



Manual de Roles, Responsabilidades y Autoridades Organizacionales del Sistema de Gestión de Seguridad de la Información Versión 3

Código:
SGSI-MA-02

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	Modificación del rol de Usuarios por el de Colaboradores de la SUNAT y personal bajo modalidades formativas y terceros vinculados con la institución. Actualización de definiciones y otros.	22/03/2023	2	Oficial de Seguridad y Confianza Digital
3	- En el documento se han hecho actualizaciones en el marco de la adecuación a la nueva norma ISO/IEC 27001:2022. - En todo el documento se han actualizado los nombres y las siglas del Oficial de Seguridad y Confianza Digital (OSCD) y del Comité de Gobierno y Transformación Digital (CGTD). - Se ha actualizado la estructura del documento de acuerdo con lo definido en el Procedimiento de Control de Información Documentada del SGSI. - En el numeral V, se ha incluido el rol del Equipo de Respuestas ante Incidentes de Seguridad Digital de la SUNAT. - En el numeral VI, se han incluido las responsabilidades del Equipo de Respuestas ante Incidentes de Seguridad Digital de la SUNAT. - En el numeral VI, para el caso del Superintendente Nacional, se ha incluido una nueva responsabilidad relacionada con el Equipo de Respuestas ante Incidentes de Seguridad Digital. - En el numeral VI, se ha incluido una nueva responsabilidad para los Intendentes, Gerentes o Jefes de las UUOO: Desempeñar los roles de propietario del activo de información, propietario del riesgo y/o custodio del activo de información según el activo de información bajo su control, pudiendo designar a los colaboradores a su cargo como respaldo para garantizar la continuidad en la gestión de dichos roles.	13/01/2026	3	Karina Miranda Vásquez - Oficial de Seguridad y Confianza Digital Omar Gonzales Elías - Gerente de Seguridad de la Información

ÍNDICE

SIGLAS	4
I. OBJETIVO	5
II. ALCANCE.....	5
III. BASE NORMATIVA	5
IV. GLOSARIO DE TÉRMINOS	6
V. ORGANIZACIÓN INTERNA	7
VI. RESPONSABILIDADES DEL SGSI.....	8

SIGLAS

- **CGTD:** Comité de Gobierno y Transformación Digital.
- **DN:** Dirección de Normalización del INACAL.
- **ERISD:** Equipo de Respuestas ante Incidentes de Seguridad Digital.
- **GSI:** Gerencia de Seguridad de la Información de la INSI.
- **IEC:** Comisión Electrotécnica Internacional (International Electrotechnical Commission, en inglés).
- **INACAL:** Instituto Nacional de Calidad.
- **INSI:** Intendencia Nacional de Sistemas de Información.
- **INRH:** Intendencia Nacional de Recursos Humanos.
- **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.
- **UOOO:** Unidad o Unidades de Organización.

I. OBJETIVO

Asignar de manera efectiva los roles, las responsabilidades y las autoridades organizacionales para la dirección, gestión y operación del SGSI, atendiendo al principio de segregación de funciones entre los integrantes de la entidad en aspectos relacionados al SGSI.

II. ALCANCE

El presente documento aplica a todos los colaboradores y personal bajo modalidades formativas y terceros vinculados con la institución que forman parte de los procesos del alcance del SGSI y a quienes se les haya asignado roles en el marco de la seguridad de la información.

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 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.
- 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 044-2022-SUNAT, que conforma el Equipo de Respuestas ante Incidentes de Seguridad Digital de la SUNAT.
- 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 177-2024/SUNAT, que designa al Oficial de Seguridad y Confianza Digital.

- 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. Comité de Gobierno y Transformación Digital:** Es un comité ejecutivo conformado por altos directivos de la entidad, designados para gestionar, supervisar, revisar e informar, de manera permanente, los aspectos del SGSI. El Comité es presidido por el Superintendente Nacional y tiene como secretario técnico al Intendente de INSI. La conformación del Comité se encuentra aprobado por la Resolución de Superintendencia vigente.
- 4.3. Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a personas, entidades o procesos no autorizados.
- 4.4. Custodio del Activo de Información:** Persona o entidad que tiene la responsabilidad de mantener un adecuado nivel de protección de los activos de información en base a las especificaciones coordinadas con el Propietario del Activo de Información.
- 4.5. Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona, entidad o proceso autorizado.
- 4.6. Equipo de Gestión de Riesgos:** Es el conjunto multidisciplinario de especialistas de la institución que se conforma previo al inicio de las actividades de gestión de riesgos con la finalidad de llevar a cabo dicha gestión. Entre sus miembros se debe considerar al Oficial de Seguridad y Confianza Digital, al Custodio del Activo de Información, al Propietario del Activo de Información, al Propietario del Riesgo, al personal de la Gerencia de Seguridad de la Información y del proceso del cual se quiere evaluar los riesgos, entre otros que se consideren necesarios. Los miembros indicados pueden designar a sus representantes.
- 4.7. Evento de Seguridad de la Información:** Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.
- 4.8. Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- 4.9. Incidente de Seguridad de la Información:** Un evento o una serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer los procesos, operaciones o la prestación de servicios de la entidad y amenazar la seguridad de la información de la entidad pública.

- 4.10. Oficial de Seguridad y Confianza Digital:** Es el responsable operativo de la implementación y mantenimiento del SGSI. Es designado mediante Resolución de Superintendencia. De acuerdo con lo indicado en la cuarta disposición complementaria final del Decreto Supremo N.º 157-2021-PCM, toda mención que se efectúe respecto al Oficial de Seguridad de la Información deberá entenderse como realizada al Oficial de Seguridad y Confianza Digital.
- 4.11. Propietario del Activo de Información:** Persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la recepción, producción, desarrollo, mantenimiento, uso y seguridad de los activos. Tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo de información.
- 4.12. Propietario del Riesgo:** Persona o entidad que tiene la responsabilidad y la autoridad para gestionar un riesgo.
- 4.13. 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.
- 4.14. 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 la confiabilidad también pueden estar involucradas.
- 4.15. 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.

V. ORGANIZACIÓN INTERNA

La SUNAT dirige el SGSI a través del Comité de Gobierno y Transformación Digital, presidido por el Superintendente Nacional o su representante, en coordinación con el Oficial de Seguridad y Confianza Digital. Los roles y autoridades identificados que soportan el SGSI son los siguientes:

- Superintendente Nacional.
- Comité de Gobierno y Transformación Digital (CGTD).
- Oficial de Seguridad y Confianza Digital.
- Equipo de Respuestas ante Incidentes de Seguridad Digital de la SUNAT.
- Equipo de Gestión de Riesgos.
- Propietario del Activo de Información.
- Custodio del Activo de Información.
- Propietario del Riesgo.
- Intendentes, Gerentes o Jefes de las UUOO.
- Colaboradores y personal bajo modalidades formativas de la SUNAT
- Terceros vinculados con la institución.

VI. RESPONSABILIDADES DEL SGSI

6.1. Superintendente Nacional

- Asegurar la disponibilidad de los recursos necesarios (humanos, de infraestructura, financieros y tecnológicos) para la implementación y operación del SGSI.
- Definir y aprobar la estructura del Comité de Gobierno y Transformación Digital y designar a sus miembros.
- Designar al Oficial de Seguridad y Confianza Digital de la institución.
- Presidir, o designar a su representante para presidir, el Comité de Gobierno y Transformación Digital, con la finalidad de dirigir el gobierno, la gestión y la operación del SGSI y respaldar los acuerdos que se tomen para la mejora continua.
- Designar al responsable del Equipo de Respuestas ante Incidentes de Seguridad Digital de la SUNAT.

6.2. Comité de Gobierno y Transformación Digital

- Gestionar, mantener y documentar el SGSI de la entidad, con apoyo del Oficial de Seguridad y Confianza Digital, vigilando el cumplimiento de la normatividad relacionada a seguridad de la información.
- Realizar las revisiones de los indicadores de desempeño del SGSI, que permitan la elaboración de informes anuales, asegurando que el SGSI alcance los resultados previstos.
- Efectuar la revisión del SGSI, asegurando una gestión eficaz y el cumplimiento de los requisitos del SGSI, promoviendo la mejora continua.
- Promover, comunicar y fomentar la gestión de la seguridad de la información, los requisitos de seguridad y la gestión de riesgos en los procesos y en la cultura organizacional.
- Gestionar la asignación de personal y recursos necesarios para la implementación y operación del SGSI.
- Revisar y aprobar la documentación relativa al SGSI según los niveles de revisión y aprobación definidos en el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01).
- Revisar y aprobar el programa anual de auditorías y la propuesta de programación de capacitación para el personal sobre el SGSI, propuesto por el Oficial de Seguridad y Confianza Digital.
- Otras responsabilidades que le asigne el Superintendente Nacional, o a quien delegue, en el ámbito de su competencia y aquellas concordantes con la seguridad de la información.

6.3. Oficial de Seguridad y Confianza Digital

- Promover y coordinar la ejecución de todas las actividades relacionadas con el proceso de implementación y operación del SGSI.
- Gestionar el control de documentos, como: versiones, almacenamiento, retención, conservación, recuperación, acceso, distribución, vigencia y disposición. Asimismo, gestiona los documentos externos.

- Elaborar, implementar y monitorear los indicadores de desempeño del SGSI.
- Elaborar, revisar y aprobar la documentación relativa al SGSI según los niveles de elaboración, revisión y aprobación definidos en el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01).
- Liderar y desarrollar los talleres de análisis, evaluación y tratamiento de riesgos de seguridad de la información como parte del Equipo de Gestión de Riesgos.
- Gestionar el programa de concientización y sensibilización en Seguridad de la Información.
- Gestionar el tratamiento de los incidentes de seguridad de la información tomando en cuenta lo definido en el Procedimiento para el Registro y Atención de Incidentes y Vulnerabilidades de Seguridad de la Información vigente.
- Promover y coordinar la ejecución de las actividades relacionadas con la implementación del SGSI.
- Coordinar la revisión del SGSI por el Comité de Gobierno y Transformación Digital, generando la información de entrada para la revisión, apoyando en el análisis de la información, registrando los resultados y realizando el seguimiento de los acuerdos generados relacionados con el SGSI.
- Reportar y comunicar al Comité de Gobierno y Transformación Digital, según corresponda, sobre temas relacionados a:
 - Los indicadores de desempeño del SGSI.
 - Los avances de la implementación del SGSI y sus controles.
 - El incumplimiento de las directivas y procedimientos de seguridad de la información.
 - La gestión del tratamiento de los incidentes de seguridad de la información.
- Colaborar y orientar a los Propietarios del Activo de Información, Custodios del Activo de Información, Propietarios del Riesgo, Intendentes, Gerentes o Jefes de las UUOO para el cumplimiento de sus responsabilidades relacionadas al SGSI.

6.4. Equipo de Respuestas ante Incidentes de Seguridad Digital de la SUNAT

- Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital, de acuerdo con lo definido en los procedimientos vigentes.
- Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital, en el marco de los procedimientos vigentes.

6.5. Equipo de Gestión de Riesgos

- Conocer la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01) y llevar a cabo del proceso de gestión de riesgos en base a dicha metodología.
- Participar activamente de los talleres de gestión de riesgos de seguridad de la información y en las fases definidas en la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01).

- Proponer controles a ser evaluados dentro del marco del plan de tratamiento de riesgos.
- Identificar oportunidades relacionadas a la seguridad de la información.
- Revisar los riesgos residuales, así como los criterios de evaluación y aceptación de riesgos, en coordinación con el Propietario del Riesgo.

6.6. Propietario del Activo de Información

- Asegurar y mantener la confidencialidad, integridad y disponibilidad de los activos de información bajo su control.
- Realizar, en coordinación con el Oficial de Seguridad y Confianza Digital, la clasificación de los activos de información, de acuerdo con los estándares establecidos en la entidad, así como etiquetar dichos activos, con el objetivo de asegurar el adecuado tratamiento de sus riesgos y establecer un nivel de protección adecuado.
- Apoyar activamente en las actividades de análisis, evaluación y tratamiento de los riesgos de seguridad de la información, así como en la elaboración del inventario de activos.

6.7. Custodio del Activo de Información

- Velar por la protección de los activos de información bajo su custodia y/o responsabilidad en coordinación con el Propietario del Activo de Información.
- Apoyar la implementación de los controles propuestos para la protección de los activos de información asignados para su custodia, según los planes de tratamiento de riesgos de seguridad de la información.
- Participar en las actividades de análisis, evaluación y tratamiento de riesgos de seguridad de la información.

6.8. Propietario del Riesgo

- Participar y/o delegar al personal que participará en las actividades de análisis, evaluación y tratamiento de los riesgos de seguridad de la información de la entidad.
- Revisar y aprobar la Matriz de Riesgos de Seguridad y el Plan de Tratamiento de Riesgos de Seguridad de la Información, asegurando la eficacia de los controles a implementar.
- Evaluar y aceptar el riesgo residual de seguridad de los activos de información, y revisarlos periódicamente; así como los criterios de evaluación y aceptación de riesgos.
- Contribuir a la implementación de los controles de seguridad de la información que mitiguen los riesgos bajo su responsabilidad, reportando su avance cuando sea requerido.
- Gestionar los recursos necesarios para la implementación de los controles de seguridad de la información.
- Brindar información oportuna y pertinente; y disponer recursos para la elaboración de indicadores y métricas, así como en la ejecución de auditorías, revisiones y mejoras al SGSI, cuando sea requerido.

6.9. Intendentes, Gerentes o Jefes de las UUOO

- Reforzar la difusión, de manera adecuada, de la Política de Seguridad de la Información, asegurando su correcto entendimiento en el personal a su cargo.
- Promover el cumplimiento de la Política de Seguridad de la Información, los procedimientos y toda normativa, control o disposición establecida en la entidad, sobre seguridad de la información, como parte del SGSI.
- Promover la participación del personal a su cargo en las actividades de concientización y sensibilización en seguridad de la información.
- Autorizar el acceso a las instalaciones, a documentos e información relevantes, y la disposición del personal a su cargo, para la ejecución de las actividades de medición de indicadores, auditorías, revisiones o investigación y solución de incidentes y vulnerabilidades de seguridad de la información.
- Gestionar los accesos otorgados al personal a su cargo, según los lineamientos establecidos en la institución.
- Aprobar planes de acción para la atención de no conformidades, observaciones u oportunidades de mejora, producto de auditorías, revisiones por la Dirección (CGTD) u otros.
- Gestionar las acciones correctivas, correcciones o mejoras bajo su responsabilidad, y reportarlo cuando sea requerido.
- Desempeñar los roles de propietario del activo de información, propietario del riesgo y/o custodio del activo de información, según el activo de información bajo su control, pudiendo designar a los colaboradores a su cargo como respaldo para garantizar la continuidad en la gestión de dichos roles.

6.10. Colaboradores de la SUNAT y personal bajo modalidades formativas

- Conocer y cumplir las políticas, procedimientos y toda normativa, control o disposición establecida en la entidad, sobre seguridad de la información, como parte del SGSI.
- Utilizar la información y sus activos únicamente para los propósitos autorizados por la SUNAT.
- Reportar inmediatamente, a través de los canales de comunicación establecidos en la entidad, cualquier evento que identifique o del que sospeche que comprometa o pueda comprometer las operaciones y afectar la seguridad de la información de la SUNAT.
- Proporcionar toda la información requerida y disponer de su tiempo para atender las consultas o reuniones solicitadas con la finalidad de resolver el incidente o vulnerabilidad reportada.
- Participar en las charlas de concientización y sensibilización en seguridad de la información promovidas por el personal a cargo del SGSI y la INRH.
- Reportar no conformidades u observaciones que sean identificadas durante el desempeño de sus labores diarias.
- Proponer mejoras para el SGSI dentro del ámbito de su competencia.

6.11. Terceros vinculados con la institución

- Conocer y cumplir las políticas, procedimientos y toda normativa, control o disposición establecida en la entidad, sobre seguridad de la información, como parte del SGSI.
- Utilizar la información y sus activos provistos como parte de los servicios brindados, únicamente para los propósitos autorizados por la SUNAT.
- Cumplir con lo estipulado en las cláusulas incluidas en contratos u órdenes de servicio, que están referidas a salvaguardar la confidencialidad, integridad y disponibilidad de la información de la entidad.
- Brindar las facilidades necesarias para que la SUNAT verifique el cumplimiento de las condiciones y aspectos de seguridad de la información incluidos en contratos u órdenes de los servicios brindados.