GRUPO ARI

SGSI.01.Política de Seguridad

Autores	Responsable documento	Aprueba documento	Clasificación
Responsable Seguridad (BMR)	Dirección IT (JLMV)	Dirección General (FGA)	PÚBLICO

Registro versiones			
VERSIÓN	FECHA	AUTORES	DESCRIPCIÓN
1	12/05/2025	BMR	Edición Inicial documento
2	10/07/2025	BMR	Actualización general
3	16/09/2025	BMR	Revisión, se obvia el apartado de normativa aplicable
4	25/09/2026	BMR	Revisión anual.

1. Introducción

La presente Política de Seguridad de la Información establece el marco general para preservar la confidencialidad, integridad y disponibilidad de la información en **ARIMOTOR GESTIÓN, S.L. (GRUPO ARI).** La información es uno de los principales activos de la compañía, al igual que las aplicaciones de gestión (DMS) y los sistemas que sustentan los procesos del negocio. Es esencial garantizar su adecuada protección frente a amenazas y riesgos, en cumplimiento de los requisitos legales y contractuales y del compromiso corporativo con la mejora continua, la excelencia, la sostenibilidad y el cumplimiento ético.

La Seguridad de la Información es entendida como el proceso destinado a proteger la información durante todo su ciclo de vida, mediante la implementación, operación y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con ISO 27001.

La Dirección General de GRUPO ARI, plenamente consciente del valor de la información y del impacto de cualquier incidente, se compromete formalmente y exige el cumplimiento de esta Política a todas las personas y partes con acceso a los activos de información.

2. Ámbito, Aprobación, Vigencia, Revisión

Esta Política se aplica a todo el ámbito de actuación de todas las empresas que conforman el **Grupo Ari**:

- Ari Ocasión S.L.U.
- Arima Motor Canarias S.L.U.
- Arimotor Canarias S.L.

- Arimotor Gestión S.L.
- Arimotor Tenerife S.L.
- Brisa Motor S.L.U.
- Izquier 2018 S.L.
- Izquier & Izquier S.L.
- Motor Ari S.A.

La presente política ha sido aprobada por la Dirección General, estableciendo de esta forma las directrices generales en relación con su objeto. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación.

La vigencia de las versiones anteriores que hayan podido distribuirse queda anulada por la última versión de esta política.

3. Definiciones

- **SGSI:** Sistema de Gestión de Seguridad de la Información diseñado conforme a ISO 27001 para implantar, operar, supervisar, revisar y mejorar los controles de seguridad aplicables a la información.
- **Activo de información:** Cualquier dato, sistema, persona o recurso relevante para la Organización.
- **Activo o sistema crítico:** Activo sin el cual los procesos de negocio principales de la empresa se ven gravemente afectados.
- **Sistema de Información:** Conjunto estructurado de recursos (aplicaciones, hardware, personas, procedimientos, etc.) para gestionar información relevante para la organización.
- **Usuario:** Toda persona o entidad con acceso a recursos informáticos de la empresa.
- **Datos personales/categoría especial:** Aquellos protegidos por RGPD, susceptibles de identificación de individuos; incluyen datos de salud, financieros, biométricos, localización, etc.
- **Confidencialidad:** Garantía de que la información solo es accesible a quienes estén autorizados.
- **Integridad:** Salvaguarda de la exactitud, completitud y validez de la información propiamente almacenada/procesada/a disposición.
- **Disponibilidad:** Aseguramiento de que la información y los sistemas estén disponibles cuando se necesiten.
- **Evento de seguridad:** cualquier detección o evento relacionado con la seguridad de la información, objeto de estudio por el Dpto. de Seguridad.
- **Incidente de seguridad:** Suceso que afecta/confirma la pérdida de confidencialidad, integridad o disponibilidad de la información.
- **Riesgo:** Probabilidad de materialización de una amenaza sobre un activo, causando daño o impacto en la organización.
- **Gestión de riesgos:** Conjunto de actividades para identificar, analizar, evaluar, tratar y monitorizar los riesgos para la información y los procesos.
- **Zonas restringidas:** CPD, salas de servidores, áreas técnicas críticas.
- **Zonas de acceso público:** Exposiciones de venta, zonas de atención al cliente, etc.

- **Zonas de acceso controlado:** Resto de zonas de la organización.
- **Sistema de Inteligencia Artificial (SIA):** Sistema basado en máquinas diseñado para operar con distintos niveles de autonomía y que puede mostrar adaptabilidad tras el despliegue, para generar salidas como contenidos, predicciones, recomendaciones o decisiones.
- **IA Generativa:** Tipo de SIA (ej. ChatGPT, Copilot, Midjourney) capaz de crear textos, imágenes, código o datos nuevos a partir de peticiones (prompts).
- **Shadow AI (IA en la sombra):** Uso de herramientas de IA por parte de los empleados para tareas laborales sin la aprobación o el conocimiento explícito del departamento de IT.

