

1. RESUMEN

Este documento establece la Política y Plan de Auditorías 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 implementación y ejecución de las auditorías busca garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

2. OBJETIVO

Definir las directrices y procedimientos para planificar, ejecutar, reportar y dar seguimiento a las auditorías internas y externas del SGSI, con el fin de:

- Verificar el cumplimiento de los requisitos establecidos por la norma ISO/IEC 27001:2022.
- Identificar áreas de mejora continua en la gestión de la seguridad de la información.
- Asegurar la eficacia del SGSI y su alineación con los objetivos estratégicos de la organización.

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 realizar auditorías periódicas y sistemáticas para evaluar el cumplimiento y la eficacia del SGSI.

- **Independencia y Objetividad:** Las auditorías serán realizadas por personal calificado, independiente de las actividades auditadas, garantizando la objetividad en los resultados.
- **Transparencia:** Los resultados de las auditorías serán comunicados de manera clara y oportuna a la alta dirección y partes interesadas pertinentes.
- **Confidencialidad:** La información recopilada durante las auditorías será tratada con estricta confidencialidad.

5. PLAN

1. Planeación de la Auditoría

Actividades

- Definir el alcance y objetivos de la auditoría.
- Elaborar el plan de auditoría.
- Seleccionar el equipo auditor.
- Notificar a las partes interesadas.

Roles

- Responsable: Coordinador del SGSI.
- Participantes: Auditores internos, responsables de áreas auditadas.

2. Ejecución de la Auditoría

Actividades

- Realizar reuniones de apertura.
- Recopilar evidencia objetiva mediante entrevistas, revisión de documentos y observación de procesos.
- Identificar no conformidades y oportunidades de mejora.

Roles

- Responsable: Equipo Auditor.

- Participantes: Responsables de los procesos auditados.

3. Informe de Auditoría

Actividades

- Elaborar el informe de auditoría con hallazgos, conclusiones y recomendaciones.
- Presentar el informe a la alta dirección.

Roles

- Responsable: Auditor Líder.
- Participantes: Coordinador del SGSI, alta dirección.

4. Seguimiento y Acciones Correctivas

Actividades

- Verificar la implementación de acciones correctivas y preventivas.
- Evaluar la eficacia de las medidas adoptadas.

Roles

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

5. Revisión de Resultados y Mejora Continua

Actividades

- Revisar los resultados de las auditorías en las reuniones de revisión por la dirección.
- Incorporar lecciones aprendidas al SGSI.

Roles

- Responsable: Alta Dirección.
- Participantes: Coordinador del SGSI, equipo auditor.

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: