POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Grupo AISA

AUTOMNIBUS INTERUEBANOS S.A.
MOSAMO S.L.U.
IBÉRICA DE CONCESIONES Y SERVICIOS S.A.U.

Compromiso de la Dirección

La Dirección de AISA asume y promueve la aplicación del Esquema Nacional de Seguridad (ENS) - Real Decreto 311/2022 - en todos los sistemas de información que soportan los servicios de transporte público prestados por las empresas que forman el Grupo. Esta política es de obligado cumplimiento para todo el personal y proveedores de la organización.

1. MISIÓN Y ALCANCE

AISA tiene como misión ofrecer un servicio de transporte público seguro, cómodo y puntual, incorporando un modelo eficiente y sostenible que satisfaga las necesidades de movilidad de los usuarios.

Esta política es de aplicación a todos los sistemas TIC de la organización y a todas las personas vinculadas a servicios o proyectos destinados al sector público que requieran la aplicación del ENS.

2. OBJETIVOS DE SEGURIDAD

La Dirección establece los siguientes objetivos en materia de seguridad de la información:

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Prevenir incidentes de seguridad y mitigar los riesgos generados por las actividades de la organización.
- Asegurar la recuperación rápida y eficiente de los servicios ante cualquier contingencia.
- Proporcionar un marco de resiliencia para dar respuesta eficaz ante incidentes.
- Mejorar continuamente el sistema de seguridad de la información.

3. MARCO NORMATIVO APLICABLE

AISA desarrolla su actividad en cumplimiento del siguiente marco legal y regulatorio:

Norma	Descripción
RD 311/2022 (ENS)	Esquema Nacional de Seguridad — norma de referencia principal
RGPD 2016/679	Protección de datos personales y libre circulación de datos
LOPDGDD 3/2018	Protección de Datos Personales y garantía de derechos digitales
LSSI 34/2002	Servicios de la Sociedad de la Información
Ley 39/2015 y 40/2015	Procedimiento Administrativo y Régimen Jurídico del Sector Público
RDL 1/1996 / Ley 2/2019	Propiedad intelectual

4. ORGANIZACIÓN Y ROLES DE SEGURIDAD

La responsabilidad esencial recae en la Dirección General. El Comité de Seguridad TIC es el órgano con mayor responsabilidad en la toma de decisiones sobre seguridad de la información. Los roles formalmente definidos son:

Rol	Función principal
Responsable de Seguridad (RSEG/CISO)	Determinar idoneidad de medidas técnicas y supervisar el sistema ENS
Responsable del Sistema (RSIS)	Coordinar implantación y mejora continua del sistema
Responsable del Servicio (RSER)	Coordinar servicios y continuidad operacional
Responsable de la Información (RINFO)	Tomar decisiones sobre la información tratada
Dirección	Proporcionar recursos y liderazgo del sistema

5. PRINCIPIOS Y ÁREAS DE ACTUACIÓN

La política de seguridad se articula en torno a los siguientes principios y áreas de gestión:

Área	Compromisos de AISA
Gestión de riesgos	Análisis de riesgos al menos anual, revisado ante cambios significativos, incidentes graves o vulnerabilidades. Metodología documentada en el Comité de Seguridad TIC.
Control de acceso	Autenticación y autorización de usuarios, control de conexiones a redes externas y revisión de eventos críticos en los sistemas.
Seguridad del personal	Formación y concienciación anual obligatoria. Compromisos de confidencialidad para todo el personal y terceros.
Protección física	Perímetro de seguridad en áreas críticas, control de acceso físico, política de puesto y pantalla limpia.
Continuidad del servicio	Copias de seguridad y mecanismos de recuperación para garantizar la continuidad operativa.
Gestión de incidentes	Procedimientos de detección, clasificación, análisis, resolución y comunicación de incidentes. Registro para mejora continua.
Seguridad en adquisiciones	Los requisitos de seguridad TIC se integran en todo el ciclo de vida de sistemas y en los pliegos de contratación.
Seguridad por defecto	Los sistemas incorporan seguridad desde su diseño hasta su retirada, como proceso transversal e integral.
Terceros y cadena de suministro	Los proveedores quedan sujetos a esta política y a la normativa de seguridad aplicable. Se establecen cauces de reporte e incidencias.
Datos personales	Tratamiento conforme al RGPD y LOPDGDD, con acceso restringido a personas autorizadas.
Registros de actividad	Monitorización, análisis y registro de actividades de usuarios para detectar conductas indebidas y garantizar la trazabilidad.
Mejora continua	Proceso de mejora continua basado en criterios de ISO 27001, con revisiones periódicas del estado de seguridad.

6. OBLIGACIONES DEL PERSONAL

Todo el personal de Grupo AISA está obligado a:

- Conocer y cumplir esta Política de Seguridad y la Normativa de Seguridad vigente.
- Asistir a las sesiones de concienciación en seguridad TIC.
- Proteger las credenciales de acceso y no compartirlas con terceros.
- Notificar de forma inmediata cualquier incidente, anomalía o debilidad de seguridad detectada.
- Aplicar la política de puesto y pantalla limpia en las instalaciones.
- Firmar y respetar el Compromiso de Confidencialidad correspondiente a su función.

7. REPORTE DE INCIDENTES

Cualquier incidente o sospecha de incidente de seguridad debe comunicarse inmediatamente al Responsable de Seguridad (CISO) a través de los canales establecidos por el Comité de Seguridad TIC. Los incidentes se gestionarán conforme al procedimiento documentado, que contempla detección, clasificación, análisis, resolución y registro para la mejora continua del sistema.

8. VIGENCIA Y REVISIÓN

Esta Política de Seguridad de la Información es efectiva desde la fecha de aprobación (24 de junio de 2026) y estará vigente hasta que sea sustituida por una versión actualizada. Se revisará al menos una vez al año, o con carácter extraordinario ante cambios relevantes en el marco normativo, los sistemas o la organización.

El texto íntegro de la Política de Seguridad y la documentación normativa complementaria está disponible para el personal autorizado en el repositorio corporativo.