1. RESUMEN

Este documento establece la Política y el Plan de Control de Cambios para el Sistema de Gestión de Seguridad de la Información (SGSI) de Focus Systems Perú S.A.C., alineado con los requisitos de la norma ISO/IEC 27001:2022. Su objetivo es garantizar que todos los cambios en los sistemas, procesos y activos de información se gestionen de manera controlada para minimizar riesgos y asegurar la continuidad del negocio.

2. OBJETIVO

Definir las directrices y procedimientos necesarios para gestionar de manera efectiva los cambios dentro del SGSI, con el fin de:

- Asegurar que los cambios sean evaluados, aprobados, implementados y documentados adecuadamente.
- Minimizar el impacto negativo en la seguridad de la información debido a cambios no controlados.
- Mantener la integridad, confidencialidad y disponibilidad de los activos de información.

3. ALCANCE

El ámbito de aplicación de las disposiciones contenidas en el presente plan comprende a toda la estructura la organización, es decir que todos los empleados, colaboradores, contratistas, consultores, temporales y demás trabajadores de la organización son responsables de hacer un uso adecuado de este documento, en cumplimiento con las políticas, leyes y regulaciones locales y las directrices establecidas por la organización.

4. POLÍTICA

- **Control y Autorización de Cambios:** Ningún cambio puede ser implementado sin la aprobación formal de las partes responsables.
- **Evaluación de Impacto:** Todos los cambios deben ser evaluados en términos de impacto en la seguridad de la información, continuidad del negocio y cumplimiento normativo.
- **Documentación Obligatoria:** Todos los cambios deben estar documentados en un registro oficial que incluya detalles sobre la solicitud, evaluación, aprobación e implementación.
- **Revisión Periódica:** Los procedimientos de control de cambios serán revisados periódicamente para garantizar su eficacia y alineación con las necesidades organizacionales.

5. PLAN

1. Solicitud de Cambio

Actividades

- Registrar la solicitud de cambio en el sistema de gestión de cambios.
- Describir el cambio propuesto, justificación y recursos necesarios.

Roles

- Responsable: Solicitante del cambio.
- Participantes: Coordinador del SGSI, responsables de áreas afectadas.

2. Evaluación del Cambio

- Analizar el impacto del cambio en la seguridad de la información.
- Evaluar los riesgos asociados y proponer medidas de mitigación.

Roles

- Responsable: Coordinador del SGSI.

- Participantes: Equipo de Gestión de Cambios, responsables de áreas.

3. **Aprobación del Cambio**

   Actividades

   - Someter la evaluación y propuesta a las partes responsables para su aprobación.
   - Documentar las aprobaciones en el registro de cambios.

   Roles

   - Responsable: Alta Dirección.
   - Participantes: Coordinador del SGSI, responsables técnicos.

4. **Implementación del Cambio**

   Actividades

   - Ejecutar el cambio conforme al plan aprobado.
   - Realizar pruebas para validar la correcta implementación.

   Roles

   - Responsable: Equipo técnico asignado.
   - Participantes: Coordinador del SGSI, responsables de procesos.

5. **Seguimiento y Revisión del Cambio**

   Actividades

   - Monitorear el impacto del cambio en los sistemas y procesos.
   - Actualizar la documentación y procedimientos relacionados.

   Roles

   - Responsable: Coordinador del SGSI.
   - Participantes: Equipo de Auditoría Interna.

6. CUMPLIMIENTO

6.1 MEDICIÓN DEL CUMPLIMIENTO

La organización realizará un seguimiento y verificación del cumplimiento de esta política y plan mediante una variedad de métodos, incluyendo:

- Visitas periódicas
- Monitoreo de video
- Informes generados por herramientas comerciales
- Auditorías internas y externas
- Inspecciones

Los resultados de estas actividades serán comunicados al propietario del plan y al gerente de la unidad de negocio correspondiente, con el fin de garantizar el cumplimiento y la mejora continua de la política.

6.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

6.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

7. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: