descripción detallada, indicando las intervenciones de las personas que hayan podido tener relación con la producción de la incidencia, así como la fecha y hora en que se ha producido o detectado, la persona que realiza la notificación, a quién se comunica y los efectos que se pueden haber derivado de la incidencia.

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

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

# REGISTRO DE INCIDENCIAS

El registro de incidencias se llevará a cabo a través del formulario denominado REGISTRO DE INCIDENCIAS. Las incidencias registradas se adjuntarán a este anexo.

| **GESTION DE INCIDENCIAS** | | | |
|---|---|---|---|
| FECHA | | HORA | |
| TIPO DE INCIDENCIA | | | |
| DESCRIPCIÓN: | | | |
| EFECTOS DERIVADOS: | | | |
| PERSONA QUE COMUNICA LA INCIDENCIA | | | |
| PERSONA QUE RECIBE LA NOTIFICACIÓN | | | |
| **ACUSE DE RECIBO** | | | |
| FECHA | | HORA | |
| FIRMA: | | | |

# ANEXO IX

## DOCUMENTACIÓN ADICIONAL

# RESUMEN DE LAS MEDIDAS DE SEGURIDAD RGPD

| | | | |
|---|---|---|---|
| **PERSONAL** | • Funciones y obligaciones de los usuarios definidas y documentadas.<br>• Acuerdos de confidencialidad con los usuarios.<br>• Entregar una copia del ANEXO XI a cada usuario. | | |
| **CONTROL DE ACCESO** | • Relación de usuarios, perfiles de usuario y accesos autorizados.<br>• Los usuarios solo deben tener acceso a los datos necesarios para las funciones asignadas.<br>• El permiso de acceso lo concede solo el personal autorizado en la normativa de protección de datos. | **SOLO FICHEROS AUTOMATIZADOS**<br>• Control de acceso físico a los locales que contienen los sistemas de información.<br>• Relación de usuarios autorizados a acceder a los locales donde están los equipos físicos que dan soporte a los sistemas de información (CPD, SRVs). | **SOLO FICHEROS AUTOMATIZADOS**<br>• Registro de accesos (2 años).<br>• Revisión mensual del registro e informe.<br>• No necesario si responsable es persona física y el único usuario.<br><br>**SOLO FICHEROS NO AUTOMATIZADOS**<br>• Registro de accesos a los documentos accesibles por varios usuarios. |
| **IDENTIFICACIÓN Y AUTENTICACIÓN** | **SOLO FICHEROS AUTOMATIZADOS**<br>• Identificación y autenticación personalizada e individual.<br>• Todos los equipos protegidos por contraseña.<br>• Cambio de contraseña como mínimo una vez al año. | **SOLO FICHEROS AUTOMATIZADOS**<br>• Límite de intentos reiterados de acceso no autorizado. | |
| **GESTIÓN DE SOPORTES** | • Inventario de soportes y documentos.<br>• Etiquetado de los soportes.<br>• Acceso restringido al lugar de almacenamiento y relación de los usuarios autorizados a acceder.<br>• Autorización de las salidas de soportes (incluidas a través de mail).<br>• Medidas para el transporte y desecho de soportes. | **SOLO FICHEROS AUTOMATIZADOS**<br>• Entrega y recepción de soportes solo por el personal autorizado en el DS.<br>• Registro de entrada y salida de soportes. | **SOLO FICHEROS AUTOMATIZADOS**<br>• Sistema de etiquetado confidencial.<br>• Cifrado de datos en la distribución de soportes.<br>• Cifrado de información en dispositivos portátiles fuera de las instalaciones. |
| **COPIAS DE RESPALDO** | **SOLO FICHEROS AUTOMATIZADOS**<br>• Copia de respaldo semanal.<br>• Procedimientos de copia y recuperación.<br>• Verificación semestral de los procedimientos. | **SOLO FICHEROS AUTOMATIZADOS**<br>• Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos. | |
| **ALMACENAMIENTO** | **SOLO FICHEROS NO AUTOMATIZADOS**<br>• Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura (bajo llave).<br>• Archivado según los criterios definidos en la normativa de protección de datos. | **SOLO FICHEROS NO AUTOMATIZADOS**<br>• Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave. | |
| **CUSTODIA DE SOPORTES** | **SOLO FICHEROS NO AUTOMATIZADOS**<br>• Durante la tramitación, la persona al cargo de los documentos debe impedir el acceso no autorizado. | | |
| **COPIA O REPRODUCCIÓN** | **SOLO FICHEROS NO AUTOMATIZADOS**<br>• Sólo por los usuarios autorizados en el DS. | | |
| **TELECOMUNICACIONES** | **SOLO FICHEROS AUTOMATIZADOS**<br>• Transmisión de datos a través de redes electrónicas cifrada. | | |
| **TRASLADO DE DOCUMENTACIÓN** | **SOLO FICHEROS NO AUTOMATIZADOS**<br>• Medidas que impidan el acceso o la manipulación. | | |
| **TRABAJO FUERA DE LOS LOCALES** | • Relación de usuarios autorizados y ficheros afectados. | | |
| **INCIDENCIAS** | • Registro de incidencias que afecten o puedan afectar a los datos.<br>• Procedimiento de notificación y gestión de incidencias conocido. | **SOLO FICHEROS AUTOMATIZADOS**<br>• Autorización para la recuperación de datos, así como los detalles de la misma. | |
| **AUDITORÍA** | • Al menos cada dos años.<br>• Informe de deficiencias y propuestas correctoras. | | |
| **RESPONSABLE DE SEGURIDAD** | • Encargado de controlar las medidas de seguridad. | | |

