



Procedimiento de Auditoría Interna Versión 2

Código:
SGSI-PR-03

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.	04/02/2019	1	Oficial de Seguridad de la Información
2	- 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 actualizó la distribución de los numerales del documento. - En el numeral I se ha incluido la revisión independiente al SGSI. - En el numeral IV se ha incluido la definición de alcance de auditoría, auditor, auditor líder, conformidad, herramienta SGSI (HSGSI), observación y oportunidad de mejora. Se retiró la definición de usuarios del documento. - El numeral V ha sido modificado incluyendo la realización de revisiones independientes al SGSI. - Se han agregado los formatos Plan de Auditoría (SGSI-PR-03.FO-02), Informe de Auditoría Interna (SGSI-PR-03.FO-03) e Informe de Revisión Independiente (SGSI-PR-03.FO-04). - En el numeral VII se incluyó el anexo N.º 2.	13/01/2026	2	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	5
V. DESCRIPCIÓN	6
5.1. Planificación de Auditoría.....	6
5.2. Ejecución de la Auditoría.....	7
5.3. Cierre de Auditoría	7
VI. REGISTROS.....	7
VII. ANEXOS.....	8

SIGLAS

- **CGTD:** Comité de Gobierno y Transformación Digital.
- **DN:** Dirección de Normalización del INACAL.
- **HSGSI:** Herramienta del Sistema de Gestión de Seguridad de la Información.
- **IEC:** Comisión Electrotécnica Internacional (International Electrotechnical Commission, en inglés).
- **INACAL:** Instituto Nacional de Calidad.
- **ISO:** Organización Internacional de Normalización (International Organization for Standardization, en inglés).
- **OSCD:** Oficial de Seguridad y Confianza Digital.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SUNAT:** Superintendencia Nacional de Aduanas y de Administración Tributaria.

I. OBJETIVO

Establecer las pautas para la planificación, ejecución y cierre de las auditorías internas y revisiones independientes al SGSI.

II. ALCANCE

Este procedimiento aplica a los procesos involucrados dentro del alcance del 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.

IV. GLOSARIO DE TÉRMINOS

- 4.1. Acción Correctiva:** Acción para eliminar la causa de una no conformidad y prevenir que vuelva a ocurrir.

- 4.2. **Alcance de Auditoría:** Extensión y límites de una auditoría.
- 4.3. **Auditor:** Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.
- 4.4. **Auditor Líder:** Auditor responsable de asegurar la conducción y realización eficiente y efectiva de la auditoría, dentro del alcance y del plan de auditoría acordado.
- 4.5. **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.
- 4.6. **Conclusiones de Auditoría:** Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.
- 4.7. **Conformidad:** Cumplimiento de un requisito.
- 4.8. **Corrección:** Acción para eliminar una no conformidad detectada.
- 4.9. **Hallazgos de Auditoría:** Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.
- 4.10. **Herramienta SGSI (HSGSI):** Herramienta para la gestión del SGSI.
- 4.11. **No Conformidad:** Incumplimiento de un requisito.
- 4.12. **Observación:** Es una falla aislada o esporádica en el contenido o implementación de los documentos del SGSI, que no llega a afectar de manera crítica al SGSI.
- 4.13. **Oportunidad de Mejora:** Acción recomendada que al ser implementada implica una mejora en el SGSI.
- 4.14. **Revisión Independiente:** Es la revisión realizada por personas independientes del área bajo revisión y que no forman parte de una línea de autoridad, con la finalidad de asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos del SGSI.

V. DESCRIPCIÓN

5.1. Planificación de Auditoría

- a) El OSCD elabora el Programa de Auditoría Interna del SGSI (SGSI-PR-03.FO-01).
- b) El OSCD selecciona al (a los) Auditor(es) teniendo en cuenta las responsabilidades y competencias especificadas en el anexo N.º 1.

- c) El OSCD solicita al Auditor Líder, el Plan de Auditoría Interna (SGSI-PR-03.FO-02).
- d) El OSCD valida con las áreas auditadas las fechas y horarios.
- e) EL OSCD aprueba el Plan de Auditoría Interna (SGSI-PR-03.FO-02) y comunica a los involucrados en la auditoría.

5.2. Ejecución de la Auditoría

- a) El Auditor Líder inicia la reunión de apertura.
- b) El (los) Auditor(es) ejecuta(n) la auditoría interna según lo establecido en el Plan de Auditoría Interna (SGSI-PR-03.FO-02).
- c) El (los) Auditor(es) revisa(n) la documentación de los procesos a auditar teniendo en cuenta los resultados de las auditorías anteriores y revisando la conformidad del SGSI.
- d) El Auditor Líder consolida la información de los hallazgos de auditoría (No Conformidad, Observación u Oportunidades de Mejora) para la elaboración del Informe de Auditoría Interna (SGSI-PR-03.FO-03). Los hallazgos de la revisión independiente se consolidan en el Informe de Revisión Independiente SGSI (SGSI-PR-03.FO-04).
- e) El Auditor Líder presenta los resultados de los hallazgos en la reunión de cierre y entrega el informe al OSCD.

