TABLA DE CONTENIDO

1. OBJETIVO, ALCANCE Y USUARIOS 2
2. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN 2
3. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 3
3.1. Objetivos y medición 3
3.2. Requisitos para la seguridad de la información 4
3.3. Controles de seguridad de la información 5
3.4. Responsabilidades 5
3.5. Comunicación de la Política 6
4. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI 6
5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 7

1. OBJETIVO, ALCANCE Y USUARIOS

El propósito de esta Política de alto nivel es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información.

Esta Política se aplica a todo el Sistema de gestión de seguridad de la información (ISMS), según se define en el Documento del Alcance del SGSI.

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

Documentos de referencia

- Norma ISO/IEC 27001, capítulos 5.2 y 5.3
- Documento sobre el alcance del Sistema de Gestión de Seguridad de la Información (SGSI)
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Lista de obligaciones legales, normativas y contractuales
- Política de la Continuidad del Negocio
- Procedimiento para gestión de incidentes

2. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

Disponibilidad(D)

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Integridad(I)

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Confidencialidad(C)

Propiedad o característica consistente en que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Trazabilidad(T)

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Seguridad de la información

Es la preservación de la disponibilidad, confidencialidad, integridad y trazabilidad de la información.

Sistema de gestión de seguridad de la información

Parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

3. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1. Objetivos y medición

- Proteger áreas y equipos donde se alojen información de valor de la organización.
- Implementar políticas y controles de seguridad para salvaguardar la información de valor de la organización.
- Implementar en un 100% para finales del año 2025 un proceso de Gestión de Incidentes para el tratamiento de eventos de seguridad de la información.
- Disminuir los riesgos asociados a seguridad de la información de por lo menos un 20% para cierre del año 2025.
- Garantizar que el 100% de los empleados de la organización reciban capacitación y concientización sobre seguridad de la información hasta finales del 2025.

3.2. Requisitos para la seguridad de la información

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales. Los requisitos mínimos para aplicar son:

Gestión de Activos

- Deben identificar y clasificar los activos de información relevantes y asignar roles y responsabilidades para su protección.

Control de Acceso

- Deben establecerse políticas y procedimientos para la asignación revocatoria de permisos de acceso a los usuarios.

Cifrado de la Información

- La organización debe implementar el cifrado de datos confidenciales durante la transmisión y en reposo, según sea necesario.

Seguridad Física y del Entorno

- Deben establecerse medidas de seguridad física para proteger los activos de información, como controles de acceso a instalaciones y sistemas de detección de intrusiones.

Gestión de Incidentes de Seguridad de la Información

- Debe existir un proceso para la notificación, registro y gestión de incidentes de seguridad de la información.

Seguridad en las Comunicaciones

- Debe existir un control de seguridad de las comunicaciones que incluya la protección de la confidencialidad, integridad y autenticidad de los datos transmitidos.

Desarrollo Seguro de Aplicaciones y Sistemas

- Deben implementarse controles de seguridad en el ciclo de vida de desarrollo de aplicaciones y sistemas, como revisiones de código, pruebas de seguridad y gestión de vulnerabilidades.

Gestión de Proveedores

- La organización debe evaluar y gestionar la seguridad de los proveedores que tienen acceso a activos de información sensibles.

Concienciación y Formación en Seguridad de la Información

- La organización debe proporcionar capacitación y concienciación en seguridad de la información a todos los empleados y partes interesadas relevantes.

Cumplimiento Legal y Regulatorio

- Deben establecerse controles para garantizar el cumplimiento de las leyes y regulaciones aplicables en relación con la seguridad de la información.

3.3. Controles de seguridad de la información

El proceso de escoger los controles (protección) está definido en la metodología de evaluación y tratamiento de riesgos.

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

Se deben aplicar y cumplir las políticas y procedimientos del Sistema de gestión de seguridad de la información (SGSI) vigentes y aprobados por el responsable del sistema de Gestión.

3.4. Responsabilidades

Las responsabilidades para el SGSI son las siguientes:

- El responsable del Sistema SGSI es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El responsable del Sistema SGSI es el responsable de la coordinación operativa del SGSI, como también de informar su desempeño.
- La Alta Dirección debe revisar el SGSI al menos una vez por año o cada vez que se produzca una modificación significativa; y debe elaborar minutas de dichas reuniones. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI.
- El responsable del Sistema SGSI a través de Capital Humano implementará programas de capacitación y concienciación de empleados sobre seguridad de la información.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad deben ser informados al responsable del Sistema SGSI.
- El responsable del Sistema SGSI definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.
- El Área de Capital Humano con el Apoyo del responsable de sistema SGSI serán responsables de adoptar e implementar el Plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.

3.5. Comunicación de la Política

El Área de Capital Humano en conjunto con el responsable del SGSI debe asegurarse de que todos los empleados de Grupo Entregas, como también los participantes externos correspondientes, estén familiarizados con esta Política.

4. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI

A través del presente, La Alta Dirección declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr

todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido hasta el 2026.

El propietario de este documento es el responsable del SGSI, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y participantes externos que cumplen una función en el SGSI pero que no están familiarizados con el presente documento.
- No cumplimiento del SGSI con las leyes y normas, las obligaciones contractuales y con los demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGSI.
- Responsabilidades ambiguas para la implementación del SGSI.

Control de cambios

FECHA ANTERIOR	CAMBIOS O MODIFICACIONES	FECHA DEL CAMBIO	AUTOR
	Creación del documento	Oct 2023	FTuston
Oct 2023	Actualización completa	Feb 2025	FQuille

Elaborado por:	Revisado por:	Aprobado por:
Luis Román Soporte IT UIO	Sergio Recalde Jefe de Calidad y Auditoría	Fernando Quille Gerente de IT

(*) Ubicación de cambio realizado en el documento