TMS Alicante

ALEATICA

ENS – ORG 1
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (EXTRACTO)

Propuesto por	GESPRODAT S.L	Fecha:05/2026
Revisado por:	Ignacio Daniel Saudi Rodriguez	Fecha: 05/2026
Aprobado por:	Andrés Romero Sánchez	Fecha: 05/2026
Alcance:	Política de seguridad de la información de TMS (Extracto)	
Clasificación del documento	Uso interno	

ÍNDICE

1. INTRODUCCIÓN

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece los principios básicos y requisitos mínimos para garantizar la seguridad de la información y de los servicios prestados mediante medios electrónicos.
De acuerdo con su artículo 12, toda organización que aplique el ENS debe contar con una Política de Seguridad de la Información formalmente aprobada por el órgano competente, conocida por todos los miembros de la organización y alineada con el marco legal aplicable, incluyendo el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.
La Política de Seguridad de la Información define los objetivos, responsabilidades, roles de seguridad, estructura de gobierno y directrices documentales necesarias para gestionar y proteger la información de la organización. Asimismo, sirve de base para implantar medidas técnicas y organizativas proporcionadas, seleccionadas conforme al análisis de riesgos y orientadas a reducir los riesgos a niveles aceptables.
El objeto de esta Política es garantizar una protección adecuada de la información, preservando los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, con independencia del formato en que se encuentre la información o del lugar desde el que sea tratada.

2. ALCANCE

La presente Política es aplicable a todos los activos de información incluyendo instalaciones, sistemas, servicios, software, bases de datos y toda la información almacenada o procesada en los sistemas informáticos.
Asimismo, deberán cumplir con la Política de Seguridad todas las personas que tengan acceso a la información objeto de alcance del Sistema de Gestión de Seguridad de la Información, y/o presten servicios para la Organización, incluso en el supuesto de que su relación no tenga carácter laboral.
Se aplicarán los principios básicos y los requisitos mínimos que se establecen en el ENS de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, que permita una protección adecuada de la información y los servicios.

3. MARCO NORMATIVO

Dentro del marco legal relativo a la seguridad de la información merecen especial mención las siguientes normas, regulaciones y estándares que serán objeto de verificación de su cumplimiento de forma periódica:

- En materia de sistemas de información:
  - ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
  - ✓ Guías CCN-STIC del CCN-CERT.

- ✓ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

- En materia de protección de datos de carácter personal:
  - ✓ 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 - RGPD).
  - ✓ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
  - ✓ Guías de la AEPD.
- Otras materias:
  - ✓ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
  - ✓ Real Decreto Legislativo 1/1996 (Ley de Propiedad Intelectual).
  - ✓ Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
  - ✓ Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

4. GESTIÓN DE RIESGOS

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.
Como metodología base para la realización de los análisis de riesgos se utilizará MAGERIT, siendo esta metodología la más recomendable.
El análisis se realizará:

- Regularmente, una vez al año.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

De acuerdo con la escala de riesgos de la metodología MAGERIT, el nivel de riesgo deberá situarse por debajo de nivel MEDIO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser BAJO). Valores de riesgo residual mayores a BAJO deberán ser aceptados explícitamente por el CSI, previa justificación de la conveniencia de su aceptación.

Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo a valores aceptables.

5. DATOS DE CARÁCTER PERSONAL

TMS solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

6. NOTIFICACIÓN DE INCIDENTES

De conformidad con los dispuesto en el artículo 33 del RD 311/2022, TMS notificara al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

7. MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.
Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

8. OBLIGACIONES DEL PERSONAL

Todo el personal de TMS, comprendido dentro del ámbito del ENS, atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al

menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.
Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

9. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la política de seguridad de la información corresponderá su resolución, en última instancia, a la Dirección de la Unidad de Negocio en su condición de máximo responsable de la Terminal.