1. RESUMEN

Este documento establece la Política y Plan de Capacitación y Concientización 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. El objetivo es garantizar que todos los colaboradores comprendan sus responsabilidades en la protección de la información y adopten buenas prácticas en su gestión.

2. OBJETIVO

Definir las directrices para desarrollar y mantener un programa efectivo de capacitación y concientización en seguridad de la información, con el fin de:

- Asegurar que todo el personal comprenda y cumpla con las políticas y procedimientos del SGSI.
- Promover una cultura organizacional orientada a la seguridad de la información.
- Reducir riesgos asociados a errores humanos o desconocimiento de las amenazas.

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 Educación Continua:** Focus Systems Perú S.A.C. se compromete a proporcionar capacitación periódica en seguridad de la información a todos los colaboradores.
- **Relevancia y Adaptabilidad:** Los contenidos de capacitación estarán alineados con los roles y responsabilidades de los participantes, así como con las amenazas y riesgos actuales.
- **Participación Activa:** Todo el personal es responsable de asistir a las capacitaciones y aplicar los conocimientos adquiridos en sus actividades diarias.
- **Medición de Eficacia:** Se evaluará periódicamente la eficacia del programa de capacitación para garantizar su mejora continua.

5. PLAN

1. Identificación de Necesidades de Capacitación

Actividades

- Realizar un análisis de las competencias necesarias por área y puesto.
- Identificar brechas de conocimiento en seguridad de la información.

Roles

- Responsable: Coordinador del SGSI.
- Participantes: Responsables de áreas, equipo de recursos humanos.

2. Diseño del Programa de Capacitación

- Definir objetivos de aprendizaje y contenidos específicos.
- Seleccionar los métodos de entrega (presencial, virtual, talleres, etc.).

Roles

- Responsable: Equipo de Recursos Humanos.

- Participantes: Coordinador del SGSI, expertos en seguridad de la información.

3. **Implementación de las Capacitaciones**

   Actividades

   - Programar sesiones de capacitación periódicas.
   - Ejecutar talleres prácticos y simulaciones de incidentes.

   Roles

   - Responsable: Coordinador del SGSI.
   - Participantes: Formadores internos y externos, empleados.

4. **Concientización Continua**

   Actividades

   - Enviar boletines informativos y recordatorios periódicos.
   - Promover días temáticos sobre seguridad de la información.

   Roles

   - Responsable: Coordinador del SGSI.
   - Participantes: Equipo de Comunicaciones Internas.

5. **Evaluación y Mejora del Programa**

   Actividades

   - Aplicar cuestionarios para evaluar el conocimiento adquirido.
   - Recopilar retroalimentación de los participantes.
   - Actualizar los contenidos y métodos de capacitación según resultados.

   Roles

   - Responsable: Coordinador del SGSI.
   - Participantes: Equipo de Recursos Humanos, 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 **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: