PLAN

CAPACITACIÓN Y SENSIBILIZACIÓN INTEGRAL EN SEGURIDAD DE LA INFORMACIÓN

SGSI-PL-01

Elaborado por:	Revisado por:	Aprobado por:
.....	.....	.....
Nombre y Firma	Nombre y Firma	Nombre y Firma

1. OBJETIVO:

Desarrollar la cultura de seguridad de la información de la SUNAT para concientizar al personal y terceros, a fin de difundir las políticas, procedimientos y controles referentes a seguridad de la información, lo cual debe estar alineado a los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI).

2. ALCANCE:

El presente plan aplica a todo el personal de la SUNAT que forman parte de los procesos comprendidos dentro del alcance del SGSI.

3. DOCUMENTOS ASOCIADOS:

- Lista de Asistencia SGSI-PL-01.FO-01.

4. DOCUMENTOS DE REFERENCIA:

- NTP ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”

5. DEFINICIONES Y SIGLAS:

Definiciones

5.1 Capacitación: Cursos en temas relacionados a seguridad de la información, seguridad informática, continuidad de negocios, cumplimiento, entre otros; son planificadas por el Oficial de Seguridad de la Información (OFSI) para el personal involucrado en el SGSI.

5.2 Inducción: Charlas de concientización en seguridad de la información dictada al nuevo personal de la SUNAT, son programadas por el OFSI en coordinación con la INRH.

5.3 Concientización: Charlas de concientización en seguridad de la información dictadas al personal de la SUNAT y terceros, proporcionan información para tomar conciencia de los riesgos que existen por el mal uso de la información y los daños que pueden causar en la SUNAT si no se toman las acciones correctas; son planificadas por el OFSI.

Siglas

5.4 OFSI: Oficial de Seguridad de la Información.

5.5 CGSI: Comité de Gestión de Seguridad de la Información.

5.6 INRH: Intendencia Nacional de Recursos Humanos.

5.7 EICCSI: Expositor de la Inducción, Concientización y Capacitación en Seguridad de la Información.

5.8 SGSI: Sistema de Gestión de Seguridad de la Información.

5.9 SUNAT: Superintendencia Nacional de Aduanas y de Administración Tributaria.

5.10 SN: Superintendente Nacional.

6. PROCEDIMIENTO:

6.1. Condiciones Generales:

Este documento será revisado por lo menos una vez al año y actualizado cuando sea necesario. Cualquier actualización debe ser realizada siguiendo las estrategias de concientización, capacitación e inducción definidas por el CGSI y en forma coordinada entre el OFSI y, Propietarios de Riesgos y/o la Intendencia Nacional de Recursos Humanos (INRH), de ser necesario.

6.2. Establecimiento de los Grupos de Trabajo:

CGSI: 1. Para lograr una sensibilización acorde con las necesidades del personal, se les ha dividido en grupos de trabajo, de acuerdo con sus roles y responsabilidades, las cuales se detallan a continuación:

- Grupo A: Intendentes, Gerentes, Jefes.
- Grupo B: Propietarios de Riesgos, Propietarios de Activos de Información.
- Grupo C: Otros Colaboradores.

6.3. Elementos de Apoyo:

OFSI: 2. Adicionalmente a los cursos y charlas de inducción y concientización en seguridad de la información es importante apoyarse en otros elementos tales como:

- Afiches.
- Folletos.
- Protectores de pantalla.
- Recordatorios.
- Correos electrónicos.

6.4. Periodicidad y Duración:

OFSI: 3. La estrategia para el personal es que:

- Reciban inducción con respecto a temas de seguridad de la información al ingresar a laborar a la SUNAT.
- Reciban por lo menos una concientización en seguridad de la información al año:
  - Grupo A: una capacitación al año.
    Duración: 20 minutos.
  - Grupo B: una capacitación al año.
    Duración: 30 minutos.
  - Grupo C: una capacitación al año.
    Duración 40 minutos.

- Reciban por lo menos una capacitación al año en seguridad de la información, seguridad informática y/o continuidad de negocios de mínimo 16 horas.

4. La estrategia para los proveedores es que:

- Se les entregue la Política de Seguridad de la Información.

6.5. Temas a Desarrollar en la Inducción en Seguridad de la Información:

OFSI / INRH: 5. Programa en la inducción al nuevo personal de la SUNAT charlas de concientización en Seguridad de la Información.