4.Propósito

El propósito de esta Política es proteger los activos de información de GRUPO ARI ante amenazas internas y externas, deliberadas o accidentales, garantizando:

Confidencialidad, integridad y disponibilidad de la información en todas sus formas y ciclos de vida.

Cumplimiento de todos los requisitos legales, regulatorios y contractuales aplicables.

Apoyo a la continuidad del negocio y a los objetivos estratégicos de la compañía.

Mantenimiento de la confianza de clientes, fabricantes, proveedores y resto de partes interesadas.

5. La Empresa. Misión, Contexto y Alcance

5.1. Sobre Grupo ARI

GRUPO ARI es un referente empresarial canario, con más de medio siglo de experiencia multisectorial y consolidado como líder regional en automoción, a través de la representación de marcas internacionales y el desarrollo de servicios avanzados de gestión, recambios y electromovilidad.

5.2. Importancia crítica de los sistemas de gestión

El desarrollo y mantenimiento de aplicaciones de gestión (DMS) y demás soluciones asociadas a los procesos de negocio (ventas, posventa, recambios, integración con fabricantes, etc.) constituye un pilar estratégico esencial, tanto por su aportación sistemática a la excelencia operativa y de servicio, como por la custodia de datos sensibles y estratégicos de clientes, fabricantes, socios y empleados.

5.3 Consideración del Cambio Climático en el SGSI

Se evaluarán periódicamente los riesgos derivados del cambio climático que puedan afectar a la seguridad de la información y a la continuidad operativa, integrándolos en la gestión del SGSI

5.4. Alcance del SGSI

El **Sistema de Información** que soporta los procesos de:

- **Mantenimiento y soporte** informático al usuario, requerido por las aplicaciones de gestión para automoción.
- **Desarrollo y mantenimiento** de aplicaciones de gestión para automoción (**SARIX** DMS).
- **Servicios integrales de gestión** empresarial vinculados.

de acuerdo a la declaración de aplicabilidad vigente.

6. Principios y Objetivos de la Seguridad de la Información

6.1 Principios fundamentales:

- **Confidencialidad:** Solo acceden a la información personas autorizadas.
- **Integridad:** La información y los sistemas se mantienen exactos, completos y sin alteraciones indebidas.
- **Disponibilidad:** Los sistemas y la información estén accesibles y operativos cuando se requiera.
- **Gestión proactiva del riesgo:** La seguridad se gestiona de modo proporcional a los riesgos evaluados del negocio y el entorno.
- **Cumplimiento:** Respeto estricto de los requerimientos legales, regulatorios y contractuales.
- **Concienciación, formación y cultura de seguridad:** Promoción activa de buenas prácticas y de la responsabilidad individual en seguridad.
- **Mejora continua:** Adaptación sistemática del SGSI y sus controles a los cambios en el contexto, la amenaza y la tecnología.

6.2 Objetivos específicos:

- Proteger los sistemas y aplicaciones de gestión (DMS) ante amenazas a la confidencialidad, integridad y disponibilidad.
- Garantizar la calidad y la resiliencia de los servicios informáticos y tecnológicos.
- Cumplir la normativa vigente, incluida LOPDGDD, RGPD y demás leyes sectoriales aplicables.
- Prevenir, detectar y responder de manera eficaz ante incidentes de seguridad.
- Mantener y revisar de manera continua los mecanismos de seguridad implantados.
- Asegurar la formación y concienciación del personal y usuarios con acceso a los activos de información.
- Velar por la seguridad de la información propia, la de los clientes, fabricantes y del resto de partes interesadas.
- Considerar los riesgos relacionados con el cambio climático en el análisis del contexto y en la planificación de la seguridad de la información, fortaleciendo la resiliencia del SGSI frente a posibles impactos medioambientales
- Desarrollar y consolidar un marco de Alfabetización en Inteligencia Artificial (AI Literacy) que capacite al personal en la comprensión del funcionamiento básico, los sesgos y el uso ético y seguro de estas tecnologías en el sector de la automoción.

- Garantizar la seguridad por defecto y desde el diseño en todas las fases del ciclo de vida del desarrollo de software propio (como SARIX DMS) y en la adquisición de nuevas plataformas tecnológicas.

