I. OBJECTIVE

Establish the Information Security and Business Continuity Policy within Grupo Industrial Saltillo, S.A.B. de C.V. (GIS).

II. SCOPE

This Policy is generally applicable to all companies that are part of GIS.

III. POLICY DESCRIPTION

1. Information Security Framework

For the proper management of information security, GIS bases this policy on the ISO/IEC 27001, TISAX, and NIST CSF standards as its reference framework.

2. Information Security Objectives

GIS protects the confidentiality, integrity, and availability of its own information, as well as that of customers and authorized third parties under its management. It also ensures the continuity of its operational and business processes, managing risks at an acceptable level and implementing controls based on security best practices, while complying with applicable regulatory, legal, and contractual requirements.
GIS develops, implements, maintains, and continuously improves its Information Security Management System (ISMS).

IV. INFORMACIÓN INFORMATION SECURITY GOVERNANCE MODEL

The Information Security Governance Model is based on the Information Security Management System (ISMS), whose objectives, in relation to information security, are as follows:

1. **Identify** risks systematically.
2. **Protect against threats** through the development and implementation of applicable security technologies.
3. **Detect threats** by leveraging multiple sources of intelligence to proactively manage them.
4. **Respond** to cybersecurity incidents through corporate protocols by:
a) Limiting their impact on the company.
b) Ensuring the continuity of operations that depend on IT services.
5. **Recover and restore** any capability or service that has been affected due to a cybersecurity event.

V. USE OF INFORMATION

Each employee must have access only to the information necessary to perform their job, and no unauthorized person should be able to access it.

The information and the assets used to safeguard it exist to fulfill business objectives and must be used solely for that purpose.

VI. INFORMATION PROTECTION

Employees must understand and apply the guidelines established by GIS for the protection of information.

VII. INFORMATION RESTRICTION

Employees, customers, and authorized third parties must have access only to the information strictly necessary to perform the activities related to their assigned tasks.

VIII. INFORMATION DISCLOSURE

Access to confidential or restricted information granted to GIS employees does not confer authority to allow access to third parties inside or outside GIS, nor to disclose such information to any person.

IX. SANCTIONS

Any violation of the principles of this Policy, as well as of the related guidelines or procedures, will result in the application of disciplinary measures in accordance with the current GIS Code of Ethics.

X. GLOSSARY OF TERMS

Concept	Definition
Information Asset	It is the information itself that has value for our organization and must be protected in any format (digital, paper, audio, video, etc.). Its loss, alteration, or unauthorized disclosure may affect the confidentiality, integrity, or availability of the information, which in turn could significantly impact the company. The value of information arises, among other factors, from the economic benefit or legal commitment (for example, due to laws or customer contracts) that the information creates in a given situation, as well as from the costs incurred to protect it. Examples: Databases: Production data, supplier information, user or customer data, etc. Documents: Contracts, procedure manuals, internal policies, reports (digital or physical), product designs, customer lists, trade secrets, financial reports, business strategies. Intellectual Property: Source code, algorithms.

	Communications: Emails, instant messages containing valuable information.
Supporting Asset	A resource that stores, processes, or transports information assets, or enables their use — such as hardware, software, networks, locations/facilities, personnel, internal and third-party services, and physical media, among others. VDA ISA 6.0.x / TISAX defines them as follows: "Supporting assets (electronic and physical) are used to store, process, and transport information assets." Why distinguish between an Information Asset and a Supporting Asset? Risk orientation: The impact is assessed on the information asset; supporting assets inherit or contribute to the risk due to their relationship with the information. Appropriate controls: Technical and organizational controls must be directed to the correct support, for example: database encryption, access control in SaaS (Software as a Service), or hardening of PLCs (Programmable Logic Controllers). Traceable audit evidence: Facilitates demonstrating that the classification, ownership, and security measures are aligned with the value of the asset and its support chain.
Logical Access	The act of accessing information stored within an Information System.
Threat	A potential cause of an unplanned incident, which may result in damage to the Information Asset.
Availability	The assurance that information is accessible and usable upon demand by an authorized entity.
Information	Data that holds meaning. It includes databases, data files, contracts and agreements, system documentation, research information, user manuals, training materials, operational or support procedures, business continuity plans, audit evidence, archived information, among others.
Security Incident	An Information Security Incident is an event in which a threat materializes by exploiting a vulnerability, causing an impact on one or more information properties of an information asset, which may include:

	• Integrity • Availability • Confidentiality
Integrity	Assurance of the accuracy and completeness of information and the methods used for its processing.
Risk	The consequence of a threat in relation to an information asset.
Information Security	The preservation of confidentiality, integrity, and availability of information.
ISMS (Information Security Management System)	A management system for establishing, implementing, maintaining, and continuously improving information security.
Information Technology (IT)	Technology required for the acquisition, storage, manipulation, management, control, exchange, transmission, reception, processing, analysis, or display of data or information. It includes computer equipment, communication systems, auxiliary devices, commercial or in-house software, and related services and resources, whether purchased, leased, or under the responsibility of the Company.
Third Party	An employee or representative of an organization other than GIS.
Collaborator	A person or entity that uses or requires access to an information system to perform one or more tasks. The user may be an employee or a third party (such as a supplier, consultant, or external user).

XI. RELATED POLICIES AND PROCEDURES

1. GIS-SEG-002 Clasificación, Administración, Respaldo y Recuperación de la Información
2. GIS-SEG-002 – Classification, Management, Backup, and Recovery of Information
3. GIS-SEG-003 – Access Control to Information Technology Systems
4. GIS-SEG-004 – Remote Access Control to GIS Infrastructure
5. GIS-SEG-005 – Assignment and Use of Passwords
6. GIS-SEG-006 – Use of Email Service
7. GIS-SEG-007 – Use of Internet Browsing
8. GIS-PROC-SEG-001 – Classification, Labeling, and Handling of Information

This Policy was approved by the Information Security Committee in its session held on January 19, 2023.

This Policy was ratified by the Information Security Committee in its session held on February 18, 2025.

This Policy was ratified by the Information Security Committee at its session held on November 25, 2025, and remains effective for the year 2026.