TMS Alicante

ALEATICA

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

Propuesto por	GESPRODAT S.L	Fecha:05/2026
Revisado por:	Responsable de Sistemas	Fecha: 07/2026
Aprobado por:	Responsable de Seguridad	Fecha: 07/2026
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 (ENS), establece los principios básicos y requisitos mínimos necesarios para proteger adecuadamente la información tratada y los servicios prestados mediante sistemas de información.

La Política de Seguridad de la Información de TMS define las directrices, objetivos, responsabilidades y mecanismos de gobierno aplicables a la protección de la información. Las medidas técnicas y organizativas se seleccionan de manera proporcionada a la categoría del sistema y a los riesgos identificados.

La protección se orienta a preservar las siguientes dimensiones de seguridad:

- **Confidencialidad**: acceso a la información únicamente por personas autorizadas.
- **Integridad**: exactitud y ausencia de alteraciones no autorizadas.
- **Disponibilidad**: acceso a la información y a los servicios cuando resulten necesarios.
- **Autenticidad**: garantía de la identidad y del origen legítimo de la información.
- **Trazabilidad**: capacidad de atribuir y reconstruir las actuaciones realizadas.

2. ALCANCE

La Política es aplicable a los activos incluidos en el alcance del ENS de TMS, entre ellos instalaciones, sistemas, servicios, aplicaciones, bases de datos, redes, soportes y la información almacenada, transmitida o procesada.

Su cumplimiento es obligatorio para el personal propio y externo, proveedores, colaboradores y cualquier otra persona que acceda a los sistemas o a la información comprendidos en dicho alcance.

3. MARCO NORMATIVO

La Política se desarrolla conforme al marco legal y técnico aplicable, entre el que se incluyen:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Instrucciones Técnicas de Seguridad aplicables: Conformidad con el ENS, Informe del Estado de la Seguridad, Auditoría de la Seguridad de los Sistemas de Información y Notificación de Incidentes de Seguridad.
- Guías CCN-STIC publicadas por el Centro Criptológico Nacional.
- Directiva (UE) 2022/2555 (NIS2), en lo que resulte aplicable.

- Reglamento (UE) 2016/679, Ley Orgánica 3/2018 y demás normativa aplicable en materia de protección de datos, servicios de la sociedad de la información, propiedad intelectual, responsabilidad penal y protección de informantes.

4. PRINCIPIOS Y REQUISITOS MÍNIMOS DE SEGURIDAD

La seguridad se integra en la actividad ordinaria de TMS y se aplica desde el diseño y durante todo el ciclo de vida de los sistemas. La Política se fundamenta en los siguientes principios:

- **Alcance estratégico**: compromiso y apoyo de la Dirección.
- **Diferenciación de responsabilidades**: separación entre responsables de la información, de los servicios, de la seguridad y del sistema.
- **Proceso integral**: consideración conjunta de los elementos humanos, técnicos, físicos y organizativos.
- **Gestión basada en riesgos**: selección proporcionada de las medidas de protección.
- **Prevención, detección, respuesta y conservación**: protección anticipada, detección de anomalías, respuesta oportuna y recuperación.
- **Líneas de defensa**: aplicación de capas organizativas, físicas y lógicas.
- **Proporcionalidad**: adecuación de las medidas al impacto y a la criticidad.
- **Vigilancia continua y reevaluación periódica**: seguimiento de amenazas, vulnerabilidades y eficacia de los controles.
- **Seguridad por defecto**: configuraciones iniciales seguras y mínimos privilegios.
- **Protección de datos personales**: medidas adecuadas a los riesgos de los tratamientos.

La Política se desarrolla aplicando los requisitos mínimos de seguridad previstos en el ENS:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal y profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema., Protección de la información almacenada y en tránsito.
- Prevención ante sistemas interconectados.
- Registro de la actividad y detección de código dañino.
- Gestión y notificación de incidentes.

- Continuidad de la actividad y recuperación.
- Mejora continua del proceso de seguridad.
- Seguridad durante el ciclo de vida de los sistemas.
- Integración de la seguridad en la gestión de proyectos.

5. ORGANIZACIÓN DE LA SEGURIDAD

TMS dispone de una estructura organizativa para la gestión de la seguridad de la información, basada en la diferenciación de responsabilidades entre los Responsables de la Información y de los Servicios, el Responsable de Seguridad, el Responsable del Sistema y el Comité de Seguridad TIC. Estos roles coordinan la definición de los requisitos de seguridad, la gestión de riesgos, la implantación de medidas y la supervisión del cumplimiento del ENS.

6. CATEGORIZACIÓN DEL SISTEMA

Los sistemas de información incluidos en el alcance se categorizan de acuerdo con el Esquema Nacional de Seguridad, atendiendo al impacto que un incidente podría producir sobre la información tratada y los servicios prestados. La categorización se revisa periódicamente y cuando se producen cambios significativos en el sistema.

7. GESTIÓN DE RIESGOS

Los servicios, la información y los activos incluidos en el alcance se someten a un proceso de identificación, análisis, evaluación y tratamiento de riesgos. TMS utiliza MAGERIT como metodología base, complementada con los criterios y procedimientos internos que resulten necesarios.
El análisis de riesgos se revisará, al menos:

- Con periodicidad anual.
- Cuando cambien los servicios esenciales o las infraestructuras que los soportan.
- Después de un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas o vulnerabilidades graves no cubiertas adecuadamente.

Los riesgos residuales de nivel superior a Bajo requerirán aceptación expresa y justificada por el órgano competente. Cuando el riesgo no resulte aceptable, se establecerá el correspondiente plan de tratamiento.

8. DATOS DE CARÁCTER PERSONAL

TMS tratará únicamente los datos personales adecuados, pertinentes y limitados a las finalidades para las que hayan sido obtenidos. Se aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo y

preservar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento.

9. NOTIFICACIÓN DE INCIDENTES

TMS dispone de un procedimiento específico para el sistema ENS que regula la detección, registro, clasificación, análisis, escalado, resolución y notificación de los incidentes de seguridad, así como la conservación de las evidencias y la incorporación de las lecciones aprendidas.
Los incidentes se clasificarán conforme a la Instrucción Técnica de Seguridad de Notificación de Incidentes y a la Guía CCN-STIC 817. En su condición de entidad privada prestadora de servicios a entidades públicas, TMS comunicará los incidentes que le afecten al CSIRT de referencia, actualmente INCIBE-CERT, que los pondrá en conocimiento del CCN-CERT, sin perjuicio de las comunicaciones directas o adicionales que resulten exigibles según el servicio afectado, el contrato o la normativa aplicable.
Cuando el incidente afecte a datos personales se aplicarán, además, las obligaciones de notificación previstas en el Reglamento General de Protección de Datos.

10.MEJORA CONTINUA

La seguridad de la información se gestiona como un proceso de mejora permanente. TMS revisará y actualizará la Política, la valoración de la información y de los servicios, la categorización, el análisis de riesgos, las medidas de seguridad y la normativa interna.
La mejora continua se apoya, entre otras actuaciones, en:

- Revisiones periódicas y seguimiento de indicadores de seguridad.
- Auditorías internas y externas cuando procedan.
- Análisis de incidentes, vulnerabilidades y cambios significativos.
- Revisión de planes de tratamiento, continuidad y recuperación.
- Actualización de procedimientos conforme a la evolución normativa y tecnológica.

11.OBLIGACIONES DEL PERSONAL

Todo el personal comprendido en el alcance del ENS deberá conocer y cumplir la Política, las normas y los procedimientos de seguridad aplicables. TMS establecerá actividades periódicas de concienciación en seguridad y protección de datos, con especial atención al personal de nueva incorporación.

Las personas responsables del uso, operación o administración de los sistemas recibirán la formación necesaria antes de asumir sus funciones y cuando se produzcan cambios relevantes en su puesto o responsabilidades.

12.RESOLUCIÓN DE CONFLICTOS

Los conflictos entre los responsables que integran la estructura organizativa de seguridad serán tratados por el Comité de Seguridad TIC. Cuando no puedan resolverse dentro de dicho órgano, corresponderá su resolución a la Dirección de la Unidad de Negocio, como máximo responsable de la Terminal.