Information Security Policy

Política de Seguridad de la Información

Rev.	Descripción/Description	Elaborado/Made by	Rev & Aprob/Chek´d & Appr.	Fecha/Date
01	Aprobado para construcción Approved for construction	RSI	Presidente	03-10-2023

HISTÓRICO DE REVISIONES DEL DOCUMENTO/ DOCUMENT HISTORICAL REVISIONS		
REV	FECHA/DATE	Cambios con respecto a la revisión previa / Changes from the previous revision
01	03-10-2023	Primera emisión / First revision

Table of Content

Tabla de Contenidos

1 Objective and scope

This Policy establishes the framework for action that defines the guidelines to effectively protect the information managed by DOSA. It is applicable and obligatory for all members of DOSA and its stakeholders. It has the following objectives:

- Ensure the level of confidentiality required for each type of information.
- Maintain the integrity of information, ensuring that it is accurate and complete, avoiding unauthorised modifications.
- Ensure the availability of information, in the appropriate medium and whenever it is needed.

2 Principles

In order to achieve the objectives described in the previous section, the following general principles are established:

- **Compliance**: the Information Security Management System, in accordance with ISO 27001 Information Security, shall be adequate to comply with the requirements of applicable legislation and internal regulations.

- **Lawful use of information**: the use of information is limited to lawful and exclusively professional purposes, for the performance of job-related tasks.

- **Classification of information**: information shall be classified according to the economic, operational and compliance impact that its loss or unauthorised disclosure would have on the organisation.
- **Awareness**: providing employees with the necessary training to understand Information Security risks and the technical competence to apply the necessary practices for the protection of information.
- **Risk management**: to carry out an adequate assessment, management and treatment of the Information Security risk, developing the necessary controls and measures to mitigate the risks identified.

1 Objetivo y alcance

La presente Política establece el marco de actuación que define las directrices para proteger de manera eficaz la información gestionada por DOSA. Es de aplicación y obligado cumplimiento para todos los miembros de DOSA y sus partes interesadas. Tiene los siguientes objetivos:

- Garantizar el nivel de confidencialidad requerido por cada tipo de información.
- Mantener la integridad de la información, asegurando que ésta sea exacta y completa, evitando modificaciones no autorizadas.
- Asegurar la disponibilidad de la información, en el soporte adecuado y siempre que sea necesaria.

2 Principios

Para alcanzar los objetivos descritos en el apartado anterior, se establecen los siguientes principios generales:

- **Cumplimiento**: el Sistema de Gestión de Seguridad de la Información, conforme a la ISO 27001 de Seguridad de la Información, será adecuado para cumplir con las exigencias de la legislación vigente y de la normativa interna que resulte de aplicación.
- **Uso lícito de la información**: el uso de la información está limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo.
- **Clasificación de la información**: la información se clasificará en función del impacto económico, operativo y de cumplimiento que su pérdida o difusión no autorizada tendría sobre la organización.
- **Concienciación**: proporcionar a los empleados la formación necesaria para comprender los riesgos de Seguridad de la Información y la competencia técnica para aplicar las prácticas necesarias para la protección de la información.
- **Gestión del riesgo**: realizar una adecuada evaluación, gestión y tratamiento del riesgo de Seguridad de la Información, desarrollando los controles y medidas necesarias para mitigar los riesgos identificados.

- **Information Security incident management**: acting appropriately to prevent, detect and respond to incidents that may affect information security.

- **Continuity**: A business continuity management process is established so that, in the event of an information security incident causing a disaster, the downtime of DOSA's critical information is reduced to acceptable levels.

- **Continuous improvement**: improving the effectiveness and efficiency of the controls in place to adapt to evolving risks.

3 Responsibilities

All DOSA employees must be familiar with, accept and comply with this Policy and the applicable internal regulations.

DOSA has appointed a Chief Information Security Officer (CISO). The CISO is responsible for managing DOSA's information security, defining strategic security objectives and plans and ensuring that good practices in information security management are applied effectively and consistently throughout the organisation. He or she will also report to the DOSA Management Committee on the state of the system, the evolution of risks and threats and significant incidents.

4 Approval

By approving this Policy, the Steering Committee commits to allocate the necessary resources for its effective implementation and to achieve a level of Information Security appropriate to the needs of the business.

- **Gestión de incidentes de Seguridad de la Información:** actuar de manera adecuada para prevenir, detectar y responder a los incidentes que puedan afectar a la seguridad de la información.
- **Continuidad**: se establece un proceso de gestión de la continuidad del negocio para que, en caso de que un incidente en materia de seguridad de la información cause un desastre, el tiempo de indisponibilidad de la información crítica para DOSA se reduzca a niveles aceptables.
- **Mejora continua**: mejorar la eficacia y eficiencia de los controles implantados para adaptarse a la evolución de los riesgos.

3 Responsabilidades

Todos los empleados de DOSA deberán conocer, asumir y cumplir la presente Política, así como la normativa interna aplicable.

DOSA ha designado un Responsable de Seguridad de la Información (RSI). Es el encargado de gestionar la Seguridad de la Información de DOSA, definir los objetivos y planes de seguridad estratégicos y asegurar que las buenas prácticas sobre la gestión de la Seguridad de la Información se apliquen de manera efectiva y consistente en la organización. Además, informará al Comité de Dirección de DOSA del estado del Sistema, la evolución de los riesgos y amenazas y los incidentes significativos.

4 Aprobación

Mediante la aprobación de esta Política, el Comité de Dirección se compromete a asignar los recursos necesarios para su implementación efectiva y alcanzar un nivel de Seguridad de la Información adecuado a las necesidades del negocio.