## 1. OBJETO

El presente documento responde a la necesidad de ENSA de cumplir con los requisitos expresados en la legislación de seguridad de la información en servicios por medios electrónicos: el Real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad – ENS, así como con la normativa y principios de seguridad de la información aplicadas en la compañía.

La gestión de las TIC debe ser llevada a cabo aplicando las medidas necesarias que permitan garantizar la protección frente a las posibles incidencias (accidentales o deliberadas) que se puedan producir, de forma que se puedan minimizar las afectaciones sobre la disponibilidad, integridad o confidencialidad de la información relacionada con los servicios prestados.

La calidad de la información y la prestación continuada de servicios tendrán que ser garantizados actuando de forma preventiva, mediante una adecuada supervisión periódica y constante, teniendo como objetivo final la seguridad de la información como cultura general en la entidad.

De acuerdo con lo que se establece en el artículo 12 del Real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), la política de seguridad debe ser aprobada por el órgano competente y debe desarrollarse aplicando los siguientes requisitos mínimos, en proporción a los riesgos identificados en cada sistema:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión del personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención frente a otros sistemas de información interconectados.
l) Registro de la actividad y detección de código nocivo.
m) Incidentes de seguridad.

n) Continuidad de la actividad.

ñMejora continua del proceso de seguridad.

Por todo lo anteriormente expuesto, en este documento se define la política de seguridad de la información de ENSA.

Mediante la presente Política de Seguridad ENSA expresa su compromiso con la administración de la seguridad de su información, de acuerdo con los requerimientos propios, así como con las leyes y normativa vigente.

Esta política de seguridad de la información es efectiva desde la fecha de aprobación por el Consejo de Administración y hasta que sea reemplazada por una nueva política.

## 2. DEFINICIONES

**Información**. Todo documento que puede ser comunicado, presentado o almacenado en cualquier forma.

**Análisis de riesgos:** Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

**Datos personales:** Cualquier información concerniente a personas físicas identificadas o identificables.

**Gestión de incidentes:** Plan de acción para atender las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

**Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización en lo que respecta a los riesgos.

**Incidente de seguridad:** Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

**Política de seguridad:** Conjunto de directrices, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

**Principios básicos de seguridad:** Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

**Responsable de la información:** Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

**Responsable de la seguridad:** El responsable de seguridad debe determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

**Responsable del servicio:** Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

**Responsable del sistema:** Persona que se encarga de la explotación del sistema de información.

**Servicio:** Función o prestación ejercida por alguna entidad oficial destinado a cuidar intereses o satisfacer necesidades de los ciudadanos.

**Sistema de información:** Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, utilizar, compartir, distribuir, poner a disposición, presentar o transmitir.

## 3. ALCANCE

Esta política se aplica sobre el personal y los sistemas TIC (infraestructuras, software, comunicaciones...) que dan soporte a los servicios dentro del ámbito de aplicación del Esquema Nacional de Seguridad en ENSA.

## 4. MARCO LEGISLATIVO

El uso de las TIC por parte de ENSA se encuentra regulado por las siguientes normas jurídicas:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real decreto 4/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Interoperabilidad.
- Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de estos datos (RGPD).
- Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD)
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Instrucciones del Centro Criptográfico Nacional, CCN-STIC.

## 5. PRINCIPIOS DE CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD

Las TIC utilizadas por ENSA deben disponer de elementos que garanticen una protección adecuada contra amenazas que, debido a su constante evolución, tienen un gran

potencial para producir afectaciones en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios.

Con el objetivo de disponer de elementos para la defensa de estas amenazas, ENSA necesita contar con una estrategia que se adapte a los constantes cambios que se producen en el entorno para garantizar la prestación continua de los servicios. Esto implica que se deben aplicar las medidas mínimas de seguridad exigidas por el Real decreto 311/2022, de 3 de mayo, que regula el ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas; y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

ENSA debe garantizar que la seguridad TIC se convierta en un elemento integral del sistema, desde su diseño inicial hasta la retirada de servicio, pasando por las decisiones de desarrollo o adquisición de software y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación del área, en la solicitud de propuestas de servicios, y en la elaboración de los pliegos para la licitación de proyectos relacionados con las TIC.

Los procedimientos y normativas aplicables a los sistemas informáticos y organización informática se recogen en la Documentación del sistema de Gestión de Seguridad de la Información.

De acuerdo con lo dispuesto en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, se establecen los siguientes principios básicos:

a) Seguridad como proceso integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema de información.
b) Gestión de la seguridad basada en los Riesgos: El análisis y la gestión de riesgos sobre los servicios, la información y los sistemas definirá el despliegue de medidas de seguridad para un nivel de riesgo aceptable.
c) Prevención, detección, respuesta y conservación de los incidentes sobre los servicios y los sistemas de información. Cuando afecten a datos personales se analizará el impacto sobre la privacidad e intimidad de las personas afectadas.
d) Existencia de líneas de defensa: Establecimiento de medidas de protección de los servicios e información de ENSA.
e) Vigilancia continua: evaluación permanente de la seguridad de los activos que permita medir su rendimiento y detectar vulnerabilidades.

f) Reevaluación periódica: Las medidas de seguridad se evaluarán y actualizarán periódicamente para determinar su eficacia y modificarla de acuerdo con los riesgos detectados, la tecnología existente y las necesidades de ENSA.
g) Diferenciación de responsabilidades. Se diferencian a los diferentes responsables de gestión del sistema y de la seguridad del mismo, especialmente entre el responsable del sistema y el responsable de la seguridad.

La aplicación de estos principios se llevará a cabo con las medidas de seguridad definidas en el Real Decreto 311/2022, de 3 de mayo, los controles definidos por la ISO 27001 y – si implica tratamiento de datos personales – las medidas de seguridad base descritas en los artículos 24, 25 y 32 del RGPD, el análisis de riesgos y sobre los datos personales y – si procede – la evaluación de impacto del tratamiento, así como cualquier medida de seguridad para garantizar la seguridad de la información y datos personales de acuerdo.

## 5.1 DATOS DE CARÁCTER PERSONAL

ENSA, en el desarrollo de sus competencias, trata datos personales de su personal y de terceros, clientes y proveedores.

Los sistemas de información que traten datos personales tendrán que aplicar lo que dispone la normativa vigente en materia de protección de datos personales. Para ello, ENSA realizará un análisis de riesgos de acuerdo con lo definido en los artículos 24 y 32 del RGPD y, en su caso, una evaluación de impacto en la protección de datos de los tratamientos de la empresa y dará soporte en la evaluación de impacto de terceros en los que actúe como encargado de tratamiento.

Los sistemas de información de ENSA deben aplicar las medidas de seguridad resultantes de estos análisis, que prevalecerán si son más exigentes a las definidas por el Esquema Nacional de Seguridad.

## 5.2 GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta política deberán ser objeto de un análisis de riesgos, donde se evalúen las amenazas y riesgos a los que están expuestos.

Este análisis se llevará cuando se produzcan las siguientes circunstancias:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios en la información tratada.

- Cuando se produzcan cambios en los servicios prestados.
- Cuando se detecte una incidencia de seguridad grave.
- Cuando se detecten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, ENSA establecerá una valoración de referencia para los distintos tipos de información manejados y los distintos servicios prestados.

ENSA garantizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

## 5.3 PREVENCIÓN Y REACCIÓN FRENTE A INCIDENTES

El personal de ENSA debe disponer de los mecanismos para la prevención, detección, respuesta ante amenazas y conservación de los datos e información para minimizar las vulnerabilidades, evitar que las amenazas se materialicen y – en caso contrario – reaccionar ante posibles incidentes, de acuerdo con el artículo 8 y 25 del ENS, y el artículo 33 del RGPD si afecta a datos personales.

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, a fin de minimizar sus vulnerabilidades y conseguir que las amenazas sobre este no se materialicen o que, en caso de hacerlo, no afecten gravemente la información que maneja o a los servicios que presta.

Las medidas de prevención, que pueden incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a averiguar la presencia de un incidente de seguridad.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que puedan haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico, garantizando que su aplicación no suponga una reducción en la aplicación de los principios básicos y requisitos mínimos establecidos.

