	POLÍTICA del SGSI	Código:	AN10
		Rev.:	0
		F. Implementación:	01/07/ 2025
		F. actualización:	

Objetivo: Establecer las directrices para controlar y proteger la información contra las amenazas y vulnerabilidades internas y externas relacionadas con la integridad, confiabilidad, disponibilidad y privacidad de la información del Sistema de Gestión de Seguridad de la Información de **OODOO**

Alcance: Esta Política se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI)

Los usuarios de este documento son todos los empleados de OODOO, como también terceros externos a la organización.

Esta política define las medidas que deben tomarse para proteger los activos de información críticos de negocio contra la modificación, divulgación o destrucción accidental o no autorizada, así como para asegurar **la confidencialidad, integridad disponibilidad y privacidad de la información.**

Términos y definiciones

- Información documentada. - Información que debe ser controlada y mantenida por la organización, así como el soporte en el que se contiene (según ISO/IEC 27001 e ISO/IEC 27701).

- SGSI. - Sistema de Gestión de Seguridad de la Información, establecido para proteger la confidencialidad, integridad y disponibilidad de la información.

- SGPI. - Sistema de Gestión de Información de Privacidad, que amplía el SGSI para gestionar los datos personales según la ISO/IEC 27701.

- Control de documentos. - Actividades para garantizar que los documentos sean revisados, actualizados, aprobados y estén disponibles cuando se requiera.

- Registro. - Evidencia objetiva que documenta actividades o resultados alcanzados.

- PIMS Sistema de Gestión de Información de Privacidad

- PII (*Personally Identifiable Information*).- Cualquier información que pueda usarse para identificar directa o indirectamente a un individuo (titular de la información. Ej. Nombre, numero ID, datos de localización, factores específicos físicos, fisiológicos, genéticos, mentales, económicos, culturales o sociales de esa persona, datos de enfermedades, etc. El tratamiento de la PII debe realizarse siempre con medidas adecuadas de seguridad, según los principios de confidencialidad, integridad y disponibilidad, además de cumplir con las regulaciones legales aplicables.

- Controlador PII (*PII controller*). - Entidad (persona u organización) que determina los propósitos y los medios del tratamiento de la Información de Identificación Personal (PII). Es quien decide por qué y cómo se procesan los datos personales.

- Procesador PII (*PII processor*). - Entidad que procesa la PII en nombre del controlador PII. No decide por qué ni cómo se procesan los datos, sino que los trata siguiendo las instrucciones recibidas del controlador.

- Subcontratado PII (*Sub-processor of PII*). - Entidad a la que el procesador PII puede subcontratar parte del procesamiento de PII. Solo puede hacerlo cuando el controlador PII lo autoriza, y debe garantizar que el subcontratado cumpla con los mismos requisitos de seguridad y privacidad aplicables.

Referencias

- ISO/IEC 27001:2022 – Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos.
- ISO/IEC 27701:2019 – Tecnología de la información – Técnicas de seguridad – Extensión a ISO/IEC 27001 y ISO/IEC 27002 para la gestión de la información de privacidad – Requisitos y directrices.
- ISO/IEC 27002:2022 – Código de prácticas para controles de seguridad de la información.
- Legislación aplicable relacionada con la protección de datos personales (por ejemplo, Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México u otras que correspondan).
- ISO/IEC 29100, Tecnología de la información — Técnicas de seguridad — Marco de privacidad

POLÍTICA

OODOO es una empresa responsable con el manejo, uso y tratamiento de la información de sus clientes, colaboradores, proveedores y socios, comprometida en adoptar, cumplir y alinear el SGSI a la normatividad, a los compromisos contractuales y a la legislación aplicable vigente, para asegurar la integridad, disponibilidad y confidencialidad y privacidad de la información, así como de los activos de información, con un enfoque de mejora continua.

Registros

- Listado maestro de información documentada F01
- Informes de auditoría interna F06

Control de cambios

No.	Descripción del cambio	Fecha del cambio	Elaboró
1	Creación del documento	01/07/2025	Fernando López