# PRINCIPIOS DE LA RGPD

| | NORMA GENERAL | EXCEPCIONES | OBSERVACIONES |
|---|---|---|---|
| **INFORMACIÓN** | • Todos los formularios de recogida de los datos personales deben contener la cláusula informativa RGPD<br>• Los contratos y demás documentos donde aparezcan datos personales, deben incluir la cláusula informativa.<br>• Es recomendable incluirla también en facturas, albaranes, etc. | | • Los contratos con los clientes deben incluir la cláusula.<br>• Los contratos de trabajo con el personal deben incluir la cláusula. |
| **CONSENTIMIENTO** | • El tratamiento de datos requiere del consentimiento del afectado.<br>• El consentimiento tendrá que ser expreso por el afectado y el Responsable del Tratamiento tendrá que demostrar que aquel consintió.<br>• En caso del afectado ser menor de edad deberá tener mínimo 16 años, si fuese menor de 16 años, el tratamiento se consideraría lícito con el consentimiento del padre o tutor. En España se ha fijado el consentimiento de un menor a partir de los 14 años. | • No es necesario cuando lo autorice una norma con rango de Ley.<br>• No es necesario cuando procedan de fuentes accesibles al público. | •En todas las clausulas se deberá de informar y establecer un apartado donde los clientes, usuarios, proveedores puedan dar su consentimiento expreso., de esa manera el Responsable del Tratamiento podrá demostrarlo. |
| **CALIDAD** | • Los datos deberán ser adecuados, pertinentes y no excesivos para la finalidad para la que son recogidos.<br>• No se podrán utilizar para ninguna otra finalidad distinta a la que se ha informado en la recogida.<br>• Serán exactos y puestos al día para reflejar la realidad del interesado.<br>• Serán cancelados cuando no sean necesarios para la finalidad para la que se han recabado. | | • Se prohíbe la recogida por medios fraudulentos, desleales o ilícitos. |
| **DATOS ESPECIALMENTE PROTEGIDOS** | • Es preciso el consentimiento expreso y por escrito para tratar datos que revelen ideología, afiliación sindical, religión o creencias.<br>• Es preciso el consentimiento expreso para el tratamiento de datos de salud, vida sexual u origen racial.<br>•Es preciso el consentimiento expreso para el tratamiento de datos biométricos y datos genéticos | • No será necesario el consentimiento cuando dicho tratamiento resulte necesario para la prevención o diagnósticos médicos, o la prestación de asistencia sanitaria, siempre que se realice por un profesional sanitario sujeto a secreto profesional o equivalente.<br><br>• Para proteger el interés vital del interesado en los términos anteriores. | • Quedan prohibidos incluir en el registro de actividades los ficheros creados con la finalidad exclusiva de almacenar datos que revelen ideología, afiliación sindical, religión, creencias, origen racial o vida sexual, datos genéticos y datos biomédicos. |
| **SEGURIDAD DE LOS DATOS** | • El Responsable del Tratamiento debe adoptar las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo. | | • El Documento de Seguridad debe recoger las medidas implantadas para garantizar la seguridad y asegurar la protección.<br>• El Documento de seguridad tiene que estar siempre actualizado. |
| **DEBER DE SECRETO** | • Todos los individuos que intervengan en el tratamiento de datos están obligados al secreto profesional y al debe de guardarlos. | | • Es conveniente firmar un Compromiso de confidencialidad y deber de secreto con los trabajadores. |
| **COMUNICACIÓN DE DATOS** | • Los datos solo podrán ser comunicados o cedidos a un tercero previo consentimiento del interesado. | • No es necesario cuando lo autorice una norma con rango de Ley.<br>• No es necesario cuando procedan de fuentes accesibles al público. | |
| **ACCESO A LOS DATOS POR CUENTA DE TERCEROS** | • El acceso a los datos por un tercero para la realización de un servicio deberá estar regulada en un contrato escrito donde se deberá garantizar que el mismo tendrá implantadas medidas de seguridad técnicas y organizativas con la finalidad de garantizar y proteger los datos regulados por el RGPD. | | • En el caso que no exista contrato, podría ser considerada una cesión de datos no consentida.<br>• Las prestaciones sin acceso a datos también deben quedar reguladas en un contrato. |

# ANEXO X

## VIDEOVIGILANCIA

## SUPRESIÓN DE LOS DATOS

Los datos grabados por cámaras de videovigilancia serán suprimidos **en el plazo máximo de un mes** desde su captación, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

## INFORMACIÓN

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto el artículo 12 del RGPD de la siguiente forma:

- Colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

## DERECHOS DE LAS PERSONAS

Para el ejercicio de los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición, el afectado deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada.

## CAPTACIÓN DE IMÁGENES

Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

# ANEXO XI

## DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN

# PROCEDIMIENTO DE ALTA, BAJA O MODIFICACIÓN DE ACCESO AL FICHERO QUE SE ENCUENTRA EN EL REGISTRO DE ACTIVIDADES

Los procedimientos para dar de alta, modificar o dar de baja el acceso autorizado a los ficheros al personal de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-** es:

- ALTA DEL ACCESO:

Cuando se incorpora un nuevo trabajador, el Responsable del Tratamiento establece un identificador único para ese nuevo usuario y le asigna privilegios en función del perfil al que pertenece. Asimismo, le ha de asignar una contraseña provisional que el usuario deberá cambiar en el primer acceso al sistema.

- MODIFICAR EL ACCESO:

Cuando un usuario desempeña distintas funciones en la empresa, o tenga que acceder a datos a los que anteriormente no accedía, el Responsable del Tratamiento deberá cambiar sus privilegios de acceso en función al nuevo perfil al que pertenece.

- DAR DE BAJA EL ACCESO:

Cuando el usuario cause baja temporal, el responsable ha de bloquear la identificación del usuario, y en caso de que sea definitiva, procederá a la eliminación inmediata de todos sus derechos de acceso.

# DESCRIPCIÓN FÍSICA DEL LUGAR

La descripción física del lugar donde se encuentran los ficheros es la siguiente:

**Ficheros automatizados:**
Se encuentran en un servidor de datos al que acceden las aplicaciones instaladas en los puestos de trabajo a través de la red local.

**Ficheros no automatizados**
Los soportes de uso cotidiano se almacenan en los dispositivos de almacenamiento de las oficinas, y los soportes de años anteriores (histórico) en un recinto protegido por llave.

## ENTORNO DE SEGURIDAD Y CONTROL DE ACCESO

Las medidas de seguridad que protegen los ficheros son las siguientes:

- **Ficheros automatizados**

  - Medidas de seguridad: Extintores
  - Control de acceso: El acceso está limitado al personal autorizado a través de un identificador y autenticador que da acceso al sistema de información.
  - El acceso al sistema se bloquea a los indefinidos intentos de acceso fallidos.

- **Ficheros no automatizados**

  - Medidas de seguridad: Trituradora de papel
  - Control de acceso: El acceso está limitado al personal autorizado que dispone de la llave que facilita la apertura de la puerta que da acceso a los ficheros manuales.

## IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS

El sistema de identificación y autenticación que da acceso a los ficheros automatizados, dispone de las siguientes características:

1. Identificación: Nombre del usuario.

2. Autenticación: Contraseña escogida por el usuario.

3. Longitud y contenido de las contraseñas: deben tener una longitud mínima de **8 caracteres y contener Letras y números.**

4. Periodicidad de cambio: el cambio de las contraseñas es cada **3 meses.**

| **Campo** | **Descripción** |
|---|---|
| Identificación Usuario | Identificador *del usuario* |
| Nombre | *Nombre del usuario* |
| Contraseña | *Clave privada del usuario* |
| Datos | *Datos significativos del usuario* |

Esta clave privada se asocia al identificador de usuario de tal forma que el procedimiento de identificación de usuarios solicita al usuario su identificador y su clave privada y tan solo le permite el acceso si estas dos le coinciden.