7. Requisitos y Directrices Generales de Seguridad

- El acceso a los sistemas estará controlado, monitorizado y limitado al personal y terceros autorizados.
- Los proyectos de desarrollo, implantación y mantenimiento de aplicaciones de gestión (DMS) integrarán la seguridad durante todo su ciclo de vida.
- La información será clasificada y protegida de acuerdo con su criticidad y sensibilidad, según procedimientos internos.
- Se adoptarán medidas de respaldo y de continuidad para servicios críticos, asegurando la recuperación ante contingencias graves.
- Todas las personas con acceso a la información estarán debidamente informadas de sus responsabilidades y formadas en seguridad.
- Los proveedores y socios que accedan a información o sistemas cumplirán los estándares exigidos contractualmente.
- Se analizarán, valorarán y tratarán los riesgos de manera recurrente, documentando el nivel de exposición residual aceptado por la Dirección.
- La gestión de incidentes estará soportada por procedimientos de notificación, análisis y respuesta rápida, garantizando el aprendizaje y la mejora.
- Se establecerán mecanismos de segregación de funciones para evitar que una misma persona pueda autorizar, ejecutar y auditar procesos críticos o modificaciones estructurales en los sistemas de información de manera unilateral.
- Las relaciones y contratos con terceros, proveedores y partners tecnológicos incluirán explícitamente la obligatoriedad de adherirse a los niveles de exigencia, confidencialidad y control establecidos por el Grupo Ari.
- El uso, despliegue o integración de Sistemas de Inteligencia Artificial (SIA) estará regulado por un marco estricto de control de riesgos, prohibiéndose el uso de tecnologías que comprometan los derechos de las personas y garantizando siempre la supervisión humana en cualquier toma de decisión automatizada.
- El cumplimiento de la política y las normas asociadas será supervisado periódicamente, gestionando los incumplimientos conforme a las disposiciones internas y legales aplicables.
- La adecuación de la política y del SGSI se revisará y actualizará periódicamente, particularmente tras hechos relevantes, cambios normativos o evolución tecnológica.

8. Roles, Responsabilidades y Autoridades

Director General:

Máxima autoridad, asume formalmente la responsabilidad sobre los activos de información, adquiere el compromiso de dotar de los recursos adecuados, aprobar y revisar la presente política y los objetivos de seguridad, así como supervisar los riesgos y el cumplimiento del SGSI.

Director de IT:

Responsable de la gestión, operación, mantenimiento y evolución de las infraestructuras tecnológicas y los sistemas que dan soporte al SGSI y a las aplicaciones de negocio. Supervisa directa y funcionalmente al Responsable de Seguridad.

Responsable de Seguridad:

Persona designada para coordinar el despliegue del SGSI, asegurar el cumplimiento de la política y los procedimientos, informar y asesorar a la Dirección sobre el estado y las necesidades de seguridad, y proponer las acciones correctivas o de mejora oportunas. Dirige el análisis de riesgos, la monitorización de controles, la gestión de incidentes y la concienciación en seguridad. Asimismo, actuará como supervisor y punto de contacto para la gobernanza, validación de riesgos y cumplimiento normativo de los Sistemas de Inteligencia Artificial utilizados en la organización.

Usuarios (personas con acceso a sistemas y datos del alcance):

Toda persona que acceda a los sistemas, aplicaciones o información asume la obligación de cumplir esta política y las normas derivadas, proteger la información, reportar incidentes o sospechas y tratar con máxima diligencia los activos de información.

9. Revisión, comunicación y actualización

La presente Política de Seguridad de la Información será revisada al menos una vez al año, o en cualquier momento en que cambios en el negocio, incidentes relevantes, auditorías u obligaciones legales así lo requieran.

El Responsable de Seguridad redactará propuestas de revisión y elevará a la Dirección General para su aprobación.

Toda actualización será debidamente comunicada a empleados y partes interesadas.

10. Vigencia, aplicación y cumplimiento

Esta política es de aplicación obligatoria para todo el personal, proveedores y terceros que accedan, traten o gestionen activos de información de GRUPO ARI contenidos en el alcance del SGSI.

El incumplimiento de la presente política, así como de las normas y procedimientos derivados de ella, será considerado una desviación de las obligaciones laborales o contractuales y podrá ser sancionado conforme a la normativa interna de la organización, los convenios colectivos de aplicación, el Estatuto de los Trabajadores y las disposiciones legales vigentes, sin perjuicio de las responsabilidades civiles o penales que correspondan.

> **La presente Política entra en vigor tras su difusión por la Dirección General. Toda persona, sistema o proceso bajo su ámbito de aplicación está obligado a su cumplimiento.**