## 1. RESUMEN

Este documento establece la Política y Plan de Mejora Continua del 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. La mejora continua es un principio fundamental para garantizar la eficacia del SGSI y adaptarse a los cambios en el entorno organizacional y las amenazas a la seguridad de la información.

## 2. OBJETIVO

Definir las directrices para identificar, planificar y ejecutar acciones que impulsen la mejora continua del SGSI, con el fin de:

- Mantener y mejorar la confidencialidad, integridad y disponibilidad de los activos de información.
- Asegurar el cumplimiento constante con los requisitos de la norma ISO/IEC 27001:2022.
- Optimizar los procesos y controles relacionados con la seguridad de la 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

- **Compromiso con la Mejora Continua:** Focus Systems Perú S.A.C. se compromete a mantener un enfoque proactivo en la identificación y aplicación de mejoras al SGSI.

- **Participación de las Partes Interesadas:** La mejora continua es una responsabilidad compartida que involucra a todos los niveles de la organización.
- **Basado en Evidencia:** Las decisiones de mejora se fundamentarán en datos obtenidos de auditorías, revisiones por la dirección, monitoreo y mediciones.
- **Revisión Periódica:** La alta dirección revisará periódicamente la eficacia de las mejoras implementadas.

## 5. PLAN

### 1. Identificación de Oportunidades de Mejora

**Actividades**

- Analizar los resultados de auditorías internas y externas.
- Revisar indicadores de rendimiento del SGSI.
- Recopilar retroalimentación de las partes interesadas.

**Roles**

- Responsable: Coordinador del SGSI.
- Participantes: Responsables de procesos, equipo auditor.

### 2. Planificación de Acciones de Mejora

**Actividades**

- Priorizar las oportunidades de mejora identificadas.
- Definir los objetivos y plazos para cada acción de mejora.
- Asignar recursos y responsables para la implementación.

**Roles**

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

### 3. Implementación de Acciones de Mejora

**Actividades**

- Ejecutar las acciones de mejora conforme al plan establecido.
- Monitorear el progreso de las acciones implementadas.

**Roles**

- Responsable: Responsables de las áreas involucradas.
- Participantes: Coordinador del SGSI.

**4. Monitoreo y Evaluación de Resultados**

**Actividades**

- Verificar la eficacia de las acciones de mejora implementadas.
- Actualizar el plan de mejora continua basado en los resultados obtenidos.

**Roles**

- Responsable: Coordinador del SGSI.
- Participantes: Equipo Auditor, Alta Dirección.

**5. Revisión y Documentación**

**Actividades**

- Documentar los resultados y lecciones aprendidas.
- Integrar los hallazgos en la revisión por la dirección.

**Roles**

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

## 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<br><br>**Oficial de Seguridad de la Información**<br><br>Fecha: | Nombre<br><br>**Gerente Administrativo**<br><br>Fecha: | Nombre<br><br>**Gerente General**<br><br>Fecha: |