Tanto el identificador de usuario como la clave privada se almacenan en el fichero de usuarios.

Las contraseñas han sido asignadas, almacenadas y distribuidas de forma absolutamente confidencial.

Se asignarán nuevas contraseñas a los usuarios periódicamente, como mínimo una vez al año.

## - Control de acceso a recursos:

Todos los usuarios tienen acceso autorizado a todos los recursos, es decir, a toda la información que precisan para el desarrollo de sus funciones, salvo que se especifique lo contrario en el presente documento, según consta en el apartado concerniente a la relación de usuarios.

El Responsable del Tratamiento y el Responsable de Seguridad controlan el acceso de los usuarios autorizados a los recursos y ficheros con datos de carácter personal, impidiendo que tengan acceso a recursos o ficheros a los que no estén autorizados.

Para ello se establece un proceso de control de acceso que comprueba que el usuario tiene autorización a utilizar los recursos o ficheros a los que pretende acceder.

Exclusivamente el Responsable del Tratamiento está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos, conforme a los criterios establecidos por él mismo.

La contraseña del usuario autorizado, le permitirá acceder exclusivamente a los recursos a los que esté autorizado, denegando el acceso a los usuarios autorizados que pretendan acceder a recursos o ficheros para los que no estén autorizados.

## - Procedimientos de asignación, distribución y almacenamiento de contraseñas:

El proceso de identificación y autenticación se basa en contraseñas por lo que existe un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantiza su absoluta confidencialidad e integridad. Las contraseñas se almacenan de forma totalmente ininteligible, en un fichero al que sólo tiene acceso el Responsable del Tratamiento o los responsables de seguridad.

## NORMAS GENERALES DE ETIQUETADO DE LOS SOPORTES

El etiquetado que identifique los soportes se realizará de la siguiente forma:

Las tres primeras letras del fichero que contiene seguido del número de soporte, que será correlativo para cada nuevo soporte dado de alta.
En el caso de ficheros que contienen datos de clientes, proveedores y trabajadores, la etiqueta se compone de las letras CLI,PRO,PER, seguido de un número consecutivo.

## NORMAS ESPECIALES DE ETIQUETADO DE LOS SOPORTES

La identificación de soportes y documentos que contengan datos de carácter personal que la organización considerase especialmente sensibles, se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de las personas.

El etiquetado de estos soportes se hará de la siguiente manera:

Las tres primeras letras serán: SPT, seguido del número de soporte, que será correlativo para cada nuevo soporte dado de alta.

Los soportes que se identificarán de esta forma son: Las copias de seguridad

## MEDIDAS ADOPTADAS EN CASO DE QUE LOS DISPOSITIVOS DE ALMACENAMIENTO NO PERMITAN LA OBSTACULIZACIÓN DE SU APERTURA

En los dispositivos que no disponen de mecanismos de obstaculización de su apertura, se evitará el acceso de personas no autorizadas de la siguiente forma:

Siempre que una persona no autorizada pueda tener acceso a soportes con datos personales, está en todo momento supervisada por alguien autorizado para acceder a dichos soportes, no dejándola sola con ellos en ninguna circunstancia.

## PROCEDIMIENTO PARA AUTORIZAR EL ACCESO AL LUGAR DONDE SE ALMACENAN LOS SOPORTES

El procedimiento para autorizar el acceso al lugar protegido donde se almacenan los soportes que contengan datos de carácter personal es el siguiente:

El usuario realizará la petición de acceso al Responsable del Tratamiento o la persona en quien ha delegado esta autorización, el cual, le proporcionará la autorización, así como el mecanismo de apertura que le permita tener acceso a los soportes almacenados en el espacio protegido.

Esta autorización deberá rellenarse según el modelo adjuntado en el ANEXO IV.

## PROCEDIMIENTO PARA AUTORIZAR LA SALIDA DE SOPORTES

El procedimiento para autorizar la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos fuera de los locales del responsable, se detalla a continuación:

El usuario realizará la petición de autorización al Responsable del Tratamiento o la persona en quien ha delegado esta función, el cual, le proporcionará la debida autorización.

Esta autorización deberá rellenarse según el modelo adjuntado en el ANEXO IV.

## CRITERIOS DE ARCHIVO

Los documentos no automatizados se almacenan de acuerdo a los siguientes criterios y procedimientos de archivo: Por fecha y nombre.

Estos criterios garantizan la correcta conservación de los documentos, la localización y consulta de la información y posibilitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

## TRASLADO DE DOCUMENTACIÓN

Siempre que se transportan soportes, ya sean automatizados o documentación no automatizada, se realiza en un maletín con cerradura, de forma que su contenido no sea accesible por personas no autorizadas.

## DESECHO DE DOCUMENTOS

Cuando se desecha cualquier documento que contiene datos de carácter personal, se destruye a través de una trituradora de papel, de forma que no es posible recuperar la información que contenía.

# ANEXO XII

# ENFOQUE DE APROXIMACIÓN AL RIESGO: PROCEDIMIENTO Y ANÁLISIS

## PROCEDIMIENTO DE APROXIMACIÓN AL RIESGO

Para el cumplimiento del principio de "Responsabilidad Proactiva" el responsable y encargado de tratamiento deberán previamente realizar un análisis **y estudio del cumplimiento en materia de protección de datos basado en el riesgo**. Es decir, deberán analizar qué medidas de protección de datos son necesarias implantar para garantizar el cumplimiento del RGPD, en función de naturaleza, alcance, contexto y finalidades del tratamiento de datos que realicen, así como de los riesgos o probabilidades de intromisión en los Derechos y libertades de los interesados.

De esta manera cuanto más probable y grave sea el riesgo del tratamiento, más medidas de protección de datos serán necesarias implantar para contrarrestarlos

## EL MÉTODO MOSLER

Con el objetivo de prevenir y reducir los riesgos en el tratamiento de datos personales hay que utilizar un método que nos permita identificar y, sobre todo, analizar y evaluar esos riesgos. Mientras que su identificación es esencial para poderlos prevenir, con el análisis de los mismos veremos qué podemos hacer para reducirlos, y una correcta evaluación nos permitirá gestionarlos eficientemente, puesto que, con la adaptación al Reglamento General de Protección de Datos, podremos ver si las medidas que se están implantando resultan o no adecuadas. Así, mediante el presente documento se propone que el método de Mosler puede ser idóneo para llevar a cabo una evaluación de los riesgos en materia de protección de datos.

