# MANUAL
# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
# SGSI-MA-01

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

## ÍNDICE

1. OBJETIVO Y CAMPO DE APLICACIÓN ..... 3
2. REFERENCIAS NORMATIVAS ..... 3
3. TÉRMINOS Y DEFINICIONES ..... 3
4. CONTEXTO DE LA ORGANIZACIÓN ..... 4
5. LIDERAZGO ..... 5
6. PLANIFICACIÓN ..... 7
7. APOYO ..... 10
8. FUNCIONAMIENTO ..... 13
9. EVALUACIÓN DEL RENDIMIENTO ..... 14
10. MEJORAMIENTO ..... 16
11. CONTROL DE CAMBIOS ..... 17

## 1. OBJETIVO Y CAMPO DE APLICACIÓN

El presente documento tiene como objetivo documentar cada una de las cláusulas obligatorias de la Norma Técnica Peruana ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requisitos. 2a. Edición", la cual está basada en la norma ISO/IEC 27001:2013, que la Superintendencia Nacional de Aduanas y de Administración Tributaria - SUNAT, debe cumplir para mantener su Sistema de Gestión de Seguridad de la Información.

## 2. REFERENCIAS NORMATIVAS

- ISO/IEC 27000:2014 "Tecnología de la Información. Técnicas de Seguridad - Sistemas de gestión de seguridad de la información – Visión general y vocabulario".

- NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 2ª Edición.

- Resolución Ministerial Nº 004-2016-PCM. Aprueban el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

## 3. TÉRMINOS Y DEFINICIONES

Se utilizarán los términos y definiciones de la Norma ISO 27000:2014, tales como:

**3.1.** Análisis de Riesgo: Proceso de comprender la naturaleza del riesgo y determinar su nivel.

Nota 1: El análisis de riesgos proporciona las bases para la evaluación del riesgo y para tomar las decisiones sobre su tratamiento.

Nota 2: El análisis de riesgo incluye su estimación.

**3.2.** Confidencialidad: Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.

**3.3.** Disponibilidad: Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

**3.4.** Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

**3.5.** Integridad: Propiedad de exactitud y totalidad de la información.

**3.6.** Riesgo de Seguridad de la Información: Posibilidad de que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la SUNAT.

**3.7.** Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.

**3.8.** Sistema de Gestión de Seguridad de la Información (SGSI): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, mantener y mejorar la seguridad de la información.

**3.9.** Revisión por la Dirección: La Alta Dirección (referido al Comité de Seguridad de la Información) debe revisar el sistema de gestión de seguridad de la información de la SUNAT a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.

## 4. CONTEXTO DE LA ORGANIZACIÓN

### 4.1. La Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT y su Contexto

La Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT, de acuerdo a su Ley de Creación N° 24829, Ley General aprobada por Decreto Legislativo Nº 501 y la Ley N° 29816 de Fortalecimiento de la SUNAT, es un organismo técnico especializado, adscrito al Ministerio de Economía y Finanzas, cuenta con personería jurídica de derecho público, con patrimonio propio y goza de autonomía funcional, técnica, económica, financiera, presupuestal y administrativa que, en virtud a lo dispuesto por el Decreto Supremo N° 061-2002-PCM, expedido al amparo de lo establecido en el numeral 13.1 del artículo 13° de la Ley N° 27658, ha absorbido a la

Superintendencia Nacional de Aduanas, asumiendo las funciones, facultades y atribuciones que por ley, correspondían a esta entidad.

La SUNAT ha definido su contexto externo e interno en el documento SGSI-OD-01 - Contexto de SUNAT.

### 4.2. Comprender las Necesidades y Expectativas de las Partes Interesadas

La SUNAT ha identificado las necesidades y expectativas de las partes interesadas en el documento SGSI-OD-01 - Contexto de SUNAT.

### 4.3. Determinar el Alcance del Sistema de Gestión de Seguridad de la Información

Después de analizar el contexto externo, el contexto interno y comprender las necesidades y expectativas de las partes interesadas de la SUNAT, se ha determinado el alcance del Sistema de Gestión de Seguridad de la Información en el documento SGSI-OD-02 - Alcance del SGSI.

### 4.4. Sistema de Gestión de Seguridad de la Información

La SUNAT establece e implementa su Sistema de Gestión de Seguridad de la Información, de acuerdo con los requisitos de la NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2ª Edición para lo cual la SUNAT expresa su compromiso de mantenerlo y mejorarlo continuamente.

## 5. LIDERAZGO

### 5.1. Liderazgo y Compromiso

La SUNAT demuestra su liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información con las siguientes acciones:

- Se ha establecido la política de seguridad de la información, la cual está alineada a los objetivos estratégicos de la SUNAT.
- Conformando el Comité de Gestión de Seguridad de la Información.
- Los requisitos de seguridad han sido identificados e incluidos en los procesos que forman parte del alcance del SGSI.

- Asegurando la disponibilidad de recursos necesarios para el SGSI.
- Comunicando la importancia de una gestión eficaz de la seguridad de la información y el cumplimiento de los requisitos del SGSI.
- Asegurando que el SGSI alcance los resultados previstos.
- Dirigiendo y apoyando al personal para contribuir a la efectividad del SGSI.
- Promoviendo la mejora continua.
- Apoyando a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.

## 5.2. Política

La SUNAT contribuye en el desarrollo económico del país aportando a la sostenibilidad fiscal y estabilidad macroeconómica, mediante el efectivo cumplimiento tributario y aduanero, la facilitación del comercio exterior y la generación de conciencia tributaria en los ciudadanos, liderando el proceso de modernización del Estado mediante soluciones tecnológicas avanzadas y procesos optimizados.

Por consiguiente, es mandatorio que la seguridad de la información sea gestionada en la SUNAT en el marco de la normatividad vigente para las entidades del Estado, las mejores prácticas, estándares y metodologías, a fin de establecer un proceso de mejora continua que sea sostenible en el tiempo y que permita mediante la gestión de riesgos crear una cultura de prevención que apoye la continuidad de los procesos de negocio, asegurando niveles adecuados de integridad, confidencialidad y disponibilidad de todos sus activos de información relevantes para la institución.

La SUNAT, consciente de la importancia de preservar la confidencialidad, integridad y disponibilidad de la información para el cumplimiento de sus funciones y objetivos se compromete a gestionar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, y a cumplir todos los aspectos regulatorios, legales y otros requerimientos exigidos con relación a la seguridad de la información.

Fecha de Aprobación: 4 de mayo del 2018

### 5.3. Roles, Responsabilidades y Autoridades Organizacionales

Se han definido los roles y asignado responsabilidades, para tal efecto se definió al:

- Comité de Gestión de Seguridad de la Información, es quien tiene autoridad y responsabilidad sobre el SGSI.
- Oficial de Seguridad de la Información, responsable de la rendición de cuentas sobre el funcionamiento del SGSI al Comité de Gestión de Seguridad de la Información.

Los roles y responsabilidades del personal se encuentran definidas en el documento SGSI-MA-02 Manual de Roles, Responsabilidades y Autoridades Organizacionales del Sistema de Gestión de Seguridad de la Información.

## 6. PLANIFICACIÓN

### 6.1. Acciones para Abordar los Riesgos y Oportunidades

#### 6.1.1. Generalidades

El Comité de Gestión de Seguridad de la Información asegura que la planificación del SGSI se lleva a cabo con el fin de cumplir con los requisitos de los numerales 4.1 y 4.2 del presente manual y que se han determinado los riesgos y oportunidades, según lo definido en el documento SGSI-ME-01 Metodología de Gestión de Riesgos de Seguridad de la Información, con el fin de:

- Asegurar que el SGSI logre los resultados previstos.
- Prevenir o reducir, efectos no deseados.
- Lograr la mejora continua.

La SUNAT planifica:

- Las acciones a tomar frente a los riesgos y oportunidades identificadas.

- La forma de integrar y poner en práctica dichas acciones en los procesos del SGSI.
- La forma de evaluar la efectividad de estas acciones.

### 6.1.2. Valoración de los Riesgos de Seguridad de Información

La SUNAT define y aplica un proceso de gestión de riesgos de seguridad de la información que:

- Se establece y mantiene los criterios de riesgo de seguridad de la información, el cual define los niveles, criterios de aceptación del riesgo y los criterios para la realización de las valoraciones de riesgos de seguridad de la información.
- Asegura que las valoraciones de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables, para tal efecto se ha desarrollado el documento SGSI-ME-01 Metodología de Gestión de Riesgos de Seguridad de la Información.

  La metodología define las siguientes fases:
  - Identificación de riesgos de seguridad de la información, se realizan en talleres de trabajo, donde se identifican a los propietarios de los riesgos, ellos son responsables de aplicar el proceso de evaluación de riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información.
  - Análisis de los riesgos de seguridad de la información, se evalúan las posibles consecuencias que se derivarían si se materializan los riesgos identificados, se evalúa la probabilidad de ocurrencia de los mismos y se determinan sus niveles.
  - Evaluación de los riesgos de seguridad de la información, se comparan los resultados del análisis de riesgos con los criterios de riesgo y se priorizan los riesgos para su tratamiento.

- El proceso de evaluación de riesgos de seguridad de la información se realiza una vez al año o cuando ocurran cambios en los activos y/o en los procesos que forman parte del SGSI, lo que ocurra primero y se encuentra detallado en el documento SGSI-ME-01 Metodología de Gestión de Riesgos de Seguridad de la Información.

Este proceso es gestionado por el Oficial de Seguridad de la Información.

### 6.1.3. Información de Tratamiento de Riesgos de Seguridad de la Información

- La SUNAT ha definido y aplicado un procedimiento de tratamiento de riesgos de seguridad de la información para:
  - Seleccionar opciones de tratamiento de riesgos de seguridad de la información adecuadas teniendo en cuenta los resultados de la evaluación de riesgos.
  - Determinar los controles que sean necesarios para poner en práctica las opciones de tratamiento de riesgos de seguridad de la información elegidas.
  - Formular un Plan de Tratamiento de Riesgos de Seguridad de la Información.
  - Elaborar una Declaración de Aplicabilidad que contenga los controles necesarios, si aplican o no y la justificación de las inclusiones y exclusiones de los controles del Anexo A de la NTP ISO/IEC 27001:2014.
  - Obtener la aprobación del propietario del riesgo del Plan de Tratamiento de Riesgos de Seguridad de la Información y la aceptación de los riesgos residuales.
- El proceso de tratamiento de riesgos de seguridad de la información se encuentra detallado en el documento SGSI-ME-01 Metodología de Gestión de Riesgos de Seguridad de la Información.

Este proceso es gestionado por el Oficial de Seguridad de la Información en coordinación con el dueño del proceso.

### 6.2. Objetivos de Seguridad de la Información y Planeamiento para Alcanzarlos

La SUNAT ha definido sus objetivos de seguridad de la información en el documento SGSI-OD-04 Objetivos de Seguridad de la Información.

Estos objetivos serán medidos de acuerdo al documento SGSI-ME-02 Metodología de Medición del Sistema de Gestión de Seguridad de la Información.

## 7. APOYO

### 7.1. Recursos

La provisión de recursos necesarios para el Sistema de Gestión de Seguridad de la Información (SGSI) es propuesta por el Oficial de Seguridad de la Información y presentada al Comité de Gestión de Seguridad de la Información para su aprobación.

### 7.2. Competencia

- El personal que forma parte del SGSI cuenta con las competencias necesarias para desarrollar sus funciones, así como también recibe formación en seguridad de la información, según lo definido en el documento SGSI-PL-01 Plan de Capacitación y Sensibilización Integral en Seguridad de la Información.
- La Intendencia Nacional de Recursos Humanos mantiene los registros actualizados sobre la educación, formación, habilidades y experiencia del personal, en el “Legajo Personal”.

### 7.3. Conciencia

Para lograr la sensibilización y toma de conciencia del personal involucrado en el Sistema de Gestión de Seguridad de la Información se realizan charlas

de sensibilización donde se difunde los temas de seguridad de la información, su contribución a la eficacia del Sistema de Gestión de Seguridad de la Información incluyendo los beneficios de un mejor desempeño de seguridad de la información y las consecuencias del incumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, cuya asistencia por parte del personal es registrada en las listas que se elaboran para tal fin en el documento SGSI-PL-01 Plan de Capacitación y Sensibilización Integral en Seguridad de la Información. Este proceso es administrado por el Oficial de Seguridad de la Información en coordinación con la Intendencia Nacional de Recursos Humanos.

## 7.4. Comunicación

La SUNAT define diversos canales de comunicación para las comunicaciones internas y externas relacionadas con el Sistema de Gestión de Seguridad de la Información, pueden ser realizadas a través del intranet, documentos escritos, e-mails, reuniones, vía telefónica, manteniendo así diferentes canales de comunicaciones entre los niveles correspondientes.

Para tal efecto se ha definido el documento SGSI-PL-02 Plan de Comunicaciones del SGSI.

Este proceso es gestionado por el Oficial de Seguridad de la Información.

## 7.5. Información Documentada

### 7.5.1. Generalidades

El SGSI de la SUNAT incluye la siguiente información documentada:

- Información documentada requerida por la NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2ª Edición, dentro de las cuales tenemos:

  - Alcance.
  - Política.

- Proceso de evaluación de riesgos.
- Proceso de tratamiento de riesgos.
- Objetivos de seguridad de la información.
- Evidencia de la competencia del personal.
- Información documentada que los procesos de la Institución se llevan a cabo según lo planificado.
- Resultados de las evaluaciones de riesgos.
- Resultado del tratamiento de riesgos.
- Evidencia de los resultados del monitoreo y medición.
- Evidencias del programa y resultados de la auditoría.
- Evidencia de los resultados de la revisión por la dirección.
- Evidencia de la naturaleza de las no conformidades y acciones derivadas y, resultados de acciones correctivas.

- Además de la información documentada determinada por la SUNAT, como necesaria para medir la efectividad del Sistema de Gestión de Seguridad de la Información.

### 7.5.2. Creación y Actualización

La SUNAT ha definido el documento SGSI-PR-01 Procedimiento de Control de Información Documentada del SGSI, el cual incluye:

- La identificación y descripción (título, fecha, autor, entre los principales);
- Formato (el idioma, la versión, gráficos, entre otros) y los medios de comunicación (papel, electrónico, entre los principales), y
- La revisión y aprobación antes de su emisión.
- Revisión y actualización necesaria, y su aprobación nuevamente.
- La identificación y control de la información documentada de origen externo, que la SUNAT determinó que es necesaria para la planificación y operación del SGSI.

### 7.5.3. Control de la Información Documentada

La SUNAT ha definido un procedimiento para controlar la información documentada requerida por el SGSI y por la Norma NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2ª Edición denominado SGSI-PR-01 Procedimiento de Control de Información Documentada del SGSI el cual define las actividades para:

- La distribución, acceso, recuperación y uso.
- El almacenamiento y conservación, incluyendo la preservación de la legibilidad.
- El control de cambios (principalmente control de versiones), y la retención y disposición.

De acuerdo con ello se asegura que la información documentada:

- Esté disponible y apta para su uso, donde y cuando sea necesario, y esté protegida adecuadamente, de la pérdida de confidencialidad, uso indebido, o la pérdida de la integridad, entre otros.

## 8. FUNCIONAMIENTO

### 8.1. Planificación y Control Operacional

La SUNAT gestiona las actividades para planificar y ejecutar la identificación, análisis, evaluación y tratamiento de riesgos, de tal forma que se pueda asegurar la realización de estos procesos que son necesarios para cumplir los requisitos de seguridad de la información y para poner en práctica las acciones determinadas en el punto 6.1. La SUNAT debe también implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2.

### 8.2. Información de la Evaluación de Riesgos de Seguridad

La SUNAT lleva a cabo las evaluaciones de riesgos de seguridad de información una vez al año o cuando se produzcan cambios significativos en

los procesos y/o activos de información parte del alcance del SGSI, teniendo en cuenta los criterios establecidos los cuales se registran en el documento SGSI-ME-01.FO-02 Matriz de Riesgos de Seguridad de la Información.

### 8.3. Información Sobre el Tratamiento de Riesgos de Seguridad

La SUNAT ha implementado el plan de tratamiento de riesgos de seguridad de la información, el cual se encuentra documentado en el documento SGSI-ME-01.FO-03 Plan de Tratamiento de Riesgos.

## 9. EVALUACIÓN DEL RENDIMIENTO

### 9.1. Monitoreo, Medición, Análisis y Evaluación

La SUNAT ha definido una metodología para el desarrollo de indicadores, la cual permite evaluar el rendimiento de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información, de tal forma que se produzcan resultados comparables y reproducibles para ser considerados válidos, la cual se encuentra plasmada en el documento SGSI-ME-02 Metodología de Medición del Sistema de Gestión de Seguridad de la Información, en el cual se define:

- Lo que se necesita monitorear y medir incluyendo los controles y procesos de seguridad de la información.
- Los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para garantizar resultados válidos.
- Cuando se llevará a cabo el seguimiento y medición.
- Quién es el responsable de controlar y medir.
- Cuando se debe analizar y evaluar los resultados de monitoreo y medición.
- Quién es el responsable de analizar y evaluar los resultados.