Propietario de Riesgo: 6. Propone temas de seguridad de la información a contemplar en la inducción, concientización y capacitación. Considerando los siguientes temas:

- ¿Qué es la Seguridad de la Información? (Confidencialidad, Integridad, Disponibilidad).
- Aspectos que comprende la Seguridad de la Información (Personas, Procesos, Tecnología).
- Amenazas de Seguridad de la Información (Malware, Virus, Ingeniería Social, Phishing, Spywares, Troyanos Informáticos, Hackers, entre otros).
- Sistema de Gestión de Seguridad de la Información (SGSI) (Definición, ISO 27001, Anexo A (Normativa) Objetivos de Control y Controles, Beneficios).
- Sistema de Gestión de Seguridad de la Información (SGSI) de la organización. (Alcance, Estructura, Funciones y Responsabilidades, Políticas de Seguridad de la Información, Gestión de Incidentes de Seguridad de la Información, entre otros).

EICCSI: 7. Desarrolla la charla de Inducción en Seguridad de la Información.

6.6. Temas a Desarrollar en la Concientización en Seguridad de la Información:

EICCSI: 8. Desarrolla la charla de Concientización en Seguridad de la Información. Considerando los siguientes temas:

TEMAS A DESARROLLAR	OBJETIVO	CONTENIDO
Marco de la Seguridad de la Información.	Lograr el compromiso y adhesión a la Política de Seguridad de la Información de la organización.	• Política de Seguridad de la Información. • Funciones y Responsabilidades en Seguridad de la Información.
Identificación de Incidentes de Seguridad de la Información.	Dar a conocer los procedimientos implementados en caso se produjera un Incidente de Seguridad de la Información.	• ¿Qué es un Incidente de Seguridad de la Información? • Políticas y Procedimientos de Seguridad de la Información existentes.
Gestión de Activos de Información.	Comunicar la necesidad de proteger los activos de información de la SUNAT.	• Clasificación, Etiquetado y Tratamiento de los Activos de Información. • Control de ingreso y salida de equipos y documentos.

Escritorio y Pantalla Limpia.	Crear conciencia sobre la importancia de proteger la información impresa y la información digital a través del bloqueo de pantalla.	• Casos prácticos y situaciones reales presentadas en la SUNAT. • Políticas y procedimientos relacionados.
Políticas de Seguridad de la Información	Dar a conocer las políticas existentes y su aplicación.	• Políticas de Seguridad de la Información implementadas en la SUNAT.
Ingeniería Social.	Crear conciencia sobre las diversas tácticas de "Ingeniería Social" que se utilizan para obtener información sensible, cómo y porqué se utilizan y la forma de evitarlas.	• ¿Qué es la Ingeniería Social? • ¿Quiénes la usan? • Tácticas usadas para obtener información sensible. • ¿Cómo identificar intentos de Ingeniería Social? • ¿Cómo proceder ante ataques de ingeniería Social?
Seguridad en la navegación en Internet.	Comunicar los riesgos de seguridad de la información asociados al navegar por Internet y las precauciones a tomar para reducir los riesgos.	• Riesgo de ingresar a páginas restringidas. • Consecuencias del mal uso del Internet. • Consecuencias de descargar programas sin autorización.
Protección contra Virus	Comunicar sobre los virus informáticos.	• Tipos de Virus: Caballos de troya, gusanos, spyware y malware en general y, las prácticas recomendadas para reducir el riesgo de infección. • Medidas tomadas por la SUNAT para minimizar la amenaza de infección por virus.

6.7. Temas a Desarrollar en la Capacitación en Seguridad de la Información:

OFSI: 9. Define las estrategias de capacitación en materia de seguridad de la información, en base a ello el OFSI en coordinación con los Propietarios de Riesgos definen las capacitaciones a realizarse. (Ejemplo temas relacionados con la implementación y auditoría del Sistema de Gestión de Seguridad de la Información, Ciberseguridad, Continuidad de Negocios, ISO 27001, entre otros).

EICCSI 10. Desarrolla la Capacitación en Seguridad de la Información.

6.8. Asistencia de los Participantes:

OFSI: 11. Registra la asistencia de los participantes a las charlas presenciales de Inducción, Concientización y Capacitación en Seguridad de la Información en el documento Lista de Asistencia SGSI-PL-01.FO-01.

7. CONTROL DE CAMBIOS:

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial	01	04/02/2019	Oficial de Seguridad de la Información