De la misma forma, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, mediante una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

## 6. ORGANIZACIÓN DE LA SEGURIDAD

### 6.1 FUNCIONES Y RESPONSABILIDADES

Los roles y funciones de la organización de la seguridad establecidos en el Esquema Nacional de Seguridad serán distribuídos de la siguiente manera:

- El Comité de Dirección de la empresa será quien ejerza las funciones de Responsable de la Información.
- El Comité de Dirección designará el Comité de Seguridad, que tendrá al menos cuatro miembros y que será el órgano encargado de coordinar y controlar las medidas definidas en esta Política de Seguridad
- Los Responsables de los Departamentos serán los Responsables del Servicio definidos por el ENS
- El Responsable de Servicios Informáticos será quien desempeñe las funciones de Responsable del Sistema definido por el ENS.

La Organización de seguridad y las funciones de los diferentes responsables para la gestión de la seguridad de la información en el ámbito del ENS de ENSA se describirán en un documento a aprobar por el Responsable de Información

El Comité de Dirección de ENSA deberá apoyar y dotar de los recursos necesarios al Comité de Seguridad de la Información y al Responsable de Servicios Informáticos de ENSA para poder llevar a cabo sus funciones. Asimismo, el Comité de Dirección se asegurará de incorporar en los planes de formación de la empresa las actuaciones necesarias para formar al personal sobre sus diferentes deberes, obligaciones y responsabilidades en materia de seguridad.

En caso de conflicto entre los diferentes responsables este deberá ser resuelto según los mecanismos definidos en cada ámbito o – en su defecto - por el superior jerárquico en la organización de seguridad, tal y como se defina en el documento que describa la organización de seguridad.

### 6.2 PROCEDIMIENTOS DE DESIGNACIÓN

El responsable de Seguridad y el Responsable de Sistema serán nombrados por el Consejo de Administración. El nombramiento se revisará cuando el puesto quede vacante o según determine el Comité de Dirección o el Consejo de Administración.

Si un servicio se desarrolla fuera del ámbito competencial del área de Tecnologías de la Información, el responsable del servicio que se preste electrónicamente deberá designar al Responsable del Sistema, previa autorización y validación expresa del Comité de Seguridad de la Información.

## 7. OBLIGACIONES DEL PERSONAL

Todos los miembros de ENSA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Responsable del Sistema que la información llegue a los afectados.

Todos los miembros de ENSA atenderán a una sesión de concienciación en materia de seguridad TIC cuando el Responsable de Seguridad lo estime necesario. Igualmente se establecerá un programa de concienciación continua para atender a todos los miembros de ENSA, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizarla. La formación es obligatoria antes de asumir una responsabilidad, ya sea su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Las obligaciones del personal se encuentran recogidas en el documento **POL-02 Política de Utilización de Sistemas Informáticos** en el uso de los sistemas de información.

## 8. TERCERAS PARTES

Cuando ENSA preste servicios a terceros o gestione información de terceros, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales por informe y coordinación de los respectivos Responsables de Seguridad y se establecerán procedimientos de actuación para la reacción frente a incidentes de seguridad.

Cuando ENSA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad que corresponda a estos servicios o información. Esta tercera parte quedará sujeta a las obligaciones establecidas en esta normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de informe y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

Cuando algún aspecto de la política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá

la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Estas obligaciones serán reguladas mediante acuerdo, convenio o contrato que defina la relación con los terceros, así como los criterios de nivel de servicio y los sistemas de control y monitorización del cumplimiento.

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

Esta política debe desarrollarse mediante normativa y procedimientos de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización, que deberán conocerla,.

Las modificaciones de esta política se llevarán a cabo por el mismo órgano que la aprueba. La normativa y procedimientos definidos en desarrollo de la misma serán aprobados por el Comité de Seguridad y difundidos para su conocimiento por todas las partes afectadas.

### 9.1 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para verificar que se cumple con todo lo que queda establecido en esta Política de Seguridad, se realizarán los controles internos que determine el Responsable de Seguridad (el Comité de Seguridad), en lo referente a los sistemas de información.

La periodicidad de estos controles será definida por el Comité de Seguridad, existiendo también la posibilidad de realizar otros controles que pueda determinar en función del desarrollo de las operaciones.

El objetivo de las auditorías será el de verificar la posibilidad de que los controles establecidos a través de las medidas de seguridad sean efectivos; y que sea posible garantizar la integridad, confidencialidad y disponibilidad de la información y servicios TIC.

Será misión del Responsable de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma.

## 10. HISTÓRICO DE REVISIONES

| Revisión | Fecha | Motivo |
|---|---|---|
| 0 | Fecha de firma | Edición inicial |
| | | |
| | | |
| | | |
| | | |