POLÍTICA DEL SISTEMA DE GESTIÓN INTEGRADO

ozmo
GLOBAL SERVICES

AGOSTO 2025

1. OBJETIVO

Establecer las directrices del Sistema de Gestión Integrado basado en las Normas Internacionales ISO 9001:2015 e ISO 27001:2022, para implementar, mantener y mejorar un Sistema de Gestión Integrado en Ozmo, que permita el cumplimiento de los objetivos de calidad y de seguridad de la información, mediante el cumplimiento de la satisfacción de nuestros clientes y de los requisitos aplicables relacionados a la seguridad de la información, garantizando la confidencialidad, disponibilidad, privacidad e integridad de la información.

2. ALCANCE

Esta política de Sistema de Gestión Integrado aplica a Ozmo y a:

- Sus colaboradores, independientemente de la relación contractual con la Organización, proveedores de servicios externos, consultores, auditores, contratistas que accedan a las instalaciones de la compañía, ya sea física o remotamente para realizar trabajos y/o empleen recursos de tecnologías de información de Ozmo.

- Todas las instalaciones, equipamiento (incluyendo equipos portátiles y accesorios móviles) para procesar o almacenar información de Ozmo.

- Todo el software para el procesamiento de datos o transporte de comunicaciones, sin importar el o los medios de almacenamiento o método de procesamiento que Ozmo disponga para sus fines.

- La utilización de hardware, software y recursos de terceros que Ozmo tenga en propiedad o bajo su dominio o licenciamiento o derecho de uso.

- Los ambientes y recintos de Ozmo en los cuales se procesa información y comunicaciones.

3. REFERENCIAS NORMATIVAS

La presente política se define considerando las recomendaciones de la siguiente normativa:

- Norma ISO 9001:2015. Sistemas de gestión de la calidad - Requisitos. Requisito 5.2
- Norma ISO/IEC 27001:2022, Seguridad de la Información, ciberseguridad y protección de la privacidad - sistemas de gestión de la seguridad de la información- Requisitos. Requisito 5.2. Política. Control A.5.1. Política para la Seguridad de la Información.

4. DEFINICIONES

Confidencialidad: La información debe ser conocida únicamente por aquellas personas que estén autorizadas para acceder información específica del negocio. Esto es necesario para proteger los asuntos reservados como planes estratégicos, información legal, de recursos humanos, información de los empleados y cualquier dato sensitivo.
Integridad: La información solamente puede ser agregada, modificada o eliminada por personas y/o procesos debidamente autorizados. Esto es necesario para garantizar que la información que soporta el negocio sea precisa y completa para que las decisiones que se tomen produzcan los resultados que se esperan.

Privacidad: Es el principio que garantiza que la información personal identificable sea recopilada, procesada, almacenada y divulgada únicamente con el consentimiento del titular y conforme a las leyes y regulaciones aplicables, protegiendo su confidencialidad, integridad y uso legítimo.

Disponibilidad: La información debe estar cuando se necesita en el formato requerido para su procesamiento, para asegurar que los procesos de negocio y las decisiones sean oportunas.

Propietario de la Información: Es el dueño del proceso que utiliza o genera dicha información.

Usuario de la Información: Es aquella persona, colaborador interno o externo, que con la debida autorización introduce, borra, cambia o lee información de la compañía. Los usuarios sólo deben tener acceso a la información a la que están autorizados para ver o procesar y las autorizaciones que se otorguen deben limitar su capacidad, de forma que no puedan realizar actividades distintas de aquellas para las que se otorgó permiso.

Satisfacción del cliente: percepción del cliente sobre el grado en que se han cumplido sus requisitos.

Mejora continua: actividad recurrente para aumentar la capacidad para cumplir los requisitos

Roles y responsabilidades:

Coordinador del SGI: Asegurar que se establezcan la Política y los Objetivos del Sistema de Gestión Integrado, que éstos sean compatibles con el contexto y la dirección estratégica de la organización y que se integren los requisitos del sistema de gestión integrado en los procesos de negocio de la organización. Asegurar que las materias abordadas en esta política se ejecutan y se cumplen, identificar como se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la presente política detectando y proponiendo mejoras. Recibir y dar respuesta a las no conformidades e incidentes de seguridad de la información ocurridos.

Colaboradores: dar cumplimiento a la presente Política de Sistema de Gestión Integrado, reportar los eventos, debilidades o incidentes de seguridad detectados.

5. DESCRIPCIÓN

Ozmo es una empresa chilena que entrega consultoría especializada para la implementación de las plataformas SIS campus y ERP Global, incluyendo la planificación, configuración y adaptación de estas plataformas a los requisitos específicos de los clientes incluyendo el diseño y desarrollo de implementación de soluciones de tecnología e infraestructura, orientadas a optimizar su funcionamiento.

La empresa busca:

- Lograr una alta satisfacción de nuestros clientes, usuarios y beneficiarios, mediante la entrega de servicios de calidad.
- Mejorar continuamente nuestro Sistema de Gestión Integrado (SGI), cumpliendo así con los requisitos y compromisos pactados.
- Garantizar la confidencialidad, integridad, privacidad y disponibilidad de la información de nuestros clientes, usuarios, beneficiarios, proveedores y resto de las partes interesadas.
- Desarrollar continuamente las capacidades de nuestros colaboradores, entendiendo con ello que la calidad del servicio está completamente vinculada a la excelencia del capital humano.
- Cumplir con toda la normativa vigente que sea aplicable en los ámbitos legales, reglamentarios y otros.