### 9.2. Auditoría Interna

- La SUNAT ha definido un proceso de auditorías internas, el cual se realiza a intervalos planificados para proporcionar información sobre si el Sistema de Gestión de Seguridad de la Información:

- Se encuentra conforme con los requisitos propios de la Institución en cuanto al Sistema de Gestión de Seguridad de la Información establecidos y los requisitos de la Norma NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2ª Edición.
- Se ha implantado y se mantiene de manera eficaz para alcanzar los objetivos del sistema.

- La planificación, establecimiento, implementación y mantenimiento del programa de auditoría que incluye la definición de criterios de auditoría y el alcance de cada auditoría, incluyendo lo referente a la selección de auditores y la realización de auditorías que garanticen la objetividad e imparcialidad del proceso de auditoría, así como el establecimiento de los mecanismos de comunicación e información, se describen en el documento SGSI-PR-03 Procedimiento de Auditoría Interna.
- El Oficial de Seguridad de la Información mantiene la información documentada del programa de auditoría y de los resultados de las auditorías internas realizadas.

### 9.3. Revisión por Parte de la Dirección

- El Comité de Gestión de Seguridad de la Información efectúa por lo menos una vez al año la revisión del SGSI con el apoyo del Oficial de Seguridad de la Información, con la finalidad de asegurar su conformidad, adecuación y eficacia continua. Para ello se ha establecido el documento SGSI-PR-02 Procedimiento de Revisión por la Dirección del Sistema de Gestión de Seguridad de la Información. La revisión incluye la evaluación de oportunidades de mejora y la necesidad de realizar cambios asociados a:
  - Estado de las acciones de revisiones por parte de la Dirección anteriores.
  - Los cambios que podrían afectar al SGSI.
  - Retroalimentación sobre el desempeño de seguridad de la información, incluir:
    - No conformidades y acciones correctivas.
    - Seguimiento y medición de los resultados.

- Resultados de auditorías.
- Cumplimiento de los objetivos de seguridad de la información.
- Necesidades de las partes interesadas.

- Estado de los proyectos relacionados al SGSI.
- Los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.
- Las oportunidades para la mejora continua.

- Los resultados de la revisión por parte de la dirección incluyen las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el SGSI.

## 10. MEJORAMIENTO

### 10.1. No Conformidad y Acciones Correctivas

Con la finalidad de eliminar las causas de las No Conformidades, evitar su repetición y asegurar que las acciones correctivas sean eficaces y apropiadas a los efectos de las No Conformidades encontradas, se ha establecido el documento SGSI-PR-04 Procedimiento de Acciones Correctivas del Sistema de Gestión de Seguridad de la Información, en este documento se definen los requisitos para:

- Reaccionar a la inconformidad y según sea el caso:
  - Adoptar medidas para controlar y corregir.
  - Hacer frente a las consecuencias.
- Evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidad, con el fin de que no se repita o se produzca en otros lugares, a través de:
  - La revisión de la no conformidad.
  - Determinar las causas de la no conformidad.
  - Determinar si existen incumplimientos similares o que podrían ocurrir potencialmente.
- Poner en práctica las medidas oportunas.
- Revisar la efectividad de las medidas correctivas tomadas.
- Realizar cambios en el Sistema de Gestión de Seguridad de la Información, si es necesario.

### 10.2. Mejora Continua

La SUNAT gestiona los procesos necesarios para mejorar continuamente la conveniencia, adecuación y efectividad del SGSI a través de la política y objetivos de seguridad de la información, los resultados de las auditorías internas, acciones correctivas, revisión por la dirección u otra información relevante, para ello se cuenta con el documento SGSI-PR-05 Procedimiento de Mejora Continua del Sistema de Gestión de Seguridad de la Información.

## 11. CONTROL DE CAMBIOS

| Detalle | Versión | Fecha de Aprobación | Responsable |
|---|---|---|---|
| Versión inicial | 01 | 25/01/2019 | Oficial de Seguridad de la Información |