




# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Ámbito de sensibilidad y distribución: PÚBLICO

Este documento es propiedad de **SETEC ACUATICA, S.L.** no puede ser utilizado para fines distintos de los cuales haya sido entregado, reproducido, completamente o en parte, o transmitido o comunicado a cualquier persona sin la autorización del titular.


CATEGORÍA DEL DOCUMENTO USO OFICIAL - PÚBLICO

Departamento emisor: Dirección General		
Realiza: <b>Comité de seguridad</b>	Revisa:	Aprueba: <b>Comité de seguridad</b>

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna-PUB.docx	Página 2 de 20

• Objeto	3
• Normas	3
• Alcance	4
• Roles y responsabilidades	5
• Guías	5
1. INTRODUCCIÓN	6
2. MISION	7
3. VISION	7
4. OBJETIVOS	7
5. VALORES	8
6. CUMPLIMIENTO ENS	9
7. ORGANIZACIÓN DE LA SEGURIDAD	13
8. DATOS DE CARÁCTER PERSONAL	17
9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	18
10. TERCERAS PARTES	19
11. APROBACION Y ENTRADA	19
12. COMUNICACIÓN DE LA POLÍTICA	20
13. REVISIÓN, ACTUALIZACIÓN Y MANTENIMIENTO DE LA POLÍTICA	20

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna-PUB.docx	Página 3 de 20

## • Objeto

El objetivo de este documento es definir la Política de Seguridad de la Información de SETEC ACUÁTICA, S.L. en relación con el Esquema Nacional de Seguridad (ENS), estableciendo los principios, criterios y directrices generales que rigen la protección de la información y los servicios digitales de la organización.

Esta Política constituye el marco de referencia de alto nivel para:


- Proteger la información y los sistemas de información frente a amenazas internas y externas, accidentales o deliberadas.
- Asegurar que la seguridad se gestiona como un proceso integral (prevención, detección, reacción y recuperación).
- Garantizar la continuidad de los servicios y la calidad de la información, reduciendo el riesgo a niveles aceptables.
- Definir la organización de la seguridad (roles, responsabilidades y órganos de coordinación) conforme al ENS.
- Servir como base para el desarrollo de normas y procedimientos internos, y para la generación de evidencias durante auditorías o procesos de certificación.

## • Normas

La base normativa que afecta al desarrollo de las actividades y competencias de SETEC ACUÁTICA, S.L. en cuanto a la prestación de servicios digitales y al uso de sistemas de información, y que implica la implantación explícita de medidas de seguridad, está constituida por la legislación recogida y mantenida en el documento interno de "Legislación Vigente ENS" (registro normativo corporativo), en el que se integran, como mínimo:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Normativa aplicable en materia de administración electrónica y seguridad cuando sea exigible por razón de clientes o proyectos.
- Normativa vigente en materia de protección de datos personales (RGPD y LOPDGDD), cuando resulte aplicable al tratamiento de datos personales en el marco de la actividad.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 4 de 20

- Resto de normativa aplicable a SETEC ACUÁTICA, S.L. como entidad privada, incluyendo obligaciones contractuales con clientes y terceros que impongan requisitos de seguridad.

El mantenimiento del marco normativo será responsabilidad de SETEC ACUÁTICA, S.L. y se realizará en coherencia con las guías e instrucciones técnicas relacionadas con el ENS, así como con las publicaciones y recomendaciones técnicas del CCN-CERT, considerando su carácter evolutivo.

Es responsabilidad de SETEC ACUÁTICA, S.L. identificar las guías técnicas del CCN-CERT que resulten de aplicación o recomendables para reforzar el cumplimiento del ENS, seleccionándolas de acuerdo con el alcance y naturaleza de los sistemas y servicios.

## • Alcance

La presente Política de Seguridad de la Información es de aplicación a SETEC ACUÁTICA, S.L., y resulta obligatoria para todas las áreas, funciones y servicios de la organización que intervienen en el uso, tratamiento, gestión, almacenamiento, transmisión o custodia de información, con independencia de su soporte, formato o grado de automatización.


El alcance comprende los sistemas de información, servicios y procesos que conforman SafeBeach y que soportan el tratamiento de la información necesaria para la prestación de los servicios de aplicación en modalidad SaaS ofrecidos a sus clientes, de acuerdo con lo dispuesto en el Real Decreto 311/2022, y conforme al Documento de Categorización y la Declaración de Aplicabilidad vigente.

La presente Política es de aplicación a todas las personas que tengan acceso a la información o a los sistemas incluidos en el alcance, con independencia de su vinculación jurídica con SETEC ACUÁTICA, S.L. En particular, resulta de obligado cumplimiento para:

- la Dirección de la entidad,
- los colaboradores y profesionales externos que presten servicios para la organización, y
- cualquier otra tercera parte que, por razón de contrato, servicio o acuerdo, tenga acceso a información o sistemas de SETEC ACUÁTICA, S.L.

La Política se aplica con independencia de que el acceso se realice desde instalaciones propias o de terceros, y con independencia del soporte tecnológico utilizado.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna-PUB.docx	Página 5 de 20

Con el fin de garantizar que el proceso de seguridad implantado se mantiene actualizado y mejora de forma continua, SETEC ACUÁTICA, S.L. establece, implementa y mantiene un Sistema de Gestión de la Seguridad de la Información, alineado con los principios del Esquema Nacional de Seguridad. El contenido de esta Política se desarrolla mediante normas y procedimientos internos complementarios, que concretan los requisitos de seguridad y permiten generar evidencias del cumplimiento.

El alcance definido en esta Política responde a la situación actual de los sistemas y servicios de la organización. No obstante, podrá ser revisado y modificado cuando se produzcan cambios significativos en los servicios, en la tecnología empleada, en los proveedores críticos o en el contexto normativo, debiendo en tal caso revisarse el análisis de riesgos y actualizarse la documentación del sistema conforme a los procedimientos establecidos.

## • Roles y responsabilidades

Para garantizar el cumplimiento del ENS y la implantación eficaz de las medidas de seguridad, la organización define roles y responsabilidades de seguridad que estarán documentados en el procedimiento interno de Roles y Responsabilidades y formalizados mediante designaciones internas aprobadas por Dirección.


Documento: Org.04-Art 13-PCD-Definición de Roles Responsabilidades y Comité de Seguridad-INT

Asimismo, la identificación y aplicación de guías y recomendaciones técnicas se gestionará mediante los mecanismos internos de actualización y consulta establecidos por la organización, de manera que las referencias técnicas se mantengan actualizadas a lo largo del tiempo.

## • Guías

Las guías que afecten a controles concretos deberán estar alineadas con la Declaración de Aplicabilidad del sistema, donde se reflejan las medidas aplicables en función del alcance y del análisis de riesgos, debido a su carácter cambiante y a que el CCN-CERT actualiza constantemente las GUÍAS. Documento: [GUIAS CCN-CERT \(por su consulta\)](#).

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 6 de 20

## 1. INTRODUCCIÓN

SETEC ACUÁTICA, S.L. depende de los sistemas TIC (Tecnologías de la Información y las Comunicaciones) para alcanzar sus objetivos empresariales, operar sus servicios y mantener la confianza de sus clientes y colaboradores. Estos sistemas deben ser administrados con diligencia, aplicando medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada o de los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con rapidez a los incidentes. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la seguridad, atendiendo al uso previsto y al valor de la información y los servicios.


En particular, la seguridad de la información resulta crítica en aquellos servicios digitales que implican la monitorización, análisis y gestión de información asociada a entornos físicos y operativos, como los prestados por SETEC ACUÁTICA, S.L. a través de sus soluciones tecnológicas. Por ello, la organización adopta un enfoque de seguridad orientado a la fiabilidad del servicio, la disponibilidad continua y la protección frente a accesos o usos no autorizados.

Para defenderse de estas amenazas se requiere una estrategia que se adapte a los cambios del entorno y garantice una operación continua y segura. Esto implica:

- Aplicar las medidas mínimas de seguridad exigidas por el ENS en función del alcance y la categorización del sistema.
- Realizar un seguimiento continuo del nivel de prestación de servicios y del estado de seguridad de los activos críticos.
- Identificar, analizar y gestionar vulnerabilidades, así como aplicar correcciones con diligencia.
- Preparar y ejecutar una respuesta efectiva ante incidentes para garantizar la continuidad de los servicios.

La seguridad debe integrarse en todo el ciclo de vida de los sistemas: desde la concepción y planificación, pasando por el desarrollo o adquisición, hasta la explotación y retirada del servicio. Los requisitos de seguridad y las necesidades de financiación deberán identificarse e incluirse en la planificación y en los procesos de contratación, especialmente cuando se trate de servicios externalizados o suministros críticos.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 7 de 20

SETEC ACUÁTICA, S.L. se compromete a prevenir, detectar, reaccionar y recuperarse de incidentes, conforme a los principios del ENS, manteniendo evidencias adecuadas y orientando su gestión hacia la mejora continua.

## 2. MISIÓN

La misión de SETEC ACUÁTICA, S.L. es dar mayor valor y sentido al trabajo del socorrismo, convirtiéndolo en conocimiento que previene accidentes y salva vidas.

## 3. VISIÓN

La visión de SETEC ACUÁTICA, S.L. es que el impacto del socorrismo sea tan visible y medible que nadie pueda volver a cuestionarlo.

## 4. OBJETIVOS

Los objetivos de seguridad de la información de SETEC ACUÁTICA, S.L. se alinean con el ENS y se desarrollan mediante el plan interno de adecuación y mejora. A nivel de Política, se establecen como objetivos generales:

4.1. Garantizar un marco jurídico y organizativo coherente con la seguridad de la información y la protección de datos personales cuando sea aplicable.

4.2. Asegurar el control de acceso lógico, gestionando identidades, privilegios y trazabilidad.


4.3. Fortalecer configuraciones y endurecimiento (hardening) en sistemas, servicios y aplicaciones.

4.4. Establecer acciones de formación y concienciación en materia de seguridad adaptadas al modelo operativo sin plantilla.

4.5. Regular y controlar el uso de soportes de almacenamiento y la protección de la información.

4.6. Implantar y mantener un sistema de gestión de seguridad que permita evidenciar cumplimiento y mejora continua.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 8 de 20

4.7. Desarrollar el marco normativo y procedimental necesario para cubrir los requisitos del ENS.

4.8. Implementar monitorización operativa y supervisión de seguridad.

4.9. Definir y mantener planes de continuidad y recuperación, acordes con la criticidad de los servicios.

4.10. Establecer procesos de operación técnica de la seguridad, incluyendo gestión de cambios y configuración.

4.11. Aplicar mecanismos de protección criptográfica y seguridad en las comunicaciones cuando proceda.

## 5. VALORES


Los valores de SETEC ACUÁTICA, S.L. guían la implantación y mantenimiento de la seguridad de la información:

- Orientación al cliente: la seguridad es un componente esencial de la confianza y continuidad del servicio.
- Calidad y diligencia: se aplican controles y procedimientos consistentes, con evidencias verificables.
- Profesionalidad: colaboradores y terceros actúan conforme a responsabilidades definidas y bajo reglas claras.
- Compromiso ético: se protege la información con respeto a la legalidad, a la confidencialidad y a los derechos de las personas.
- Visión de futuro: la seguridad se concibe como mejora continua y como requisito estratégico para el crecimiento.

## 6. CUMPLIMIENTO ENS

SETEC ACUÁTICA, S.L., para conseguir el cumplimiento del Real Decreto 311/2022 y los principios básicos y requisitos mínimos que establece, adopta medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger, de acuerdo con el alcance del sistema y con los resultados del análisis de riesgos.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 9 de 20

### **6.1. Gestión documental del ENS**

Para dar cumplimiento a los requisitos del ENS, se establece un conjunto de procedimientos documentales que darán cobertura a todos los aspectos y requerimientos necesarios según el alcance definido. Este sistema documental permitirá:

- mantener la coherencia del conjunto de políticas, normas y procedimientos;
- controlar versiones, aprobaciones, distribución y retirada;
- asegurar que las evidencias se conservan y están disponibles para auditoría;
- permitir la trazabilidad de decisiones y actuaciones de seguridad.

La gestión documental se realizará conforme al procedimiento interno de creación, clasificación y gestión de información documentada, aplicando criterios de acceso controlado y preservación.

### **6.2. Seguridad como un proceso integral y seguridad por defecto**


La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. La aplicación del ENS en SETEC ACUÁTICA, S.L. se basa en este principio, excluyendo actuaciones puntuales o tratamientos coyunturales.

Se prestará atención especial a la concienciación y a la correcta definición de instrucciones para evitar que la falta de organización, coordinación o directrices inadecuadas sean fuente de riesgo.

Los sistemas se diseñarán y configurarán de manera que garanticen la seguridad por defecto. En particular:

- a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias y solo serán accesibles por personas autorizadas, pudiendo establecerse restricciones de horario, ubicaciones o puntos de acceso cuando proceda.
- c) En explotación se eliminarán o desactivarán, mediante control de configuración, funciones innecesarias o inadecuadas para la finalidad perseguida.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 10 de 20

d) El uso ordinario del sistema será sencillo y seguro, de manera que una utilización insegura requiera una actuación consciente y excepcional.

Este enfoque resulta especialmente relevante en servicios digitales prestados en modalidad SaaS y soportados por infraestructuras cloud y proveedores especializados, donde la correcta coordinación entre controles propios y controles de terceros es esencial para garantizar la seguridad global del sistema.

### **6.3. Reevaluación periódica, integridad y actualización del sistema**

SETEC ACUÁTICA, S.L. implementa controles y evaluaciones regulares de la seguridad para conocer en todo momento el estado de los sistemas respecto a vulnerabilidades, actualizaciones y recomendaciones relevantes, reaccionando con diligencia.

Antes de introducir nuevos elementos (físicos o lógicos), se realizará un análisis formal del impacto en seguridad. Asimismo, se promoverán revisiones periódicas por terceros cuando resulte conveniente para disponer de una evaluación independiente.

### **6.4. Gestión de personal y profesionalidad**

Dado el modelo operativo sin plantilla, las obligaciones de este apartado se aplican a Dirección y a terceros/colaboradores con acceso a sistemas o información.

Se establecerán acciones de concienciación y formación en seguridad, al menos con periodicidad anual, y siempre antes de asignar responsabilidades críticas a cualquier colaborador o proveedor con acceso relevante. La formación será proporcional al rol y al nivel de acceso concedido.


### **6.5. Gestión de la seguridad basada en riesgos. Análisis y gestión de riesgos**

Todos los sistemas afectados por esta Política y los tratamientos de datos personales que procedan serán objeto de un análisis de riesgos, evaluando amenazas y riesgos. Este análisis se repetirá:

- de forma regular, al menos una vez al año;
- cuando cambie significativamente la información manejada o los servicios prestados;
- cuando ocurra un incidente grave o se detecten vulnerabilidades graves.

El Responsable de Seguridad coordinará la ejecución del análisis de riesgos, identificará carencias y debilidades, y lo elevará al Comité de Seguridad para la toma de decisiones y priorización de medidas.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 11 de 20

### **6.6. Incidentes de seguridad: prevención, reacción y recuperación**

SETEC ACUÁTICA, S.L. establece un proceso integral de detección, reacción y recuperación ante incidentes de seguridad. Dicho proceso incluye:

- mecanismos de detección y notificación;
- criterios de clasificación y priorización;
- procedimientos de análisis, contención, erradicación y recuperación;
- vías de comunicación con partes interesadas y proveedores;
- registro de actuaciones y evidencias para mejora continua.

Para evitar perjuicios a la información o a los servicios, la organización aplica las medidas de seguridad del ENS y controles adicionales derivados del análisis de riesgos. Los roles y responsabilidades en materia de incidentes están definidos y documentados.

Se habilitarán mecanismos para que desviaciones significativas respecto de parámetros normales generen alertas y reportes a responsables.

La organización establecerá, como mínimo:


- Mecanismos para responder eficazmente a incidentes.
- Un punto de contacto para comunicaciones relativas a incidentes con terceros.
- Protocolos para intercambio de información asociada al incidente, incluidos contactos con equipos de respuesta (CERT) cuando proceda.
- Medios y técnicas para garantizar la recuperación de los servicios más críticos.

### **6.7. Líneas de defensa y prevención ante sistemas interconectados**

SETEC ACUÁTICA, S.L. adopta una estrategia de protección basada en múltiples capas (organizativas, físicas y lógicas), de manera que el fallo de una capa no implique el compromiso total del sistema. Este enfoque permite:

- ganar tiempo para una reacción adecuada ante incidentes no evitados;
- reducir la probabilidad de compromiso global;

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna-PUB.docx	Página 12 de 20

- minimizar el impacto final.

Cuando existan interconexiones con redes públicas o con sistemas de terceros, se analizarán los riesgos derivados y se controlarán los puntos de unión, aplicando controles específicos y restricciones necesarias.

#### **6.8. Función diferenciada. Organización e implantación del proceso de seguridad**

La organización compromete a los responsables designados mediante roles de seguridad diferenciados y claramente definidos. La segregación de funciones se aplicará de manera proporcional, asegurando supervisión y control aun cuando existan terceros que ejecuten tareas técnicas.

#### **6.9. Autorización y control de accesos**

SETEC ACUÁTICA, S.L. implementa mecanismos de control de acceso limitados a los estrictamente necesarios y debidamente autorizados, garantizando la trazabilidad de las actuaciones y la revocación inmediata cuando deje de existir necesidad o habilitación.

#### **6.10. Adquisición de productos y contratación de servicios de seguridad**

En la adquisición de productos o contratación de servicios, se valorará la funcionalidad de seguridad necesaria y la idoneidad del proveedor. Se aplicará el principio de proporcionalidad y se exigirá que los proveedores críticos aporten garantías suficientes para el nivel de seguridad requerido, estableciendo obligaciones contractuales coherentes con el ENS.


#### **6.11. Protección de la información almacenada y en tránsito. Continuidad de la actividad**

La organización protege la información almacenada o en tránsito, especialmente en entornos expuestos (equipos portátiles, dispositivos móviles, soportes de información, redes abiertas o entornos de terceros). Se dispondrá de copias de seguridad y mecanismos de continuidad que permitan recuperar operaciones en caso de pérdida de medios habituales.

Se establecerán procedimientos para la recuperación y conservación a largo plazo de documentación y registros, y medidas para garantizar que la información en soporte no electrónico se protege con un grado equivalente a la información electrónica.

#### **6.12. Registros de actividad**

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 13 de 20

SETEC ACUÁTICA, S.L. habilita registros de actividad de usuarios y administradores, reteniendo información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar a la persona que actúa en cada momento. Todo ello con la finalidad exclusiva de garantizar seguridad y cumplimiento, respetando los derechos y garantías aplicables, incluida la normativa de protección de datos y, cuando proceda, la normativa laboral.

## 7. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la Seguridad de la Información en SETEC ACUÁTICA, S.L. se establece conforme a lo indicado a continuación.

### 7.1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y adaptación de las medidas exigidas por reglamento, se han definido roles o perfiles de seguridad y se designarán los cargos u órganos que los ocuparán, como mínimo:

- Responsable de la Información.
- Responsable del Servicio.
- Responsable de Seguridad.
- Responsable del Sistema.
- Responsable de Contacto (POC) con proveedores (cuando proceda por criticidad y número de proveedores).


Las designaciones se formalizarán y se conservarán como evidencia del marco de gobernanza.

### 7.2. Comité de Seguridad de la Información

SETEC ACUÁTICA, S.L. constituye un Comité de Seguridad de la Información como órgano colegiado, con composición proporcional al tamaño y estructura de la entidad. Estará formado, como mínimo, por:

- Presidente (Dirección o persona delegada).
- Secretario/a (designado por el Comité).

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna-PUB.docx	Página 14 de 20

- Miembros:
  - Responsable de Seguridad.
  - Responsable del Sistema.
  - Responsable de la Información y/o Responsable del Servicio cuando proceda.
  - Delegado de Protección de Datos cuando se traten asuntos que afecten a datos personales.

El Delegado de Protección de Datos participará con voz y sin voto cuando el Comité trate cuestiones de protección de datos personales; en caso de votación, se hará constar expresamente en acta su criterio u observaciones. Se trata de un asesor externo.

La periodicidad mínima de reunión será anual, sin perjuicio de reuniones extraordinarias cuando existan incidentes relevantes, cambios significativos o necesidades de auditoría.

### 7.3. Responsabilidades asociadas al Esquema Nacional de Seguridad


#### 7.3.1. Funciones del Responsable de la Información y del Responsable del Servicio

- Establecer y aprobar requisitos de seguridad aplicables al servicio y a la información, dentro del marco del ENS, a propuesta del Responsable de Seguridad y/o del Comité.
- Aceptar niveles de riesgo residual que afecten al servicio y/o a la información, de acuerdo con el procedimiento de gestión de riesgos y con la aprobación que corresponda.

#### 7.3.2. Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la información tratada y de los servicios prestados.
- Promover la formación y concienciación en materia de seguridad.
- Coordinar la ejecución del análisis de riesgos, la declaración de aplicabilidad, la identificación de medidas y la elaboración de documentación del sistema.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 15 de 20

- Asesorar en la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y el Comité.
- Participar en planes de mejora y continuidad, procediendo a su validación.
- Gestionar revisiones internas o externas y procesos de auditoría.
- Coordinar, cuando aplique, procesos de certificación o evaluación independiente.
- Elevar al Comité la aprobación de cambios y requisitos del sistema que afecten a seguridad.

### 7.3.3. Funciones del Responsable del Sistema

Como administrador de seguridad del sistema, corresponde al Responsable del Sistema:

- Gestionar, configurar y actualizar el hardware y software vinculados a mecanismos de seguridad.
- Gestionar autorizaciones y privilegios, monitorizando la actividad y su correspondencia con lo autorizado.
- Aprobar cambios de configuración conforme al procedimiento de gestión de cambios.
- Asegurar que los controles de seguridad se cumplen estrictamente.
- Aplicar procedimientos aprobados para la gestión segura del sistema.
- Supervisar instalaciones, modificaciones y mejoras para asegurar que la seguridad no se compromete.
- Monitorizar el estado de seguridad a través de herramientas y mecanismos de auditoría técnica.


Cuando la complejidad lo justifique, podrá designar responsables delegados o delegar funciones concretas manteniendo la trazabilidad de la delegación.

### 7.3.4. Funciones del Responsable de contacto con proveedores (POC)

El responsable POC con proveedores, cuando aplique, realizará funciones tales como:

- Mantener inventario de proveedores relevantes y su modalidad de servicio.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna-PUB.docx	Página 16 de 20


- Recabar información sobre arquitectura de seguridad y ubicación de la información.
- Verificar medidas de seguridad implementadas por el proveedor conforme a obligaciones contractuales.
- Confirmar cumplimiento de normativa aplicable (incluida protección de datos cuando proceda).
- Coordinar notificación y seguimiento de incidentes de seguridad.
- Controlar cadena de subcontratación y cambios relevantes.
- Realizar seguimiento de acuerdos de nivel de servicio (SLA) cuando impacten en seguridad o continuidad.

#### 7.4. Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá, entre otras, las siguientes funciones:

- Atender solicitudes en materia de seguridad, informar del estado de seguridad y asesorar en decisiones.
- Resolver conflictos de responsabilidad o discrepancias entre roles.
- Promover la mejora continua del sistema de gestión de seguridad, coordinando esfuerzos para asegurar consistencia, alineación y evitar duplicidades.
- Proponer planes de mejora y priorización de actuaciones, considerando recursos disponibles.
- Velar por que la seguridad se contemple en todos los proyectos desde su inicio.
- Realizar seguimiento de riesgos residuales relevantes y recomendar actuaciones.
- Realizar seguimiento de incidentes y recomendar medidas correctoras.
- Elaborar y revisar regularmente la presente Política para su aprobación por Dirección.
- Verificar la normativa y procedimientos de seguridad para su aprobación, cuando proceda.
- Promover programas de formación y sensibilización, adaptados al modelo operativo sin plantilla.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 17 de 20

- Promover auditorías periódicas de seguridad y, cuando proceda, revisiones relacionadas con protección de datos.

### 7.5. Procedimientos de designación

La creación del Comité de Seguridad, el nombramiento de sus integrantes y la designación de responsables identificados en esta Política se formalizará por la organización, quedando documentada y comunicada a las partes afectadas. Las designaciones se revisarán periódicamente y siempre que exista vacante, cambio relevante de alcance o modificación del modelo operativo.

### 7.6. Resolución de conflictos

El Comité de Seguridad se encargará de resolver conflictos o diferencias de criterio entre roles, documentando acuerdos y, cuando proceda, escalando a Dirección para decisión final.

## 8. DATOS DE CARÁCTER PERSONAL


SETEC ACUÁTICA, S.L. tratará datos personales únicamente cuando sean adecuados, pertinentes y no excesivos, y siempre relacionados con finalidades legítimas y definidas. La organización adoptará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, de conformidad con la normativa vigente.

Cuando proceda, se mantendrán:

- Registro de actividades de tratamiento.
- Análisis de riesgos y, en su caso, evaluación de impacto.
- Procedimientos de atención de derechos y gestión de brechas.
- Designación y funciones del delegado de Protección de Datos cuando sea exigible o se haya designado voluntariamente.

En caso de incidentes que puedan afectar a datos personales, se activarán mecanismos internos de evaluación, documentación y, cuando corresponda, comunicación y notificación en los plazos legalmente establecidos.

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna-PUB.docx	Página 18 de 20

## 9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad y la Dirección impulsan el desarrollo de un sistema de gestión que será establecido, implementado, mantenido y mejorado, de forma coherente con el ENS y con las necesidades reales de la organización.

Este sistema se documentará y permitirá generar evidencias de controles y del cumplimiento de objetivos. Existirá un procedimiento de gestión documental que establecerá directrices para la estructuración, acceso, preservación y control de documentación de seguridad.

Corresponde al Comité de Seguridad la revisión anual de la presente Política y, cuando proceda, la propuesta de mejoras para su aprobación por Dirección.

