



R3-GZPSI-002 INFORMATION SECURITY POLICY STATEMENT

R3-GZPSI-002

REV. 2
ISSUE 2

R3-GZPSI-002 INFORMATION SECURITY POLICY STATEMENT

R3-GZPSI-002 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Público

ELABORADO POR CREATED BY	REVISADO POR REVIEW BY	APROBADO POR APPROVED BY
Nombre / Name: Hard2bit S.L. Cargo / Post: Compliance and Implementation Consultancy Fecha / Date: 21/01/2026	Nombre / Name: Hard2bit S.L. Cargo / Post: Hard2bit Point of Contact Fecha / Date: 21/01/2026	Nombre / Name: Comité de Seguridad, Protección de Datos y Crisis Cargo / Post: N/A Fecha / Date: Ver acta de Comité



INDICE

0	OBJETIVO	4
1	ALCANCE	4
2	MARCO DE REFERENCIA	5
3	MARCO PARA EL ESTABLECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN	6
4	CUMPLIMIENTO.....	8
5	REVISIÓN Y MEJORA	8

TABLE OF CONTENTS

0.	OBJECTIVE.....	4
1.	SCOPE	4
2.	REFERENCE FRAMEWORK	5
3.	FRAMEWORK FOR ESTABLISHING INFORMATION SECURITY.....	6
4.	COMPLIANCE	8
5.	REVIEW AND IMPROVEMENT.....	8

Público



R3-GZPSI-002 INFORMATION SECURITY POLICY STATEMENT

R3-GZPSI-002

REV. 2
ISSUE 2

VERSION CONTROL

Revisión Issue	Fecha Date	Modificación Modification	Elaborado por: Created by:	Revisado por: Review by:	Aprobado por: Approval by:
1	27/11/2021	Se crea el documento. The document is created.	GAZC	GAZC	GAZC
2	21/01/2026	Se actualiza el documento con base a los requisitos de la ISO/IEC 27001. Document updated in accordance with ISO/IEC 27001 requirements.	Hard2bit SL.	Hard2bit SL.	GAZC

Público



R3-GZPSI-002 INFORMATION SECURITY POLICY STATEMENT

R3-GZPSI-002

REV. 2
ISSUE 2

0 OBJETIVO

El objetivo de la presente Política de Seguridad de la Información es establecer el marco de actuación necesario para proteger los activos de información, tanto propios como de las partes interesadas, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de preservar su confidencialidad, integridad y disponibilidad.

Asimismo, esta política tiene como finalidad asegurar la adecuada gestión de los riesgos de seguridad de la información, considerando su posible impacto en la seguridad de la aviación civil, en la continuidad de las operaciones y en el cumplimiento de los requisitos legales y regulatorios aplicables.

1 ALCANCE

La presente Política de Seguridad de la Información es de aplicación a todas las empresas del grupo GAZC, incluidas:

- Grupo Aeronáutico Zona Centro S.A.
- GAZC Tratamientos Superficiales S.L.
- GAZC Sevilla S.L.
- GAZC Aeroestructuras Integrales S.L.

0. OBJECTIVE

The purpose of this Information Security Policy is to establish the framework required to protect information assets, both those of the organization and those of its interested parties, against internal or external threats, whether deliberate or accidental, in order to preserve their confidentiality, integrity, and availability.

Furthermore, this policy aims to ensure the proper management of information security risks, considering their potential impact on civil aviation security, operational continuity, and compliance with applicable legal and regulatory requirements

1. SCOPE

This Information Security Policy applies to the entire GAZC Group, including the following:

- Grupo Aeronáutico Zona Centro S.A.
- GAZC Tratamientos Superficiales S.L.
- GAZC Sevilla S.L.
- GAZC Aeroestructuras Integrales S.L.



R3-GZPSI-002 INFORMATION SECURITY POLICY STATEMENT

R3-GZPSI-002

REV. 2
ISSUE 2

Esta política resulta de obligado cumplimiento para todo el personal, directivos, colaboradores y terceros que tengan acceso a la información, a los sistemas de información o a los servicios prestados por el grupo.

El alcance de esta política comprende toda la información gestionada por la organización, con independencia de su origen, formato, soporte o medio de transmisión, así como los activos, sistemas, procesos y servicios que la soportan.

Asimismo, la política es aplicable a todas las actividades relacionadas con la gestión, uso, almacenamiento, tratamiento, transmisión y destrucción de la información, tanto en entornos internos como externalizados, y durante todo el ciclo de vida de la información.

2 MARCO DE REFERENCIA

Se establece conforme a los principios y requisitos definidos en la norma ISO/IEC 27001, así como a la normativa legal y regulatoria aplicable, incluyendo, cuando proceda, los requisitos específicos del sector aeronáutico.

This policy shall be complied with by all personnel, management, collaborators, and third parties who have access to the Group's information, information systems, or services. The scope of this policy covers all information managed by the organization, regardless of its origin, format, medium, or means of transmission, as well as the assets, systems, processes, and services that support it.

