

1. RESUMEN

Este documento establece la Política y el Plan de Control de Documentos 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 toda la documentación del SGSI se gestione de manera controlada, asegurando su disponibilidad, integridad y confidencialidad.

2. OBJETIVO

Definir las directrices y procedimientos necesarios para gestionar de manera efectiva la creación, revisión, aprobación, distribución y eliminación de documentos dentro del SGSI, con el fin de:

- Garantizar que solo se utilicen documentos vigentes y aprobados oficialmente.
- Prevenir el uso no autorizado o inapropiado de la información contenida en los documentos.
- Asegurar la trazabilidad y control de los cambios realizados en la documentación.

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 de Creación y Revisión:** Todo documento debe pasar por un proceso formal de creación, revisión y aprobación antes de ser distribuido.
- **Identificación Unívoca:** Todos los documentos deben ser identificados con un código único que permita su fácil localización y control.
- **Distribución Controlada:** La distribución de documentos será limitada a las personas autorizadas y se registrará en el sistema de gestión de documentos.
- **Revisión Periódica:** Los documentos serán revisados periódicamente para garantizar su vigencia y adecuación a los objetivos del SGSI.
- **Eliminación Segura:** Los documentos obsoletos serán eliminados de manera segura para evitar el acceso no autorizado.

5. PLAN

1. Creación y Revisión del Documento

Actividades

- Elaborar el documento según los lineamientos establecidos.
- Revisar el contenido para garantizar su calidad y alineación con los objetivos del SGSI.

Roles

- Responsable: Autor del documento.
- Participantes: Revisor designado, Coordinador del SGSI.

2. Aprobación del Documento

- Someter el documento revisado para su aprobación formal.
- Registrar la aprobación en el sistema de gestión de documentos.

Roles

- Responsable: Alta Dirección.
- Participantes: Coordinador del SGSI.

3. Distribución del Documento

Actividades

- Publicar el documento aprobado en el repositorio oficial del SGSI.
- Notificar a los usuarios relevantes sobre la disponibilidad del documento.

Roles

- Responsable: Administrador del sistema de gestión de documentos.
- Participantes: Usuarios finales.

4. Control de Cambios en Documentos

Actividades

- Registrar cualquier modificación en el historial de cambios del documento.
- Someter los cambios a revisión y aprobación formal.

Roles

- Responsable: Autor del cambio.
- Participantes: Revisor designado, Coordinador del SGSI.

5. Eliminación de Documentos Obsoletos

Actividades

- Identificar documentos obsoletos y asegurar su eliminación segura.
- Actualizar el registro de documentos para reflejar su eliminación.

Roles

- Responsable: Administrador del sistema de gestión de documentos.
- Participantes: Coordinador del SGSI.

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	Nombre	Nombre
Oficial de Seguridad de la Información	Gerente Administrativo	Gerente General
Fecha:	Fecha:	Fecha: