	Política del Sistema de Gestión de la Seguridad de la Información	CÓDIGO	3DS-GCA-PT-02
		VERSIÓN	2
		FECHA	NOV/2023
		CLASIFICACIÓN	PÚBLICO
		PÁGINA	1 de 2

Goal

Define the commitment and provide the company's framework for the implementation and operation of the Information Security Management System.

Scope

The scope of this policy covers all processes and operational areas of the organization.

Information Security Management System Policy


Our main goal lies in developing customized technology solutions to meet the needs of our customers. Thus, building applications and systems that fulfill the requirements of each project.

In Asociación de Ingenieros de Sistemas 3D Grupo Empresarial, we develop customized software, recognizing the value of information management in achieving our objectives.

We assume the responsibility of ensuring confidentiality, integrity, and availability of data, information, and resources through the implementation and improvement of the Information Security Management System based on ISO 27001:2022 standards.

This decision reflects our determination to establish and maintain solid information security standards. Consequently, through this system, we are committed to:

1. Identify and mitigate proactively all security risks associated with information. We recognize that, if we anticipate and assess efficiently the risks, we will be able to ensure the integrity and confidentiality of our information assets, as well as guarantee continuous operation in a safe environment.
2. Promote a security culture that involves all members of our organization, thus ensuring continuous training and awareness of information security.

	Política del Sistema de Gestión de la Seguridad de la Información	CÓDIGO	3DS-GCA-PT-02
		VERSIÓN	2
		FECHA	NOV/2023
		CLASIFICACIÓN	PÚBLICO
		PÁGINA	1 de 2

3. Provide all resources needed for effective maintenance and operation of the information security management system.
4. Establish appropriate access controls to ensure confidentiality, integrity, and information availability.
5. Establish the necessary communication channels to notify incidents, events, vulnerabilities, and risks that may impact the information assets of the organization.
6. Act nimbly and skillfully when responding to security incidents, thus minimizing adverse effects.
7. Comply with all legal and regulatory requirements relating to information security.

The top management promotes this policy to ensure that it is understood, implemented, broadcasted, and maintained at all levels of the organization.