



Manual del Sistema de Gestión de Seguridad de la Información Versión 3

Código:
SGSI-MA-01

Modificado por: Karina Miranda Vásquez Oficial de Seguridad y Confianza Digital	Revisado por: Carlos Rojas Chávez Presidente del CGTD	Aprobado por: Javier Franco Castillo Superintendente Nacional de Aduanas y de Administración Tributaria
--	---	---

Gerencia de Seguridad de la Información
Superintendencia Nacional de Aduanas y de Administración
Tributaria

Enero 2026

CUADRO DE CONTROL DE CAMBIOS

Ítem	Breve descripción del cambio	Fecha del documento	Versión	Responsable del documento
1	Versión inicial del documento.	25/01/2019	1	Oficial de Seguridad de la Información
2	Actualización de definiciones y roles como el Comité de Gobierno Digital. Inclusión del formato Reporte de Revisión del SGSI (SGSI-MA-01.FO-01).	22/03/2023	2	Oficial de Seguridad y Confianza Digital
3	- En todo el documento se han hecho actualizaciones en el marco de la adecuación a la nueva norma ISO/IEC 27001:2022. Asimismo, se han actualizado los nombres y siglas del Oficial de Seguridad y Confianza Digital (OSCD) y del Comité de Gobierno y Transformación Digital (CGTD). - En el numeral 5.3, se ha incluido el detalle del alcance del SGSI, anteriormente definido en el documento Alcance del SGSI (SGSI-OD-02). Se incluye proceso de atención de denuncias por presuntos actos de corrupción y medidas de protección al denunciante en la SUNAT, y el proceso de aplicación de criterios para asegurar la calidad de datos utilizados en la gestión de riesgos, además de las unidades orgánicas de fiscalización a nivel nacional y los centros de cómputo para el proceso de intercambio de información. - En el numeral 7.2, se ha incluido el detalle de los objetivos de seguridad de la información, el cual anteriormente estaba definido en el documento Objetivos de Seguridad de la Información (SGSI-OD-04). Los objetivos han sido actualizados. - Se ha incluido el numeral 7.3 en el marco de la adecuación a la nueva norma ISO/IEC 27001:2022. - En el numeral 9.1, se ha incluido la Lista de Verificación de Controles del SGSI (SGSI-MA-01.FO-07).	13/01/2026	3	Karina Miranda Vásquez - Oficial de Seguridad y Confianza Digital Omar Gonzales Elías - Gerente de Seguridad de la Información

Ítem	Breve descripción del cambio	Fecha del documento	Versión	Responsable del documento
	• En el numeral 10.1, se ha reemplazado la Metodología de Medición del SGSI (SGSI-ME-02) por el Tablero de Indicadores del SGSI (SGSI-MA-01.FO-06). • En el numeral XII, se han incluido nuevos registros: Contexto de la SUNAT, Plan de Operación y Mantenimiento del SGSI, Lista de Asistencia, Plan de Comunicaciones del SGSI, Tablero de Indicadores del SGSI y la Lista de Verificación de Controles del SGSI. En todo el documento se han hecho referencias a estos nuevos formatos.			

ÍNDICE

SIGLAS	5
I. OBJETIVO	6
II. ALCANCE	6
III. BASE NORMATIVA	6
IV. GLOSARIO DE TÉRMINOS	7
V. CONTEXTO DE LA ORGANIZACIÓN	8
VI. LIDERAZGO	9
VII. PLANIFICACIÓN	10
VIII. SOPORTE	12
IX. OPERACIÓN	13
X. EVALUACIÓN DEL DESEMPEÑO	14
XI. MEJORA	16
XII. REGISTROS	16

SIGLAS

- **CGTD:** Comité de Gobierno y Transformación Digital.
- **DN:** Dirección de Normalización del INACAL.
- **GSI:** Gerencia de Seguridad de la Información de la INSI.
- **IEC:** Comisión Electrotécnica Internacional (International Electrotechnical Commission, en inglés).
- **INACAL:** Instituto Nacional de Calidad.
- **INRH:** Intendencia Nacional de Recursos Humanos.
- **INSI:** Intendencia Nacional de Sistemas de Información.
- **ISO:** Organización Internacional de Normalización (International Organization for Standardization, en inglés).
- **NTP:** Norma Técnica Peruana.
- **OSCD:** Oficial de Seguridad y Confianza Digital.
- **PCM:** Presidencia del Consejo de Ministros.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SN:** Superintendente Nacional.
- **SUNAT:** Superintendencia Nacional de Aduanas y de Administración Tributaria.
- **UUOO:** Unidad o Unidades de Organización.

I. OBJETIVO

El presente documento tiene como objetivo documentar cada una de las cláusulas obligatorias de la NTP-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3era Edición, la cual está basada en la norma internacional ISO/IEC 27001:2022, que la SUNAT debe cumplir para mantener su SGSI.

II. ALCANCE

El presente documento es de aplicación obligatoria para todas las UUOO involucradas en el SGSI.

III. BASE NORMATIVA

- Decreto Legislativo N.º 1412, que aprueba la Ley de Gobierno Digital.
- Resolución de Superintendencia N.º 050-2019/SUNAT, que aprueba documentos concernientes al Sistema de Gestión de Seguridad de la Información de la SUNAT.
- Decreto de Urgencia N.º 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N.º 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N.º 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N.º 157-2021-PCM, que aprueba el reglamento del Decreto de Urgencia N.º 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Resolución Directoral N.º 022-2022-INACAL/DN, que aprueba la NTP-ISO/IEC 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3era Edición”.
- Resolución de Superintendencia N.º 148-2023/SUNAT, que modifica los documentos referentes al Sistema de Gestión de Seguridad de la Información de la SUNAT.
- Resolución de Secretaría de Gobierno y Transformación Digital N.º 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.

- Resolución de Superintendencia N.º 000395-2025/SUNAT, que aprueba el Plan Estratégico Institucional para el periodo 2026-2030 de la SUNAT.

IV. GLOSARIO DE TÉRMINOS

- 4.1. **Activo de Información:** Es cualquier información o elemento relacionado (sistemas, soportes, equipamiento informático, edificios, personas, etc.) que tenga valor para una organización. Los activos son los recursos necesarios para que la entidad funcione y consiga los objetivos que se ha propuesto.
- 4.2. **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.
- 4.3. **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a personas, entidades o procesos no autorizados.
- 4.4. **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona, entidad o proceso autorizado.
- 4.5. **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar el riesgo en una entidad.
- 4.6. **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- 4.7. **Revisión por la Dirección:** Actividad realizada por la Alta Dirección (a través del CGTD), a intervalos planificados, para determinar la idoneidad, adecuación y efectividad del SGSI de la institución para lograr los objetivos establecidos.
- 4.8. **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.
- 4.9. **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.
- 4.10. **Sistema de Gestión de Seguridad de la Información:** 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.

V. CONTEXTO DE LA ORGANIZACIÓN

5.1. La SUNAT y su Contexto

La Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT, de acuerdo a su Ley de Creación N.º 24829, Ley General aprobada por Decreto Legislativo N.º 501 y la Ley N.º 29816, Ley 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.º 061-2002-PCM, expedido al amparo de lo establecido en el numeral 13.1 del artículo 13º de la Ley N.º 27658, ha absorbido a la Superintendencia Nacional de Aduanas, asumiendo las funciones, facultades y atribuciones que por ley, correspondían a esta entidad.

La SUNAT determina su contexto externo e interno en el formato Contexto de la SUNAT (SGSI-MA-01.FO-02), el cual es revisado, por lo menos, una vez al año.

5.2. Comprender las Necesidades y Expectativas de las Partes Interesadas

Las necesidades y expectativas de las partes interesadas se identifican y plasman en el formato Contexto de la SUNAT (SGSI-MA-01.FO-02) , el cual es revisado, por lo menos, una vez al año.

5.3. Determinar el Alcance del SGSI

En base a los aspectos internos y externos, las necesidades y expectativas de las partes interesadas y las interfaces y dependencias entre actividades realizadas en la institución, se ha definido el alcance del SGSI en la SUNAT de la siguiente manera:

Un SGSI de conformidad con el estándar NTP-ISO/IEC 27001:2022, para los procesos de:

- **Intercambio de información con Administraciones Tributarias del extranjero**, realizado en las siguientes sedes:
 - Sede Central, Edificio San Mateo y Edificio Sulamérica - Av. Garcilaso de la Vega 1472, Lima.
 - Sede Miraflores - Av. Benavides 222, Miraflores.
 - Unidades orgánicas de fiscalización realizadas en las dependencias a nivel nacional.
 - Centros de cómputo.
- **Aplicación de criterios para asegurar la calidad de datos utilizados en la gestión de riesgos**, realizado en las siguientes sedes:
 - Sede Central, Edificio San Mateo y Edificio Sulamérica - Av. Garcilaso de la Vega 1472, Lima.

- **Atención de denuncias por presuntos actos de corrupción y medidas de protección al denunciante en la SUNAT**, realizado en las siguientes sedes:
 - Sede Central, Edificio Sulamérica - Av. Garcilaso de la Vega 1472, Lima.

El detalle de los activos de información que forman parte de los procesos antes indicados se encuentra en los Inventarios de Activos de Información (SGSI-ME-01.FO-01) de cada proceso.

5.4. Sistema de Gestión de Seguridad de la Información

El SGSI de la SUNAT se ha establecido y se implementa, mantiene y mejora continuamente, para los procesos descritos en el numeral 5.3 y sus interacciones, de acuerdo con los requisitos de la NTP-ISO/IEC 27001 vigente.

VI. LIDERAZGO

6.1. 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 CGTD, 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 eficacia 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.

6.2. 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).

6.3. 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).

VII. PLANIFICACIÓN

7.1. Acciones para Abordar los Riesgos y Oportunidades

7.1.1. Generalidades

El CGTD 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 implementar 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 eficacia de estas acciones.

7.1.2. Evaluación 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 la que:

- Se establecen y mantienen los criterios de riesgo de seguridad de la información como, por ejemplo: i) los niveles de riesgo; ii) los criterios de aceptación del riesgo; y, iii) 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.

Este proceso es gestionado por el OSCD.

7.1.3. 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.
- 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 vigente.
- 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 OSCD.

7.2. Objetivos de Seguridad de la Información y su Planificación para Conseguirlos

7.2.1. Objetivos de Seguridad de la Información

La SUNAT ha definido los siguientes objetivos de seguridad de la información:

- **OBJ-1:** Gestionar el tratamiento de los incidentes de seguridad de la información identificados en los procesos del alcance del SGSI y con impacto crítico.
- **OBJ-2:** Concientizar y sensibilizar en aspectos de seguridad de la información al personal involucrado en el alcance del SGSI.

- **OBJ-3:** Verificar que las cuentas y perfiles de acceso hayan sido otorgadas en función de las necesidades institucionales, las competencias y las funciones de las áreas del alcance del SGSI.

El detalle de la medición de los objetivos de seguridad de la información y la planificación de su seguimiento se encuentran definidos en el Tablero de Indicadores del SGSI (SGSI-MA-01.FO-06) y en el Plan de Operación y Mantenimiento del SGSI (SGSI-MA-01.FO-03).

7.3. Planificación de Cambios

Los cambios en el SGSI se realizan de manera planificada y definidos en el Plan de Operación y Mantenimiento del SGSI (SGSI-MA-01.FO-03).

VIII. SOPORTE

8.1. Recursos

La provisión de recursos necesarios para el SGSI es propuesta por el OSCD y presentada al CGTD, presidido por el SN o su representante, para su gestión.

8.2. 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. La INRH mantiene los registros actualizados sobre la educación, formación, habilidades y experiencia del personal, en el "Legajo Personal".