Este método se suele utilizar para evaluar los riesgos que se provocan en determinadas actividades, relaciona la importancia del suceso, el daño ocasionado y la probabilidad de que dicho suceso realmente llegue a ser real

Para ello, se valoran en una escala de 1 a 5 (siendo 1 la puntuación de menos importancia o la menor probabilidad, y 5 la más alta) las siguientes variables:

- **Función:** se valora, en términos generales, la afectación que el daño produciría en la organización, en caso de que el riesgo se llegase a materializar.

- **Sustitución:** se evalúa la facilidad de sustituir a la/s pieza/s o la/s persona/s afectada/s.

- **Profundidad:** se mide el efecto psicológico que tendría el daño si se materializase.

- **Externalización:** se calcula si los efectos negativos serían de carácter individual, local, regional, estatal o internacional.

- **Agresión:** se determina la magnitud del daño real que el daño llegaría a producir.

- **Vulnerabilidad:** se valora la posibilidad real de que, con las circunstancias actuales, se llegue a materializar el daño.

Matemáticamente, tras valorar del 1 al 5 cada uno de estos elementos, se obtienen los siguientes valores:

- **Importancia del suceso:** Función x Sustitución.

- **Daño ocasionado:** Profundidad x Externalización

- **Probabilidad:** Agresión x Vulnerabilidad

Además, Importancia + Daño es igual a "Impacto", con lo que la evaluación global del mismo se obtiene de multiplicar los valores de "Impacto" por "Probabilidad". El valor obtenido oscilará entre 2 y 1.250, de manera que a cada riesgo le corresponderá la siguiente calificación:

- 2-250: Riesgo muy bajo

- 251-500: Riesgo bajo

- 501-700: Riesgo medio

- 701-1.000: Riesgo alto

- 1.000-1.250: Riesgo muy alto

Los principales riesgos que hemos de tener en cuenta son:

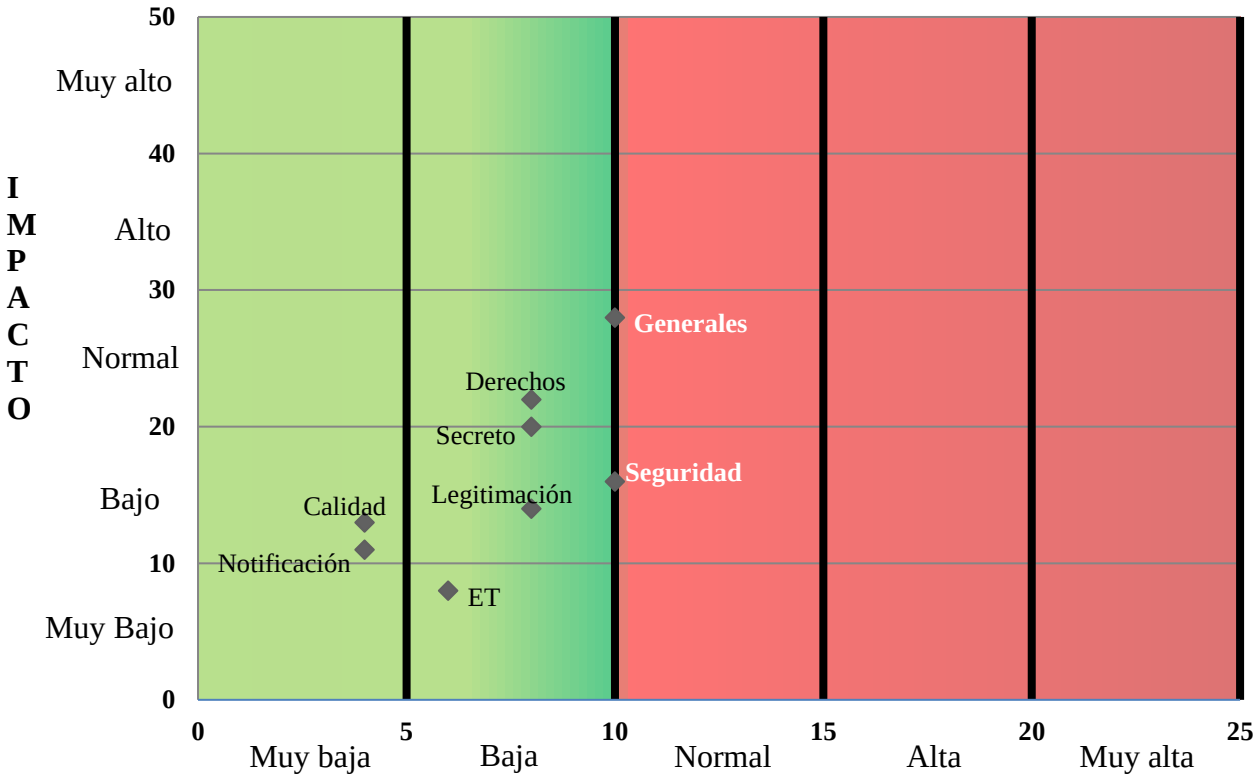
- **Generales:** cualquier riesgo que pueda afectar tanto a la empresa como a las personas y que pueda ocasionar un daños reputacionales así y como económicos.
- **Legitimación de los tratamientos y cesión de datos personales**: cuando el tratamiento de los datos no es el adecuado o se ha obtenido un consentimiento dudoso para el tratamiento o cesión de datos o cuando se obtiene con una finalidad distintita a la perseguida.
- **Transferencias internacionales:** riesgo que aparece cuando no se adoptan las medidas de seguridad adecuadas o cuando no se obtiene la autorización de la autoridad competente para garantizar la protección en la transferencia de datos a cualquier país fuera de la UE.

- **Registro de los tratamientos:** este riesgo aparece cuando el Responsable del Tratamiento no tiene un registro de los datos objeto de tratamientos contenidos en ficheros para garantizar la protección.
- **Transparencia de los tratamientos:** cuando el Responsable del Tratamiento no recoge datos personales sin proporcionar la debida información o cuando la proporciona pero en un lenguaje oscuro o impreciso que resulte entendible para los afectados.
- **Calidad de los datos:** Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas.
- **Datos especialmente Protegidos (D.E.P.):** cuando no se utilizan las medidas de seguridad adecuadas para proteger datos relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, violencias de género, datos personales relativos a las características genéticas y biométricas.
- **Deber de secreto:** riesgo que aparece cuando se viola la confidencialidad o cuando hay un acceso no autorizado de los datos personales del Responsable del Tratamiento.
- **Tratamiento por Encargo:** riesgo que aparece cuando no se ha realizado un contrato que refleje las medidas y garantías necesarias para proteger los datos del Responsable del Tratamiento respecto el Encargado del Tratamiento.
- **Derechos del interesado:** cuando el Responsable del Tratamiento no proporciona, dificulta o carece de procedimientos para el ejercicio de dichos derechos a los afectados.
- **Seguridad:** Inexistencia de políticas de seguridad para la protección de los datos personales.