Furthermore, this policy applies to all activities related to the management, use, storage, processing, transmission, and disposal of information, both in internal and outsourced environments, throughout the entire information lifecycle.

2. REFERENCE FRAMEWORK

This Information Security Policy is established in accordance with the principles and requirements defined in the ISO/IEC 27001 standard, as well as the applicable legal and regulatory framework, including, where applicable, the specific requirements of the aeronautical sector.

3 MARCO PARA EL ESTABLECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información del grupo se rige por los siguientes principios fundamentales:

- Protección de la confidencialidad, integridad y disponibilidad de la información.
- Gestión sistemática y continua de los riesgos de seguridad de la información.
- Prevención, detección y respuesta eficaz ante incidentes de seguridad.
- Mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Cumplimiento de los requisitos legales, regulatorios y contractuales aplicables.

Los objetivos del Sistema de Gestión de la Seguridad de la Información (SGSI) se definirán, revisarán y mantendrán conforme a los siguientes principios:

- Los objetivos del SGSI estarán alineados con la estrategia, misión y objetivos de negocio del grupo.
- Los objetivos se establecerán considerando los resultados del análisis y tratamiento de riesgos de seguridad de la información.

3. FRAMEWORK FOR ESTABLISHING INFORMATION SECURITY

Information security within the Group is guided by the following fundamental principles:

- Protection of the confidentiality, integrity, and availability of information.
- Systematic and continuous management of information security risks.
- Prevention, detection, and effective response to security incidents.
- Continuous improvement of the Information Security Management System (ISMS).
- Compliance with applicable legal, regulatory, and contractual requirements.

The objectives of the Information Security Management System (ISMS) shall be defined, reviewed, and maintained in accordance with the following principles:

- The objectives of the Information Security Management System (ISMS) shall be aligned with the Group's strategy, mission, and business goals.
- Objectives shall be established taking into account the results of information security risk analysis and risk treatment.



R3-GZPSI-002 INFORMATION SECURITY POLICY STATEMENT

R3-GZPSI-002

REV. 2
ISSUE 2

- Los objetivos deberán contribuir a garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se considerará de forma específica el posible impacto de los riesgos de seguridad de la información en la seguridad de la aviación civil, priorizando aquellos objetivos que mitiguen riesgos con efectos directos o indirectos sobre la misma.
- Los objetivos del SGSI tendrán en cuenta los requisitos legales, regulatorios, contractuales y sectoriales aplicables.
- Los objetivos deberán apoyar la continuidad de los sistemas de información y de los servicios críticos del grupo.
- Los objetivos del SGSI promoverán la mejora continua de los controles, procesos y capacidades de seguridad de la información.
- Los objetivos deberán ser medibles, alcanzables y sujetos a seguimiento mediante indicadores definidos.
- Los objetivos asignarán responsabilidades claras y fomentarán la concienciación y capacitación del personal en materia de seguridad de la información.
- Los objetivos se definirán de forma proporcional al nivel de riesgo y al contexto de la organización, garantizando un uso eficiente de los recursos.

- Objectives shall contribute to ensuring the confidentiality, integrity, and availability of information.
- Specific consideration shall be given to the potential impact of information security risks on civil aviation safety, prioritizing objectives that mitigate risks with direct or indirect effects on it.
- ISMS objectives shall take into account applicable legal, regulatory, contractual, and sector-specific requirements.
- The objectives shall support the continuity and resilience of the Group's information systems and critical services.
- ISMS objectives shall promote the continuous improvement of information security controls, processes, and capabilities.
- Objectives shall be measurable, achievable, and subject to monitoring through defined indicators.
- Objectives shall assign clear responsibilities and promote awareness and training of personnel in information security.
- Objectives shall be defined proportionately to the level of risk and the organizational context, ensuring efficient use of resources.

In this regard, Top Management expresses its commitment to the establishment, implementation, maintenance, and continual improvement of the Information Security Management System (ISMS).



R3-GZPSI-002 INFORMATION SECURITY POLICY STATEMENT

R3-GZPSI-002

REV. 2
ISSUE 2

En este sentido, la Alta Dirección manifiesta su compromiso con el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

4 CUMPLIMIENTO

El incumplimiento de esta política podrá dar lugar a la adopción de las medidas disciplinarias, contractuales o legales que correspondan, de acuerdo con la normativa vigente y los procedimientos internos del grupo.

5 REVISIÓN Y MEJORA

La presente Política de Seguridad de la Información será revisada al menos una vez al año, o cuando se produzcan cambios significativos en la organización, en los riesgos, en los servicios prestados o en el marco normativo aplicable, con el fin de asegurar su adecuación, eficacia y alineación con los objetivos estratégicos del grupo.

4. COMPLIANCE

Non-compliance with this policy may result in disciplinary, contractual, or legal actions, in accordance with applicable legislation and the Group's internal procedures.

5. REVIEW AND IMPROVEMENT

This Information Security Policy shall be reviewed at least once a year, or whenever significant changes occur within the organization, in the risk landscape, in the services provided, or in the applicable regulatory framework, in order to ensure its continued adequacy, effectiveness, and alignment with the Group's strategic objectives.