

POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS



POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS

1. Objetivo

Establecer las directrices para el uso adecuado, seguro y responsable de los medios tecnológicos de la organización, garantizando la confidencialidad, integridad y disponibilidad de la información, en conformidad con los principios y controles establecidos en la Norma ISO/IEC 27001 y su Anexo A.

2. Alcance

La presente política es de aplicación obligatoria para todos los colaboradores, directivos, contratistas, proveedores y terceros que tengan acceso a los medios tecnológicos y a la información de la empresa dedicada a la prestación de servicios de gestión de flotas y geolocalización de bienes móviles, incluyendo el tratamiento de la información asociada, así como el uso, desarrollo, mantenimiento y operación de las plataformas tecnológicas y sistemas de información que soportan dichos servicios.

Incluye, entre otros:

- Equipos informáticos (PC, portátiles, servidores).
- Dispositivos móviles (teléfonos, tabletas, GPS, IoT).
- Redes de comunicaciones y servicios en la nube.
- Aplicaciones, plataformas de geolocalización y sistemas de información.
- Medios de almacenamiento físicos y lógicos.

3. Marco normativo y de referencia

Esta política se alinea con:

- Norma ISO/IEC 27001 vigente.
- Norma ISO/IEC 27002 (buenas prácticas de seguridad de la información).
- Reglamento (UE) 2016/679, 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 (LOPDGDD).
- Legislación aplicable en materia de seguridad de la información y telecomunicaciones.
- Otras políticas internas del Sistema de Gestión de Seguridad de la Información (SGSI).

4. Principios generales

El uso de los medios tecnológicos deberá regirse por los siguientes principios:

- Uso profesional y autorizado.

POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS



- Necesidad de conocer y mínimo privilegio.
- Responsabilidad individual sobre los accesos y activos asignados.
- Protección de la información de clientes, usuarios y de la organización.
- Prevención de incidentes de seguridad de la información.

5. Uso aceptable de los medios tecnológicos

5.1 Los medios tecnológicos proporcionados por la organización deben utilizarse exclusivamente para fines laborales y en el marco de las funciones asignadas.

5.2 Se permite un uso personal mínimo, siempre que no interfiera con las actividades laborales, no comprometa la seguridad de la información ni infrinja esta política.

5.3 Está prohibido:

- Acceder, modificar o eliminar información sin autorización.
- Utilizar los sistemas para actividades ilegales, fraudulentas o no éticas.
- Instalar software, aplicaciones o dispositivos sin autorización del área responsable de TI.
- Desactivar o evadir controles de seguridad.

6. Gestión de accesos y credenciales

6.1 Cada usuario dispondrá de credenciales únicas e intransferibles.

6.2 Las contraseñas deberán cumplir con los requisitos definidos por la organización y no deberán ser compartidas.

6.3 El acceso a sistemas de gestión de flotas, plataformas de geolocalización y bases de datos estará limitado según el rol y funciones del usuario.

6.4 Los accesos serán revisados periódicamente y revocados cuando dejen de ser necesarios.

7. Uso de dispositivos y equipos

7.1 Los equipos asignados son responsabilidad del usuario.

7.2 Los dispositivos GPS, sensores IoT y equipos de geolocalización deberán utilizarse conforme a los procedimientos definidos y no podrán ser manipulados sin autorización.

7.3 En caso de pérdida, robo o daño de un equipo, el usuario deberá notificarlo de inmediato.

8. Uso de redes, internet y correo electrónico

POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS



8.1 El acceso a internet y a redes corporativas deberá realizarse a través de los mecanismos autorizados.

8.2 El correo electrónico corporativo es una herramienta de trabajo y no debe utilizarse para fines personales indebidos ni para el envío de información confidencial sin las protecciones adecuadas.

8.3 Está prohibido conectarse a redes no seguras sin las medidas de protección definidas por la organización.

9. Protección de la información

9.1 La información deberá ser clasificada y tratada de acuerdo con su nivel de sensibilidad y criticidad.

9.2 Se deberán aplicar medidas técnicas y organizativas apropiadas para garantizar la seguridad de la información de geolocalización, los datos de flotas y los datos personales de clientes, usuarios y empleados, conforme a lo establecido en el RGPD y la LOPDGDD.

9.3 El tratamiento de datos de geolocalización y otros datos personales se realizará únicamente para fines legítimos, explícitos y determinados, y estará limitado a lo necesario para la prestación de los servicios.

9.4 Está prohibida la copia, extracción, cesión o divulgación de información sin autorización expresa y sin base legal que lo habilite.

9.5 Los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición deberán ser garantizados conforme a la normativa vigente en materia de protección de datos personales.

10. Desarrollo y mantenimiento de sistemas

10.1 El desarrollo, mantenimiento y operación de plataformas tecnológicas se realizará siguiendo prácticas seguras y controles definidos por el SGSI.

10.2 Los cambios en los sistemas deberán ser autorizados, documentados y probados antes de su puesta en producción.

11. Monitoreo y registro

11.1 La organización podrá realizar actividades de monitoreo y registro del uso de los medios tecnológicos, conforme a la legislación aplicable.

11.2 Los registros serán utilizados exclusivamente para fines de seguridad, auditoría y mejora continua.

12. Incidentes de seguridad

POLÍTICA DE USO DE MEDIOS TECNOLÓGICOS



12.1 Todo usuario está obligado a reportar de inmediato cualquier incidente o sospecha de incidente de seguridad de la información.

12.2 Los incidentes serán gestionados conforme al procedimiento de gestión de incidentes del SGSI.

13. Concienciación y cumplimiento

13.1 Los usuarios deberán participar en actividades de concienciación y formación en seguridad de la información.

13.2 El incumplimiento de esta política podrá dar lugar a medidas disciplinarias, sanciones contractuales y/o acciones legales, según corresponda.

14. Revisión y actualización

La presente política será revisada periódicamente o cuando se produzcan cambios relevantes en la organización, en la tecnología o en los requisitos legales y normativos.

15. Aprobación y vigencia

Esta política entra en vigor a partir de su aprobación por la Dirección y es de cumplimiento obligatorio para todas las partes incluidas en su alcance.

Madrid, a 02 de febrero de 2026

Fdo.: La dirección



CIF - ESBZ0950465