



PERÚ

Ministerio de Cultura

ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI

[SGSI-DOC-003]



Firmado digitalmente por
PALACIOS RAMIREZ Joan Miguel
FAU 20537630222 soft
Motivo: Doy V° B°
Fecha: 01.04.2026 15:50:02 -05:00

Elaborado por:	Revisado por:	Aprobado por:
Oficial de Seguridad y Confianza Digital  Firmado digitalmente por LOPEZ VIDAL Roxana Jovita FAU 20537630222 soft Motivo: Soy el autor del documento Fecha: 01.04.2026 14:14:26 -05:00	Comité de Gobierno y Transformación Digital	Titular del pliego

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.03

HOJA DE CONTROL DE CAMBIOS

Versión	Justificación	Texto modificado	Aprobador
01	Versión Inicial	-	Titular del pliego
02	Revisión Anual	Comité de Gobierno Digital Cambio en modalidades de trabajo por contexto de emergencia sanitaria	Titular del Pliego
03	Actualización 10.02.2026	Incorporación de los roles asociados a los términos de Ciberseguridad y Protección de la Privacidad de acuerdo con la norma NTP ISO/IEC 27001:2022	Titular del Pliego

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.03

Contenido

1. OBJETIVO.....	4
2. ALCANCE	4
3. ESTRUCTURA ORGANIZACIONAL	4
4. ROLES Y RESPONSABILIDADES	4
4.1. Comité de Gobierno y Transformación Digital	4
4.2. Equipo de Respuestas ante Incidentes de Seguridad Digital – CSIRT	5
4.3. Oficial de Seguridad y Confianza Digital	5
4.4. Oficial de Datos Personales	6
4.5. Propietarios de la Información	6
4.6. Custodios de la Información	7
4.7. Usuarios	7
4.8. Auditor	8
4.9. Auditado	8

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.03

1. **OBJETIVO**

Definir la estructura organizacional para la gestión y operación del Sistema de Gestión de Seguridad de la Información – SGSI, en el Ministerio de Cultura mediante una adecuada distribución de roles y responsabilidades.

2. **ALCANCE**

El presente documento involucra a todo el personal que forma parte del alcance del Sistema de Gestión de Seguridad de la Información – SGSI.

3. **ESTRUCTURA ORGANIZACIONAL**

En el marco de la gestión de la seguridad de la información, la Alta Dirección define los siguientes roles y las responsabilidades entre los diferentes niveles directivos y operativos de la organización:

- Comité de Gobierno y Transformación Digital.
- Equipo de Respuestas ante Incidentes de Seguridad Digital - CSIRT
- Oficial de Seguridad y Confianza Digital.
- Oficial de Datos Personales
- Propietarios de la Información.
- Custodios de la Información.
- Usuarios.
- Auditor.
- Auditado.

4. **ROLES Y RESPONSABILIDADES**

4.1. **Comité de Gobierno y Transformación Digital**

Con Resolución Ministerial N° 087-2019-PCM, en los numerales d), e), f), g) e i) del artículo 2 “De las funciones del Comité de Gobierno Digital”, establecen las siguientes funciones relacionadas al SGSI:

- a) Gestionar la asignación de personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en sus Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.
- b) Promover y gestionar la implementación de estándares y buenas prácticas en seguridad digital en la entidad.
- c) Elaborar informes anuales que midan el progreso de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
- d) Vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información.
- e) Gestionar, mantener y documentar el Sistema de Gestión de la Seguridad de la Información (SGSI) de la entidad.

Asimismo, considerando la Norma Técnica Peruana “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. 3ª. Edición”, se han añadido las siguientes responsabilidades:

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.03

- f) Establecer la política y objetivos de seguridad de la información alineados con la dirección estratégica del Ministerio, entre ellos, el Plan Estratégico Institucional; así como las políticas del sector y la regulación en el ámbito de seguridad de la información.
- g) Promover la gestión de seguridad de la información en los procesos y cultura organizacional.
- h) Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, de conformidad con los requisitos del SGSI.
- i) Asegurar que se logre los resultados previstos del SGSI, con un enfoque de mejora continua del referido sistema.
- j) Dirigir y apoyar a las personas y a los otros roles relevantes para que contribuyan con la efectividad del SGSI.