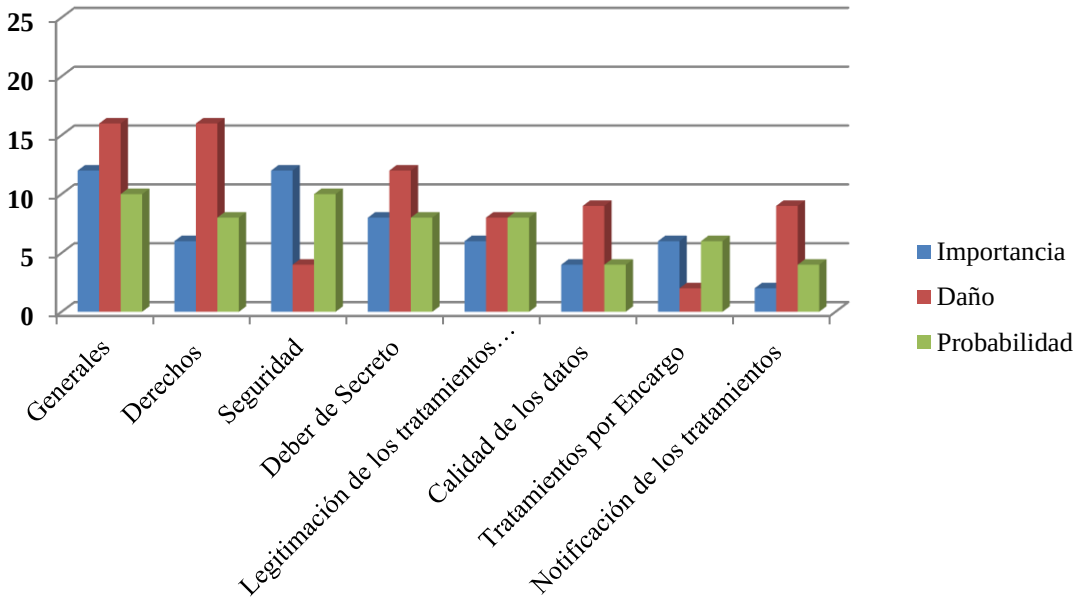
En el caso de **AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -AUSMAR-** teniendo en cuenta los riesgos que hemos relacionado anteriormente, podemos analizarlos y evaluarlos como sigue:

| Riesgo | Evaluación | | | | | |
|---|---|---|---|---|---|---|
| | Función | Sustitución | Profundidad | External. | Agresión | Vulnerab. |
| Generales | 4 | 3 | 4 | 4 | 5 | 2 |
| Derechos | 3 | 2 | 4 | 4 | 4 | 2 |
| Seguridad | 4 | 3 | 2 | 2 | 5 | 2 |
| Deber de Secreto | 2 | 4 | 4 | 3 | 4 | 2 |
| Legitimación | 3 | 2 | 4 | 2 | 4 | 2 |
| Calidad de los datos | 2 | 2 | 3 | 3 | 2 | 2 |
| Tratamientos por Encargo | 3 | 2 | 1 | 2 | 3 | 2 |
| Notificación | 1 | 2 | 3 | 3 | 2 | 2 |

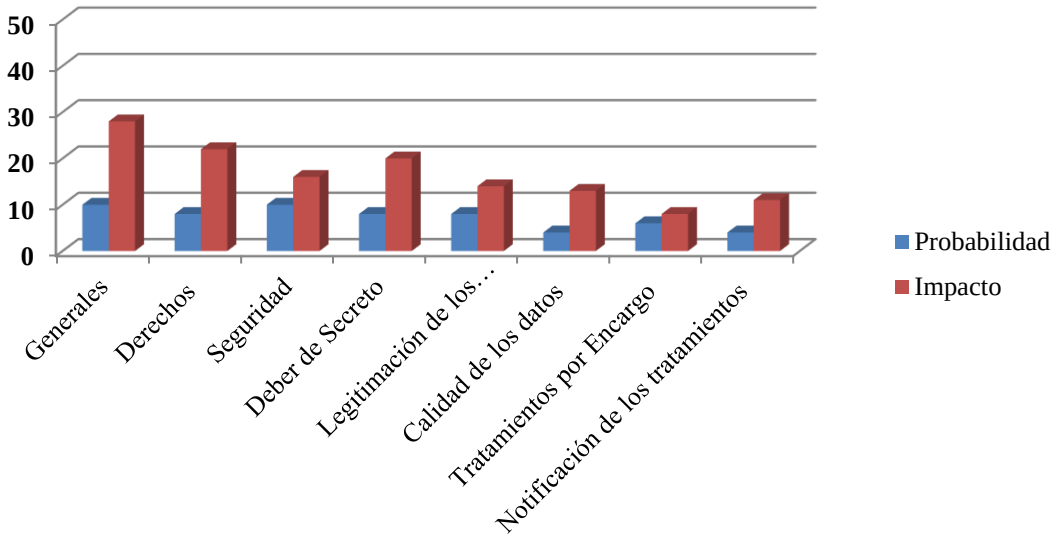
## MAPA DE RIESGOS



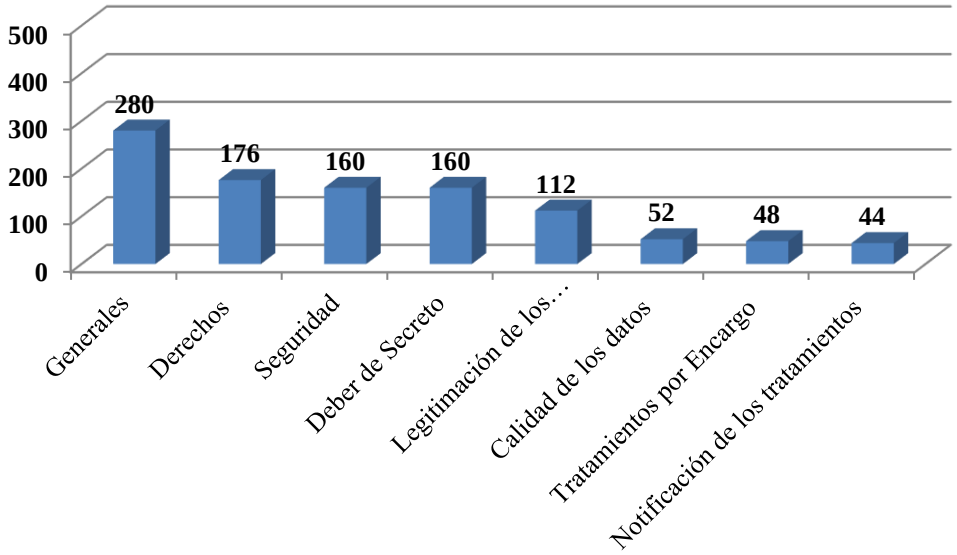
## RIESGOS PROTECCIÓN DE DATOS




## RIESGOS PROTECCIÓN DE DATOS: PROBABILIDAD-IMPACTO



## GRAVEDAD


500
400
300
200
100
0
280
176
160
160
112
52
48
44
Generales
Derechos
Seguridad
Deber de Secreto
Legitimación de los…
Calidad de los datos
Tratamientos por Encargo
Notificación de los tratamientos

