POLÍTICA DE GESTIÓN DE CAMBIO

Versión 1.0
7. Apoyo

Código:	POL-07/023/V1.0-Política de gestión de cambio
Versión:	1.0
Fecha de emisión:	2025
Creador por:	Depto. Seguridad de la Información
Responsable:	Coordinación del SGSI
Revisión	Anual o ante cambios regulatorios
Nivel de Confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
28-may-25	1.0	Coordinación del SGSI	Creación de documento

Tabla de contenido

1. Objetivo, alcance y usuarios 2

2. Documentos de referencia 2

3. Gestión de cambios 2

4. Gestión de registros guardados en base a este documento 3

5. Validez y gestión de documentos 3

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir cómo se controlan los cambios en los sistemas de información.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todas las tecnologías de la información y de la comunicación utilizadas dentro del alcance del SGSI.

Los usuarios de este documento son empleados de EthicsGlobal.

2. Documentos de referencia

- Norma ISO/IEC 27001, puntos A.12.1.2, A.14.2.4
- Política de seguridad de la información

3. Gestión de cambios

Cualquier cambio (instalación de nuevo software o de una versión nueva de un software existente, actualización de controlador, instalación de parches, cambios de configuración, etc.) sobre sistemas operativos o de producción debe ser realizado de la siguiente forma:

1. Los cambios pueden ser propuestos por los gerentes de cada área operativa y/o administrativa.
2. Los cambios deben ser autorizados por el Coordinador del SGSI, que debe evaluar su justificación para el negocio y las potenciales consecuencias negativas sobre la seguridad.
3. Los cambios deben ser implementados por los gerentes de las áreas involucradas.
4. El Coordinador del SGSI es el responsable de verificar que los cambios se han implementado de acuerdo a los requerimientos.
5. El gerente de operaciones es el responsable de probar y verificar la estabilidad del sistema; el sistema no debe ser puesto en producción antes de haber realizado pruebas exhaustivas.
6. La implementación de los cambios debe ser reportada a las siguientes personas: Dirección general y áreas involucradas.

Los registros sobre los cambios son llevados mediante el proyecto ISO27001 de JIRA a modo de tickets de soporte.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Ticket de solicitud de cambios	JIRA Cloud	Coordinador del SGSI	Una vez creado, el registro ya no puede ser modificado.	3 años

5. Validez y gestión de documentos

Esta política será revisada anualmente por el Comité de Seguridad de la Información o, cuando ocurra un cambio significativo en los roles organizacionales.

El propietario de este documento es el Coordinador 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 cambios no realizados de acuerdo con este documento.
• Cantidad de cambios que no consiguieron los resultados deseados.

Representante de la Dirección General
Liuva Anahí Figueroa Gracián