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

ÍNDICE

1. OBJETIVO Y CAMPO DE APLICACIÓN

El presente documento tiene como objetivo documentar cada una de las cláusulas obligatorias 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, la cual está basada en la norma internacional 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, que aprueba el uso obligatorio de la NTP-ISO/IEC 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial Nº 004-2016-PCM.

3. DEFINICIONES

3.1. Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, equipamiento informático, edificios, personas, etc.) que tenga valor para la organización.

3.2. Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo. El análisis de riesgos proporciona la base para la evaluación de riesgos y las decisiones sobre el tratamiento de riesgos.

3.3. Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a personas, entidades o procesos no autorizados.

3.4. Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona, entidad o proceso autorizado.

3.5. Gestión de Riesgos: Actividades coordinadas para dirigir y controlar el riesgo en una entidad.

3.6. Integridad: Propiedad de la información relativa a su exactitud y completitud.

3.7. Revisión por la Dirección: Actividad realizada por la Alta Dirección (a través del Comité de Gobierno Digital), a intervalos planificados, para determinar la idoneidad, adecuación y efectividad del SGSI de la institución para lograr los objetivos establecidos.

3.8. Riesgo de Seguridad de la Información: Potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, cause daños a una organización.

3.9. Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información cualquiera sea su formato y soporte. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y confiabilidad también pueden estar involucradas.

3.10. Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

4. CONTEXTO DE LA ORGANIZACIÓN

4.1. La 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 Contexto de SUNAT (SGSI-OD-01).

4.2. Comprender las Necesidades y Expectativas de las Partes Interesadas

Las necesidades y expectativas de las partes interesadas se han identificado y plasmado en el documento Contexto de SUNAT (SGSI-OD-01).

4.3. Determinar el Alcance del SGSI

Después de analizar el contexto externo, el contexto interno y comprender las necesidades y expectativas de las partes interesadas, se ha determinado el alcance del SGSI de la institución en el documento Alcance del SGSI (SGSI-OD-02).

4.4. Sistema de Gestión de Seguridad de la Información

El SGSI de la SUNAT se ha establecido y se implementa, mantiene y mejora continuamente, 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.

5. LIDERAZGO

5.1. Liderazgo y Compromiso

La SUNAT demuestra su liderazgo y compromiso con el SGSI, con las siguientes acciones:

- Estableciendo la Política y los Objetivos de Seguridad de la Información alineados a los objetivos estratégicos de la institución.
- Conformando el Comité de Gobierno Digital, así como otros roles y responsabilidades en seguridad de la información.
- Identificando e incluyendo los requisitos de seguridad en los procesos que forman parte del alcance del SGSI.

- Asegurando la disponibilidad de los recursos necesarios para la implementación y operación del 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 institución ha definido la siguiente política de seguridad de la información:

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.

Dicha política, aprobada el 4 de mayo de 2018, ha sido plasmada en el documento Política de Seguridad de la Información (SGSI-PO-01).

5.3. Roles, Responsabilidades y Autoridades Organizacionales

En la institución, se han definido roles y asignado responsabilidades del SGSI. Para tal efecto, se ha elaborado el Manual de Roles, Responsabilidades y Autoridades Organizacionales del SGSI (SGSI-MA-02).

6. PLANIFICACIÓN

6.1. Acciones para Abordar los Riesgos y Oportunidades

6.1.1. Generalidades

El Comité de Gobierno Digital asegura que la planificación del SGSI se lleve a cabo con el fin de cumplir con lo definido en los numerales 4.1 y 4.2 del presente manual, y que se hayan determinado los riesgos y oportunidades según lo definido en la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01), 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 por 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

En la institución se ha definido y se aplica la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01) en el que:

- Se establecen y mantienen los criterios de riesgo de seguridad de la información como, por ejemplo, los niveles de riesgo, criterios de aceptación del riesgo y los criterios para la realización de las valoraciones de riesgos de seguridad de la información.
- Se asegura que las valoraciones de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables.

El proceso de gestión de riesgos de seguridad de la información se realiza una vez al año o cuando ocurran cambios significativos[1] en la entidad, en los activos de información y/o en los procesos que forman parte del SGSI, lo que ocurra primero.

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

En la institución se ha definido y se aplica la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01) para:

- Seleccionar las opciones de tratamiento de riesgos de seguridad de la información más adecuadas, teniendo en cuenta los resultados de la evaluación de riesgos, y determinar los controles que sean necesarios para su implementación.
- Plasmar dichas definiciones en un Plan de Tratamiento de Riesgos de Seguridad de la Información.

[1] Puede considerarse, por ejemplo, cambios en la estructura organizacional, así como en las designaciones en cargos de la Alta Dirección o de las áreas cuyos procesos forman parte del alcance del SGSI, entre otros.

- Elaborar una Declaración de Aplicabilidad en el que se identifique la aplicación 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 sobre el Plan de Tratamiento de Riesgos de Seguridad de la Información y la aceptación de los riesgos residuales.

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

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 Objetivos de Seguridad de la Información (SGSI-OD-04).

Estos objetivos son medidos de acuerdo con lo indicado en la Metodología de Medición del SGSI (SGSI-ME-02).

7. SOPORTE

7.1. Recursos

La provisión de recursos necesarios para el SGSI es propuesta por el Oficial de Seguridad de la Información y presentada al Comité de Gobierno Digital, presidido por el Superintendente Nacional o su representante, para su gestión.

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 Plan de Capacitación y Sensibilización Integral en Seguridad de la Información (SGSI-PL-01).

La INRH 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 SGSI, se realizan charlas de sensibilización donde se difunde los temas de seguridad de la información, su contribución a la eficacia del SGSI incluyendo los beneficios de un mejor desempeño de seguridad de la información y las consecuencias del incumplimiento de los requisitos del SGSI. La asistencia por parte del personal es registrada en el formato Lista de Asistencia (SGSI-PL-01.FO-01) elaborada para tal fin de acuerdo con lo definido en el Plan de Capacitación y Sensibilización Integral en Seguridad de la Información (SGSI-PL-01). Este proceso es administrado por el Oficial de Seguridad de la Información en coordinación con la INRH.

7.4. Comunicación

Se han definido diversos canales para las comunicaciones internas y externas relacionadas con el SGSI. Dichas comunicaciones pueden ser realizadas a través de la intranet o por documentos escritos, e-mails, reuniones o vía telefónica. Para tal efecto se ha definido el Plan de Comunicaciones del SGSI (SGSI-PL-02). 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 información documentada requerida por la NTP-ISO/IEC 27001:2014, como, por ejemplo, el alcance del SGSI y la política de seguridad de la información, el proceso de evaluación y tratamiento de riesgos de seguridad de la información, entre otros; además de la información documentada determinada por la SUNAT, como necesaria para medir la efectividad del SGSI.

7.5.2. Creación y Actualización

La SUNAT ha definido el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01), 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
- Los niveles de elaboración, revisión y aprobación de los documentos.
- 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

Se ha definido el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01) con la finalidad de controlar la información documentada requerida por el SGSI y por la NTP-ISO/IEC 27001:2014. En dicho documento se definen las actividades para:

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

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 institución gestiona las actividades para planificar y ejecutar el 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. Para tal fin, se ha definido la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01) y, anualmente, se elabora el Plan de Trabajo del SGSI de manera tal que se pongan en práctica las acciones determinadas en el numeral 6.1 y se logren los objetivos de seguridad de la información según lo indicado en el numeral 6.2.

8.2. Información de la Evaluación de Riesgos de Seguridad

De acuerdo con lo establecido en la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01), se llevan a cabo las evaluaciones de riesgos de seguridad de información una vez al año o cuando se produzcan cambios significativos en la entidad, en los procesos y/o activos de información que forman parte del alcance del SGSI teniendo en cuenta los criterios establecidos en dicho documento. Los resultados de las evaluaciones se plasman en el formato Matriz de Riesgos de Seguridad de la Información (SGSI-ME-01.FO-02).

8.3. Tratamiento de Riesgos de Seguridad de la Información

La SUNAT ha implementado planes de tratamiento de riesgos de seguridad de la información, los cuales se plasman en el formato Plan de Tratamiento de Riesgos (SGSI-ME-01.FO-03) establecido como parte de la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01).

9. EVALUACIÓN DEL RENDIMIENTO

9.1. Monitoreo, Medición, Análisis y Evaluación

Se ha definido la Metodología de Medición del SGSI (SGSI-ME-02), la cual permite evaluar el rendimiento de la seguridad de la información y la eficacia del SGSI, de tal forma que se produzcan resultados comparables y reproducibles para ser considerados válidos. En dicho documento 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.

- Cuándo se llevará a cabo el seguimiento y medición.
- Quién es el responsable de controlar y medir.
- Cuándo 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

Se ha definido un proceso de auditorías internas, el cual se realiza a intervalos planificados para proporcionar información sobre si el SGSI:

- Se encuentra conforme con los requisitos propios de la Institución en cuanto al SGSI establecidos y los requisitos de la NTP-ISO/IEC 27001:2014.
- 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 Procedimiento de Auditoría Interna (SGSI-PR-03).

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 la Dirección

El Comité de Gobierno Digital 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. Lo antes indicado, es informado por el Oficial de Seguridad de la Información a través del Reporte de Revisión del SGSI (SGSI-MA-01.FO-01). La revisión

incluye la evaluación de oportunidades de mejora y la necesidad de realizar cambios asociados a:

- Estado de las acciones de revisiones anteriores por parte de la Dirección.
- Los cambios que podrían afectar al SGSI.
- Retroalimentación sobre el desempeño de seguridad de la información, considerando:
  - 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. MEJORAS

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 Procedimiento de Acciones Correctivas del SGSI (SGSI-PR-04). En este documento se definen los requisitos para:

- Reaccionar a la no conformidad 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 las no conformidades, 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 SGSI, si es necesario.

10.2. Mejora Continua

La institución 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, acciones correctivas, revisión por la dirección u otra información relevante que permita implementar oportunidades de mejora, para lo cual se cuenta con el Procedimiento de Mejora Continua del SGSI (SGSI-PR-05).

11. REGISTROS Y ANEXOS

a) SGSI-MA-01.FO-01 Reporte de Revisión del SGSI.

12. CONTROL DE CAMBIOS

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial	01	25/01/2019	Oficial de Seguridad de la Información
Actualización de definiciones y roles como el Comité de Gobierno Digital. Inclusión del formato Reporte de Revisión del SGSI (SGSI-MA-01.FO-01)	02	22/03/2023	Oficial de Seguridad de la Información