# ANEXO XIII

## REGISTRO DE ACTIVIDADES EN EL TRATAMIENTO DE DATOS

**REGISTRO DE ACTIVIDADES DE AUXILIAR DE SEGURIDAD EN LA MAR, S.A. -Ausmar-**

*Domicilio Social: C/ Serrano, 93, 3º E, , 28006,,Madrid*

*CIF:* A-28709319

*Teléfono / Mail:* 93.637.48.48, info@ausmar.es

*Representante Legal: Juan Fargas Duarry*

*Datos del D.P.O.: No aplica*

| IDENTIFICACIÓN DEL TRATAMIENTO | FINALIDAD DEL TRATAMIENTO | TRANSFERENCIA DE DATOS FUERA DE LA UE | TIPOLOGIA DE DATOS |
|---|---|---|---|
| **CONTABILIDAD** | Fichero destinado a la gestión de la contabilidad de la empresa. | No aplica | Categorías no especiales de datos |
| **PERSONAL** | Fichero destinado a la gestión de los recursos humanos de la empresa y a la tramitación de sus nóminas, contratos y seguros sociales. | No aplica | Categorías no especiales de datos |
| **CLIENTES** | Fichero destinado a la gestión de la base de datos de los clientes | No aplica | Categorías no especiales de datos |
| **PROVEEDORES** | Fichero destinado a la gestión de la base de datos de los proveedores. | No aplica | Categorías no especiales de datos |
| **VIDEOVIGILANCIA** | Fichero destinado al tratamiento de las imágenes captadas a través de sistemas de videocámaras para la vigilancia del acceso a las instalaciones y control de flotas. | Sí/no y dónde | Categorías no especiales de datos |

| Concepto | Descripción |
|---|---|
| Nombre del Fichero | **CONTABILIDAD** |
| Descripción y Finalidad del tratamiento | Fichero destinado a la gestión de la contabilidad de la empresa. |
| Tipo de información | Contable y fiscal |
| Categorías de interesados | • Usuarios, persona responsable y familiares.<br>• Trabajadores.<br>• Proveedores. |
| Categoría de datos: | • D.N.I./N.I.F.<br>• Nombre y Apellidos.<br>• Dirección (Postal, Electrónica).<br>• Teléfono.<br>• Información comercial<br>• Económicos, financieros y de seguros.<br>• Transacciones de bienes y servicios. |
| Categorías especiales de datos | **No** |
| Destinatarios | • Encargados del Tratamiento<br>• Organizaciones o personas directamente relacionadas con el responsable.<br>• Registros públicos.<br>• Administración Tributaria.<br>• Otros órganos de la Administración Pública.<br>• Bancos, entidades financieras.<br>• Entidades aseguradoras.<br>• Entidades Sanitarias.<br>• Asociaciones y organizaciones sin ánimo de lucro.<br>• Administración Pública con competencia en la materia. |
| Medidas de Seguridad | Las medidas de seguridad vienen establecidas en la normativa interna de protección de datos de carácter personal del responsable del tratamiento, entre ellas:<br>• La seudonimización y el cifrado de datos personales;<br>• La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;<br>• La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;<br>• La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. |
| Plazo previsto para la supresión | El plazo legalmente establecido, teniendo en cuenta el principio de limitación del plazo de conservación establecido en el art.5.1 e) del RGPD y de posibles exigencias de responsabilidades derivadas del tratamiento. |

| Concepto | Descripción |
|---|---|
| Nombre del Fichero | **PERSONAL** |
| Descripción y Finalidad del tratamiento | Fichero destinado a la gestión de los recursos humanos de la empresa y a la tramitación de sus nóminas, contratos y seguros sociales. |
| Tipo de información | Laboral |
| Categorías de interesados | • Trabajadores. |
| Categoría de datos | • D.N.I./N.I.F.<br>• Nombre y Apellidos.<br>• Dirección (Postal, Electrónica).<br>• Teléfono.<br>• N.ss / Mutualidad<br>• Firma<br>• Currículum Vitae<br>• Huella<br>• Características personales<br>• Circunstancias sociales<br>• Académicos y profesionales<br>• Detalles del empleo<br>• Económicos, financieros y de seguros. |
| Categorías especiales de datos | **No** |
| Destinatarios | • Encargados del Tratamiento<br>• Organizaciones o personas directamente relacionadas con el responsable.<br>• Organismos de la Seguridad Social.<br>• Administración Tributaria.<br>• Otros órganos de la Administración Pública.<br>• Bancos, entidades financieras.<br>• Entidades aseguradoras.<br>• Entidades Sanitarias.<br>• Sindicatos y Juntas del personal.<br>• Administración Pública con competencia en la materia. |
| Medidas de Seguridad | Las medidas de seguridad vienen establecidas en la normativa interna de protección de datos de carácter personal del responsable del tratamiento, entre ellas:<br>• La seudonimización y el cifrado de datos personales;<br>• La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;<br>• La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;<br>• La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. |
| Plazo previsto para la supresión | El plazo legalmente establecido, teniendo en cuenta el principio de limitación del plazo de conservación establecido en el art.5.1 e) del RGPD y de posibles exigencias de responsabilidades derivadas del tratamiento. |