5.1 RELACIÓN CON PROVEEDORES (A.5.19, A.5.20, A.5.21)

Todo proveedor crítico externo de la compañía debe contar con un documento formal que respalde de la relación con Ozmo, ya sea un acuerdo de servicios o un Contrato. En dicho documento se deben abordar todos los requisitos de seguridad de información pertinente, para mitigar riesgos asociados al acceso del proveedor a los activos de Ozmo.
Al momento de definir cada acuerdo de servicio o contrato de servicio se deben tener en cuenta los siguientes ámbitos de acción a controlar según sean los servicios por contratar:

- Control de accesos físicos.
- Control de accesos a información.
- Control de activos.
- Confidencialidad de información
- Seguridad en las operaciones y todos aquellos ámbitos regulados por la presente política de seguridad de la información.

En caso de ausencia de un documento formal, el proveedor crítico debe aceptar explícitamente el presente punto 5 de la POL-01 Política del Sistema de Gestión Integrado de la empresa, y comprometerse a su cumplimiento.

Dicho proveedor debe comprometerse a administrar y tratar la información y otros activos de Ozmo con la debida confidencialidad y uso de información únicamente con fin de cumplir con las obligaciones contractuales.

Queda formalmente prohibido que los proveedores hagan uso de la información de la compañía o de sus clientes para fines personales o fuera del alcance del contrato de servicio.

En caso de tener proveedores que generen una cadena de suministro de tecnologías de información y comunicación, dichos proveedores deben velar por el cumplimiento de la presente política según la aplicabilidad.

Es decir, para los servicios de tecnologías de información y comunicación, se requiere que se propaguen los requisitos de seguridad de la información en toda la cadena de suministro, si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados a Ozmo.
Igualmente, para los productos de tecnologías de información y comunicación, se requiere que se propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro, si estos productos incluyen componentes comprados a otros proveedores.

También se debe obtener una garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado y que la garantía de los componentes críticos y su origen se puede rastrear a través de toda la cadena de suministro.

5.2 POLÍTICAS COMPLEMENTARIAS RELACIONADAS

Ozmo, adicional a lo mencionado en el punto anterior, donde se detalla la política de seguridad de la información, considera la definición de las siguientes políticas que son parte integral del conjunto de políticas de seguridad de la información.

5.2.1 POL-08 POLÍTICA DE DISPOSITIVOS DE PUNTO FINAL DE USUARIO

Establece las directrices de seguridad para los Dispositivos de Punto Final de Usuario, que son propiedad de LA EMPRESA, o propiedad de sus colaboradores, de tal manera que se encuentre protegida la información almacenada, procesada o accedida a través de dichos dispositivos.

5.2.2 POL-06 POLÍTICA DE TELETRABAJO

Establece las directrices para regular el trabajo remoto para los colaboradores y controlar los riesgos de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.

z5.2.3 POL-04 POLÍTICA DE CONTROL DE ACCESO
Establece las directrices de control de acceso lógico a los activos que son propiedad de LA EMPRESA y de sus colaboradores, controlar el acceso a la información y a la infraestructura de procesamiento de dicha información y evitar accesos no autorizados, daños o interferencias contra las instalaciones y la información de la Compañía o de sus clientes.

5.2.4 POL-07 POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

Establece lineamientos y normas generales que regulen la protección y el uso de pantallas y escritorios no supervisados, durante y después de la jornada laboral, entendiendo éstos como pantallas de computador y/o escritorios que permanecen sin uso y sin un colaborador que esté vigilando y ejerciendo supervisión sobre la información que éstos contienen.

5.2.5 POL-02 POLÍTICA DE GESTIÓN DE ACTIVOS

Establece las directrices para la gestión de activos que son propiedad de Ozmo y de sus colaboradores y controlar los riesgos de seguridad asociados a dichos activos.

5.2.6 POL-03 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN
Establece lineamientos para garantizar la seguridad de la información que se transfiere dentro de Ozmo y con cualquier entidad externa a la misma, haciendo uso de cualquier recurso de comunicación.

5.2.7 POL-09 POLÍTICA DE CONTROL CRIPTOGRÁFICO
Establece reglas para el uso efectivo de la criptografía dentro de LA EMPRESA, incluyendo la gestión de claves criptográficas para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo con los requisitos comerciales y de seguridad de la información, teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

5.2.8 POL-11 POLÍTICA DE DESARROLLO
Definir los lineamientos generales para el diseño e implementación de desarrollo seguro de software para la organización y/o clientes de LA EMPRESA.

5.2.9 POL-10 POLÍTICA DE RESPALDO DE DATOS
Establece normas y políticas para el resguardo de la información, para posibilitar la recuperación de ésta en el menor tiempo posible, a través de la restauración del respaldo.

5.2.10 POL-05 POLÍTICA DE SEGURIDAD PARA LOS SERVICIOS EN LA NUBE
Establece los requisitos de seguridad de la información en los procesos de adquisición, uso, gestión y salida de los servicios en la nube, con el fin de administrar la seguridad de la información en su uso.

6. ACTUALIZACIÓN DE LA POLÍTICA

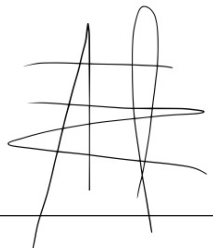
Dentro de la mejora continua de las políticas de seguridad de la información, esta política debe ser revisada al menos una vez al año, a partir de la fecha de entrada en vigor. El proceso se debe realizar según las definiciones del procedimiento PR-01 Información Documentada.

7. DIFUSIÓN DE LA POLÍTICA

- La totalidad de las políticas, procedimientos y protocolos deben ser informados a las Jefaturas para que las difundan según el nivel de acceso permitido a cada colaborador.

8. REGISTROS

Registro información en SharePoint.
Listado Maestro de Documentos.



Alfredo Busch
CEO - Ozmo Global Services