5.3. Cierre de Auditoría

- a) El OSCD informa los resultados a las gerencias pertinentes.
- b) El OSCD gestiona los hallazgos según lo definido en el Procedimiento de Acciones Correctivas del SGSI (SGSI-PR-04) y el Procedimiento de Mejora Continua del SGSI (SGSI-PR-05), determinando las acciones que correspondan.

La Información de la auditoría y de la revisión independiente se encuentra disponible en la herramienta SGSI (HSGSI).

VI. REGISTROS

Código	Nombre del registro	Responsable
SGSI-PR-03.FO-01	Programa de Auditoría Interna	OSCD
SGSI-PR-03.FO-02	Plan de Auditoría Interna	OSCD
SGSI-PR-03.FO-03	Informe de Auditoría Interna	OSCD

SGSI-PR-03.FO-04	Informe de Revisión Independiente SGSI	OSCD
------------------	---	------

VII. ANEXOS

Anexo N.º 1 – Responsabilidades y competencias para auditar.

Anexo N.º 2 – HSGSI - Auditorías.

ANEXO N.º 1 – RESPONSABILIDADES Y COMPETENCIAS PARA AUDITAR**Auditor Líder:****Responsabilidades:**

- Preparar el Plan de Auditoría Interna en coordinación con el OSCD.
- Liderar las reuniones de apertura y de cierre de la auditoría interna.
- Ejecutar la auditoría interna de acuerdo con lo definido en el Plan de Auditoría Interna.
- Presentar los hallazgos de la auditoría.
- Entregar al OSCD el informe de Auditoría Interna.

Competencias

- Profesional titulado o bachiller en ingeniería informática, de sistemas y carreras afines.
- Conocer la Norma ISO/IEC 27001 vigente, Seguridad de la información y afines.
- Estar familiarizado con técnicas de auditoría.
- Contar con certificación vigente de Auditor Líder en ISO/IEC 27001.
- Contar con número de registro de certificado habilitado y válido de Auditor Líder.
- Haber participado en dos (2) auditorías como auditor SGSI y en una (1) auditoría como auditor líder SGSI.

Auditor:**Responsabilidades:**

- Apoyar al Auditor Líder en las actividades de la auditoría.
- Participar en las reuniones que designe el Auditor Líder.

Competencias

- Profesional titulado o bachiller en ingeniería informática, de sistemas y carreras afines.
- Conocer la Norma ISO/IEC 27001 vigente.
- Estar familiarizado con técnicas de auditoría.
- Haber aprobado un curso de formación de auditores internos en ISO/IEC 27001 en la versión vigente.
- Haber participado en dos (2) auditorías como auditor bajo supervisión de un auditor líder.

Auditor Líder Técnico (Revisión independiente):**Responsabilidades:**

- Preparar el plan de trabajo de revisión independiente en coordinación con el OSCD.
- Liderar las reuniones de apertura y de cierre.

- Ejecutar la revisión independiente de acuerdo con lo definido en el Plan.
- Presentar los hallazgos de revisión independiente.
- Entregar al OSCD el informe de revisión independiente de la seguridad de la información.

Competencias

- Profesional titulado o bachiller en ingeniería informática, de sistemas y carreras afines.
- Contar con certificación vigente de Auditor Líder en ISO/IEC 27001.
- Contar con número de registro de certificado habilitado y válido de Auditor Líder.
- Haber implementado al menos un (1) SGSI completo.
- Haber realizado cursos en Seguridad Informática y/o Ciberseguridad y/o Continuidad de Negocio y/o Gestión de Riesgos bajo ISO 27005 o ISO 31000 y/o NIST y/o Centro de Datos.
- Haber participado en dos (2) auditorías como auditor SGSI y en una (1) auditoría como auditor líder SGSI.

ANEXO N.º 2 – HSGSI - Auditorías

GlobalSuite

SUNAT

fbernardo | ADMINISTRADOR PLATAFORMA | Salir

HomeInicioAnálisisPlanesGestiónScoreCardAdministración

Auditorías - Planificación: Programa de Auditoría Interna 2023SUNAT |

←

Opciones

Continuidad

Disponibilidad

Capacidad

Formación y Capacitación

Auditorías

Programa de Pruebas

Secciones

Actas de Reunión

Gestor Documental

Sin tareas pendientes

Alertas

Informes

Sin descargas pendientes

Proyectos

Equipo de Trabajo

Gestión del Proyecto

Calendario

Ver Históricos Proyecto

PlanificaciónInforme de auditoría

GuardarVolverCopiar Alcance

Información Preliminar

CódigoSGSI-PR-03.FO-01-2023

NombrePrograma de Auditoría Interna 2023

SGSG

+ Añadir

- Eliminar

ISO 27001

SG

EstadoPlanificada

Descripción

Servicios

Servicios

Procesos

+ Añadir Servicio

+ Añadir Proceso

- Eliminar

Ver Dependencias

Servicios/Procesos

Intercambio de información

Versión1

Fecha prevista de01/04/2024 11:32:34