| Concepto | Descripción |
|---|---|
| Nombre del Fichero | **CLIENTES** |
| Descripción y Finalidad del tratamiento | Fichero destinado a la gestión de la base de datos de clientes |
| Tipo de información | Comercial, contable |
| Categorías de interesados | • Persona Responsable<br>• Clientes y Usuarios |
| Categoría de datos | • D.N.I./N.I.F.<br>• Nombre y Apellidos.<br>• Dirección (Postal, Electrónica).<br>• Teléfono.<br>• Firma<br>• Firma electrónica<br>• Información comercial<br>• Económicos, financieros y de seguros.<br>• Transacciones de bienes y servicios. |
| Categorías especiales de datos | **No** |
| Destinatarios | • Encargados del Tratamiento<br>• Organizaciones o personas directamente relacionadas con el responsable.<br>• Registros públicos.<br>• Administración Tributaria.<br>• Otros órganos de la Administración Pública.<br>• Bancos, entidades financieras.<br>• Entidades aseguradoras.<br>• Entidades Sanitarias.<br>• Administración Pública con competencia en la materia. |
| Medidas de Seguridad | Las medidas de seguridad vienen establecidas en la normativa interna de protección de datos de carácter personal del responsable del tratamiento, entre ellas:<br>• La seudonimización y el cifrado de datos personales;<br>• La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;<br>• La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;<br>• La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. |
| Plazo previsto para la supresión | El plazo legalmente establecido, teniendo en cuenta el principio de limitación del plazo de conservación establecido en el art.5.1 e) del RGPD y de posibles exigencias de responsabilidades derivadas del tratamiento. |

| Concepto | Descripción |
|---|---|
| Nombre del Fichero | **PROVEEDORES** |
| Descripción y Finalidad del tratamiento | Fichero destinado a la gestión de la base de datos de proveedores |
| Tipo de información | Comercial, contable |
| Categorías de interesados | • Persona Responsable<br>• Proveedores |
| Categoría de datos | • D.N.I./N.I.F.<br>• Nombre y Apellidos.<br>• Dirección (Postal, Electrónica).<br>• Teléfono.<br>• Firma<br>• Firma electrónica<br>• Información comercial<br>• Económicos, financieros y de seguros.<br>• Transacciones de bienes y servicios. |
| Categorías especiales de datos | **No** |
| Destinatarios | • Encargados del Tratamiento<br>• Organizaciones o personas directamente relacionadas con el responsable.<br>• Registros públicos.<br>• Administración Tributaria.<br>• Otros órganos de la Administración Pública.<br>• Bancos, entidades financieras.<br>• Entidades aseguradoras.<br>• Entidades Sanitarias.<br>• Administración Pública con competencia en la materia. |
| Medidas de Seguridad | Las medidas de seguridad vienen establecidas en la normativa interna de protección de datos de carácter personal del responsable del tratamiento, entre ellas:<br>• La seudonimización y el cifrado de datos personales;<br>• La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;<br>• La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;<br>• La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. |
| Plazo previsto para la supresión | El plazo legalmente establecido, teniendo en cuenta el principio de limitación del plazo de conservación establecido en el art.5.1 e) del RGPD y de posibles exigencias de responsabilidades derivadas del tratamiento. |

| Concepto | Descripción |
|---|---|
| Nombre del Fichero | **VIDEOVIGILANCIA** |
| Descripción y Finalidad del tratamiento | Fichero destinado al tratamiento de las imágenes captadas a través de sistemas de cámaras o videocámaras para la vigilancia del acceso a las instalaciones |
| Tipo de información | Videovigilancia |
| Categorías de interesados | • Persona Responsable<br>• Trabajadores<br>• Clientes y Usuarios<br>• Proveedores |
| Categorías de interesados | • Usuarios, persona responsable y familiares.<br>• Trabajadores.<br>• Proveedores.<br>• Visitas |
| Categoría de datos | • Imagen / Sonido<br>• Características personales |
| Categorías especiales de datos | • No |
| Destinatarios | • Encargados del Tratamiento<br>• Organizaciones o personas directamente relacionadas con el responsable.<br>• Administración Pública con competencia en la materia. |
| Medidas de Seguridad | • Las medidas de seguridad vienen establecidas en la normativa interna de protección de datos de carácter personal del responsable del tratamiento, entre ellas:<br>• La seudonimización y el cifrado de datos personales;<br>• La capacidad permanente de garantizar la confidencialidad, integridad, disponibilidad y resiliencia o adaptación al cambio de los sistemas de información y servicios de tratamiento;<br>• La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;<br>• La verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. |
| Plazo previsto para la supresión | • El plazo legalmente establecido, teniendo en cuenta el principio de limitación del plazo de conservación establecido en el art.5.1 e) del RGPD y de posibles exigencias de responsabilidades derivadas del tratamiento. |

# ANEXO XIV

## USUARIOS CON ACCESO A LOS FICHEROS INCLUIDOS EN EL REGISTRO DE ACTIVIDADES

**- SEDE VILADECANS –**

| | |
|---|---|
| Datos de la persona | **Juan Fargas Duarry** |
| Puesto | Director General – Administrador Legal |
| Identificador de usuario | **46.231.993-S** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☒ PERSONAL<br>☒CLIENTES<br>☒PROVEEDORES<br>☒ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: Él mismo<br>▪ Fecha de Alta: 2010 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Víctor Infiesta Ramoneda** |
| Puesto | Comercial |
| Identificador de usuario | **46.231.027-S** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2010 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Mª Isabel Chávez Chávez** |
| Puesto | Administrativa |
| Identificador de usuario | **47875762-C** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2019 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Antonio Celdrán Celdrán** |
| Puesto | Oficial 2ª Industria |
| Identificador de usuario | **38.551.443-Q** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2010 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Jeremy Fr. Barlari Arriagada** |
| Puesto | Oficial 2ª Industria |
| Identificador de usuario | **46.599.920-B** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2010 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Mikel Cherigny Díaz-Perona** |
| Puesto | Comercial |
| Identificador de usuario | **46.364.169-X** |
| Recursos autorizados | Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2014 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Laura Gonzalez Agustin** |
| Puesto | Contable |
| Identificador de usuario | **34.758.867-W** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☒ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2021 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Natalia Gutiérrez Garangou** |
| Puesto | Dirección de Administración |
| Identificador de usuario | **43.627.874-W** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☒ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☒ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Belén Mateu Casacuberta** |
| Puesto | Asistente departamento comercial |
| Identificador de usuario | **46.238.232-K** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2024 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Javier Garcia Hernández** |
| Puesto | Técnico |
| Identificador de usuario | **70870181M** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2019 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Mahamadou  Sanoussy Diakhaby** |
| Puesto | Mozo de Almacén |
| Identificador de usuario | **Y9947493F** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2021 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Sanoussy Diakhaby** |
| Puesto | Mozo de Almacén |
| Identificador de usuario | **Y5632442D** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2022 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Patricio Marcet Ogier** |
| Puesto | Comercial |
| Identificador de usuario | 47.886.701-B |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2023 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Crisanto José Villalobos Gutiérrez** |
| Puesto | Director de compras |
| Identificador de usuario | Y-4970891-F |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2023 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Mohamed Konari** |
| Puesto | Mozo de Almacén |
| Identificador de usuario | **Y8290614W** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 2023 |
| Observaciones | |

