






# Information Security Policy

In **Gestamp Technology and Innovation Office (TIO)**, we are constantly working to become an Innovating leader in automotive sector. We make every effort to research and to develop innovative designed products and trendsetting technologies.

**Gestamp TIO**, is committed to maintaining the necessary measures to ensure that the product and technology knowledge of Gestamp and our Clients is safely preserved in our organization.

The basic principles of **Gestamp TIO's** Information Security Policy are:

-  **Information Security, a strategic goal in our company.** The protection and secure use of information assets are priorities in our organization for ensuring supply chain and business continuity processes, as defined in the Policy General Information Security of Gestamp Automoción, S.A. Protection is focused on maintaining the confidentiality of information as the main feature, and integrity and availability as additional features, following the VDA-ISA standard.
-  **Protection and secure use of information assets to enable sharing of information.** It is the organization's policy that the information assets are appropriately secured both in internal use and in exchange with third parties, to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.
-  **Establishing risk assessment.** To determine the appropriate levels of security measures applied to information systems, a process of risk assessment is carried out for each system to identify the probability and impact of security failures. A contingency plan and a disaster continuity plan are developed.
-  **Documented system.** Policies associated with this policy are established and included in Information Security Management System (ISMS) and are aligned with the Gestamp Group's General Information Security Policy and must comply with regulatory and contractual requirements.  
Guidelines for the revision and updating of the ISMS are established and its compliance is periodically checked.
-  **Responsibilities.** It is responsibility of CTIO Director to manage and regularly revise of this policy.
  - All TIO R&D center directors and managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
  - Employees must comply with the policies and procedures of the ISMS. An employee who violates any of these regulations shall be involved in disciplinary process in accordance with employee rules and regulations.
  - Business partners with whom Gestamp information is shared are informed about the Information Security requirements and the necessary contractual relationships are established. Legal action will be taken in case of non-compliance.

*Approved by:*

Ignacio Martín Gonzalez

**CHIEF TECHNOLOGY AND INNOVATION OFFICER - CTIO**