## 10. TERCERAS PARTES

Cuando SETEC ACUÁTICA, S.L. preste servicios a clientes públicos o privados, o utilice servicios de terceros, se les hará partícipes de esta Política en la medida que les afecte, y se establecerán canales de coordinación e intercambio de información para:


- la gestión de incidentes;
- la continuidad del servicio;
- la comunicación de cambios relevantes;
- el cumplimiento de obligaciones contractuales y, cuando proceda, normativas.

Cuando SETEC ACUÁTICA ceda información o permita accesos a terceros, estos quedarán sujetos a las obligaciones de seguridad definidas contractualmente, pudiendo desarrollar procedimientos propios siempre que garanticen niveles de protección coherentes con los requisitos exigidos.

Se solicitará que el personal de terceros esté adecuadamente concienciado en seguridad, al menos al mismo nivel requerido por esta Política, y se establecerán mecanismos específicos de comunicación y resolución de incidencias.

Si algún aspecto de esta Política no pudiera ser satisfecho por un tercero, se requerirá un informe del Responsable de Seguridad que identifique el riesgo, proponga medidas

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	SafeBeach
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página 19 de 20

de tratamiento o compensación y, cuando proceda, obtenga aprobación de Dirección y/o de los responsables afectados antes de continuar.

La gestión de terceros constituye un elemento clave del modelo de seguridad de SETEC ACUÁTICA, S.L., dado que parte de los servicios se prestan sobre infraestructuras y plataformas externas. La organización mantiene un control activo de dichos terceros, asegurando que las responsabilidades de seguridad se encuentran claramente definidas y alineadas con los requisitos del ENS.

## 11. APROBACION Y ENTRADA

La presente Política de Seguridad de la Información ha sido aprobada por resolución de la Dirección de SETEC ACUÁTICA, S.L. en fecha 24 de marzo de 2026 entrando en vigor desde ese momento. Es de obligado cumplimiento para todas las personas y terceros incluidos en su alcance.

La Política de Seguridad es aplicable en toda la organización y obligatoria para el personal, colaboradores, proveedores y terceros que tengan acceso a la información o sistemas de SETEC ACUÁTICA, S.L.


## 12. COMUNICACIÓN DE LA POLÍTICA

La efectividad de esta Política de Seguridad depende no solo de su correcta redacción y aprobación, sino también de su adecuada comunicación a todas las personas y entidades que deben cumplirla. El ENS establece que la Política debe ser conocida por todo el personal, con independencia de su rol, y por todos los terceros que tengan relación con el sistema de información. SETEC ACUÁTICA adopta un enfoque estructurado de comunicación que garantiza que la Política es accesible, comprensible y aplicable en todos los niveles de la organización.

## 13. REVISIÓN, ACTUALIZACIÓN Y MANTENIMIENTO DE LA POLÍTICA

La Política de Seguridad de SETEC ACUÁTICA, S.L. es un documento vivo que debe adaptarse a la evolución tecnológica, a los cambios organizativos, a la aparición de nuevas amenazas, a los resultados de auditorías y a las modificaciones en el marco normativo aplicable, especialmente en relación con el ENS y normativa afecta a la

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		

	POLITICA	POL
	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	
	Org.01-Art.12-POL-Política de Seguridad de Información Interna- PUB.docx	Página <b>20</b> de <b>20</b>

ciberseguridad. Por ello, la Política de Seguridad permanece vigente, eficaz y ajustada al contexto real de la organización, constituyendo una pieza clave en el ciclo de mejora continua del sistema corporativo.

Nº Edición	Fecha	Motivo
4	24/03/2026	Aprobación en Comité
3	23/12/2025	Se actualizan alcance, misión y visión
2	17/12/2025	Actualización Política Seguridad
1	13/12/2025	Creación Política Seguridad

ENS Real Decreto 311/2022	Clasificación del documento: USO PUBLICO	<b>SafeBeach</b>
	<b>SETEC ACUÁTICA S.L.</b> con CIF número B- 88276514	
<a href="https://www.safebeach.es">https://www.safebeach.es</a>		