**- SEDE PASAJES (GUIPÚZCOA) -**

| | |
|---|---|
| Datos de la persona | **Eduardo Fernández- Berridi Olano** |
| Puesto | Responsable de la estación Ausmar Euskadi |
| Identificador de usuario | **44.161.370-J** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 07.01.2018 |
| Observaciones | |

| | |
|---|---|
| Datos de la persona | **Javier López Huertas** |
| Puesto | Técnico de la estación Ausmar Euskadi |
| Identificador de usuario | **44.153.365-N** |
| Recursos autorizados | ▪ Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>▪ Persona que lo autorizó: El Director General<br>▪ Fecha de Alta: 21/07/2005 |
| Observaciones | |

# ANEXO XV

## APLICACIONES QUE ACCEDEN A LOS FICHEROS

| Concepto | Descripción |
|---|---|
| Aplicación utilizada | **WINDOWS OFFICE** |
| Descripción | Software de gestión integral |
| Ficheros a que accede | *Contabilidad, Personal, Clientes, Proveedores y Videovigilancia.* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **SQL SERVER** |
| Descripción | Programa de acceso al servidor |
| Ficheros a que accede | *Clientes, Clientes Potenciales, Proveedores y Personal.* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **"DECADA"** |
| Descripción | Software hecho a medida para la gestión de la base de datos de los Clientes. |
| Ficheros a que accede | *Clientes* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **SUPER LIFE PRO** |
| Descripción | Software destinado a la gestión de la videovigilancia de la empresa. |
| Ficheros a que accede | *Videovigilancia* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **EVOPLUSLITE** |
| Descripción | Software destinado a la gestión de la videovigilancia de la empresa. |
| Ficheros a que accede | *Videovigilancia* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **GLOBALSITE** |
| Descripción | Software destinado a la gestión del seguimiento de flotas de la empresa. |
| Ficheros a que accede | |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **QUARTUP** |
| Descripción | Software destinado a la gestión integral de la empresa. |
| Ficheros a que accede | *Contabilidad, Personal, Clientes, Proveedores.* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **MCHARD** |
| Descripción | Software destinado al mantenimiento informático de la empresa. |
| Ficheros a que accede | *Contabilidad, Personal, Clientes, Proveedores.* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **CROSSCHEX STANDARD** |
| Descripción | Software destinado al control de la jornada laboral de los trabajadores de la empresa. |
| Ficheros a que accede | *Personal* |
| Observaciones | |

| Concepto | Descripción |
|---|---|
| Identificación Proceso | **TIMENET** |
| Descripción | Software destinado al control de la jornada laboral de los trabajadores de la empresa. |
| Ficheros a que accede | *Personal* |
| Observaciones | |

# ANEXO XVI

## ENCARGADOS DEL TRATAMIENTO

| Encargado del Tratamiento | **ASSESSORIA PARES ROURA, S.L.** |
|---|---|
| Domicilio Social | C/ Valencia, 55, Esc. D, ent. 3ª, 08015 Barcelona. |
| CIF | B-63.175.939 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☒ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de asesoramiento laboral y RRHH. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Persona responsable | Jordi Parés Roura |
| DNI Responsable | 37.739.691-A |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **CENTRAL AUTOCONTABLE, S.A.** |
|---|---|
| Domicilio Social | C/ Tallers, 77, 2º 2ª, 08001 Barcelona |
| CIF | A-58.525.254 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☐ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de asesoramiento fiscal y contable. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Persona responsable | Guillem Clavell Mallol |
| DNI Responsable | 46.116.054-L |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **BUFETE DE ASESORAMIENTO FISCAL TEJEIRO MEDINA TEJEIRO, S.L.** |
|---|---|
| Domicilio Social | C/ Balmes, 224, 4º 1ª, 08006 Barcelona |
| CIF | B-63.924.856 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☐ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de asesoramiento fiscal.. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Persona responsable | Miguel Tejeiro Losada |
| DNI Responsable | 46.112.494-R |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **QUARTUP, SL** |
|---|---|
| Domicilio Social | C/Sicilia 386, Bajos1, 08025, Barcelona |
| CIF | B-65899890 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☒ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☒ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de mantenimiento informático. |
| Persona responsable | Miguel Ángel Torres Romero |
| DNI Responsable | 1.107.175-R |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **VALORA PREVENCIÓN UMIVALE** |
|---|---|
| Domicilio Social | C/ Colón, 82, 46004 Valencia |
| CIF | B-97.673.453 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☒ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de Prevención de Riesgos laborales y Vigilancia de la Salud. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **UP2YOU CREATIVOS DEL MARKETING, S.L.** |
|---|---|
| Domicilio Social | Avda. Miquel Batllori, 81-83 Baixos – 25001 Lleida |
| CIF | B-25813171 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☒ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA<br>. |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de gestión de la página web y marketing |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **CAP FINANCE , S.L.** |
|---|---|
| Domicilio Social | C/ Marqués de Monistrol 19, 08011, Barcelona |
| CIF | B-65581936 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☐ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio contable y fiscal. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **BUFETE ESCURA, S.L.** |
|---|---|
| Domicilio Social | C/Londres nº 43 bajos 08029 Barcelona |
| CIF | B-61534004 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☐ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de protección de datos. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **ECOGESA XXI, S.L.** |
|---|---|
| Domicilio Social | Av. Diagonal 482, 1ª Plnta , 08006 Barcelona |
| CIF | B-61933396 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☒ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de auditoría de calidad de la empresa. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **MC HARD SOLUCIONES EN SISTEMAS SL** |
|---|---|
| Domicilio Social | Calle Valldemosa 34, 08016 Barcelona |
| CIF | B-67121152 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☒ CONTABILIDAD<br>☒ PERSONAL<br>☒ CLIENTES<br>☒ PROVEEDORES<br>☒ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de mantenimiento informático. |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **ANVIZ GLOBAL INC.,** |
|---|---|
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☒ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de mantenimiento del programa de gestión de la jornada laboral "**CROSSCHEX".** |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |

| Encargado del Tratamiento | **GPI SOFTWARE INTERNET, SL,** |
|---|---|
| Domicilio Social | Av. Sant Jordi, 168, 17800 Olot, Girona |
| CIF | B-17821232 |
| Ficheros a los que tiene acceso | • Acceso a los ficheros:<br>☐ CONTABILIDAD<br>☒ PERSONAL<br>☐ CLIENTES<br>☐ PROVEEDORES<br>☐ VIDEOVIGILANCIA |
| Finalidad del Encargo | La finalidad del encargo es la prestación del servicio de mantenimiento del programa de gestión de la jornada laboral "**TIMENET".** |
| Donde se presta el servicio | La prestación del servicio se realiza en los locales del encargado del tratamiento. |
| Duración del contrato | Mientras dure la relación jurídica entre ambos |
| Observaciones | |