8.3. Toma de 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-MA-01.FO-04) elaborada para tal fin de acuerdo con lo definido en el Plan de Operación y Mantenimiento del SGSI (SGSI-MA-01.FO-03). Este proceso es administrado por el OSCD en coordinación con la INRH.

8.4. 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 formato Plan de Comunicaciones del SGSI (SGSI-MA-01.FO-05). Este proceso es gestionado por el OSCD.

8.5. Información Documentada

8.5.1. Generalidades

El SGSI de la SUNAT incluye la información documentada requerida por la NTP-ISO/IEC 27001 vigente, 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.

8.5.2. Creación y Actualización

La SUNAT ha definido el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01) que, como parte de la creación y actualización de la información documentada, incluye:

- La identificación y descripción (título, fecha, autor, entre otros).
- Formato (el idioma, la versión, gráficos, entre otros) y los medios de comunicación (papel, electrónico, entre otros).
- Los niveles de elaboración, revisión y aprobación de los documentos.
- La identificación de la información documentada de origen externo, que la SUNAT determinó que es necesaria para la planificación y operación del SGSI.

8.5.3. 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 vigente. 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.

IX. OPERACIÓN

9.1. Planificación y Control Operacional

La institución gestiona las actividades para planificar y ejecutar el análisis, evaluación y tratamiento de riesgos de seguridad de la información, 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 los cambios en el SGSI. Asimismo, se gestionan los objetivos 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), el Tablero de Indicadores del SGSI (SGSI-MA-01.FO-06), la Lista de Verificación de Controles del SGSI (SGSI-MA-01.FO-07) y, anualmente, se elabora el Plan de Operación y Mantenimiento del SGSI (SGSI-MA-01.FO-03) de manera tal que se pongan en práctica las acciones determinadas en el numeral VII.

9.2. 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 en intervalos planificados o cuando se produzcan cambios significativos¹ en la entidad, en los procesos y/o activos de información que forman parte del alcance del SGSI, lo que ocurra primero, 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).

9.3. 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).

X. EVALUACIÓN DEL DESEMPEÑO

10.1. Seguimiento, Medición, Análisis y Evaluación

Se ha definido el Tablero de Indicadores del SGSI (SGSI-MA-01.FO-06), el 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 del seguimiento y la medición.
- Cuándo se debe analizar y evaluar los resultados del seguimiento y medición.
- Quién es el responsable de analizar y evaluar los resultados.

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.

10.2. 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 entidad y los requisitos de la NTP-ISO/IEC 27001 vigente.
- 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 OSCD mantiene la información documentada del programa de auditoría y de los resultados de las auditorías internas realizadas.

10.3. Revisión por la Dirección

El CGTD efectúa, por lo menos una vez al año, la revisión del SGSI, con el apoyo del OSCD, con la finalidad de asegurar su conformidad, adecuación y eficacia continua. Lo antes indicado, es informado por el OSCD 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 (CGTD) incluyen las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el SGSI.

XI. MEJORA

11.1. Mejora Continua

La institución gestiona los procesos necesarios para mejorar continuamente la conveniencia, adecuación y eficacia 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).

11.2. 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 eficacia de las medidas correctivas tomadas.
- Realizar cambios en el SGSI, si es necesario.

XII. REGISTROS

Código	Nombre del registro	Responsable
SGSI-MA-01.FO-01	Reporte de Revisión del SGSI	OSCD
SGSI-MA-01.FO-02	Contexto de la SUNAT	OSCD
SGSI-MA-01.FO-03	Plan de Operación y Mantenimiento del SGSI	OSCD
SGSI-MA-01.FO-04	Lista de Asistencia	OSCD
SGSI-MA-01.FO-05	Plan de Comunicaciones del SGSI	OSCD
SGSI-MA-01.FO-06	Tablero de Indicadores del SGSI	OSCD
SGSI-MA-01.FO-07	Lista de Verificación de Controles del SGSI	OSCD