4.2. Equipo de Respuestas ante Incidentes de Seguridad Digital – CSIRT

Mediante la Resolución Ministerial N° 159-2025-MC, se conforma el Equipo de Respuestas ante Incidentes de Seguridad Digital del Ministerio de Cultura (CSIRT-MC), integrado en su totalidad por servidores de la Oficina General de Estadística y Tecnologías de la Información y Comunicación – OGETIC del Ministerio de Cultura y es de naturaleza permanente, el cual tiene las siguientes funciones:

- a) Comunicar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
- b) Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad.
- c) Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en su entidad.
- d) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.
- e) Proveer los recursos y medidas necesarias para asegurar la efectiva gestión de incidentes de seguridad digital.
- f) Requerir a los proveedores de desarrollo de software el cumplimiento de estándares, normas técnicas y mejores prácticas de seguridad ampliamente reconocidos.
- g) Coordinar y colaborar a través del Centro Nacional de Seguridad Digital con otros Equipos de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital en el ámbito de las redes de confianza.
- h) Otras que determine la alta dirección de la institución.

4.3. Oficial de Seguridad y Confianza Digital

Coordinador/a del mantenimiento y mejora continua del SGSI en el Ministerio de Cultura. Tiene como responsabilidades:

- a) Participar en la creación y revisión de las políticas, lineamientos, metodologías, procedimientos y planes referidos al SGSI.
- b) Evaluar, coordinar y monitorear el cumplimiento de las políticas, procedimientos y controles del SGSI.
- c) Coordinar con los propietarios y custodios de la información para la elaboración del inventario de activos de la información y ejecución de la gestión de riesgos.
- d) Informar los resultados de la gestión del SGSI al Comité de Gobierno y

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.03

Transformación Digital.

- e) Dar seguimiento a los incidentes de seguridad de la información y ciberseguridad.
- f) Promover la difusión de los temas de seguridad de la información y ciberseguridad.
- g) Supervisar la ejecución de las actividades que se deriven de los informes de las auditorías al SGSI.

4.4. Oficial de Datos Personales

Es la persona designada por el responsable de tratamiento o encargado del tratamiento de datos personales para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales, y de acuerdo con el artículo 39, del Reglamento de La Ley N° 29733, Ley De Protección de Datos Personales aprobado con Decreto Supremo N° 016-2024-JUS, tiene como mínimo las siguientes funciones:

- a) Informar y asesorar al titular del banco de datos personales o al responsable del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales respecto de las obligaciones que les incumben en virtud de la Ley, el presente Reglamento y de otras disposiciones de protección de datos.
- b) Verificar e informar sobre el cumplimiento de lo dispuesto en la Ley, el presente Reglamento y de otras disposiciones de protección de datos personales, así como del cumplimiento de las políticas del titular del banco de datos o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la sensibilización y formación del personal que participa en las operaciones de tratamiento, y las auditorías que se realicen.
- c) Cooperar, en lo que resulte pertinente, con la Autoridad Nacional de Protección de Datos Personales para el desempeño de sus fines y atribuciones.
- d) Actuar como punto de contacto de la Autoridad Nacional de Protección de Datos Personales para cuestiones relativas al tratamiento de datos personales.

4.5. Propietarios de la Información

Son los/as responsables de la información que se genera y se utiliza en las operaciones de su Unidad Orgánica. Tienen como responsabilidades:

- a) Participar en la identificación de los activos de información y en su clasificación de acuerdo a su grado de confidencialidad, integridad y disponibilidad; documentándolos y manteniendo su clasificación y etiquetado debidamente actualizado.
- b) Participar en la gestión de riesgos de los activos de información, analizando, evaluando y realizando su respectivo tratamiento de riesgos de manera coordinada con el/la Oficial de Seguridad y Confianza Digital.
- c) Definir los usuarios que deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias, revisando periódicamente los niveles de acceso a los sistemas de información a su cargo.
- d) Sugerir y apoyar en la elaboración de lineamientos y procedimientos del SGSI dentro de sus respectivas áreas y procesos.
- e) Supervisar y verificar la aplicación de los controles de seguridad con el custodio de la información.

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.03

4.6. Custodios de la Información

Son los/as encargados/as de la administración diaria de la seguridad de los activos de información y el monitoreo del cumplimiento de las políticas y los controles de seguridad en los activos de información que se encuentren bajo su administración, y tienen como responsabilidades:

- Administrar los controles relevantes al SGSI, acorde a las medidas de tratamiento de la información especificadas por los propietarios de la información (restricción de accesos, validación de autenticidad, mecanismos de resguardo, entre otros).
- Cumplir con los controles implementados para la protección de los activos de información asignados para su custodia.
- Colaborar en la investigación de los incidentes de seguridad de la información ciberseguridad y protección de la privacidad.
- Identificar oportunidades de mejora y comunicarlas a el/la Oficial de Seguridad y Confianza Digital.
- Respalidar, verificar y recuperar la información de los respaldos, manteniendo el registro del resguardo debidamente estructurado que permita tener la disponibilidad de los respaldos de acuerdo a su clasificación.
- Proteger y resguardar los activos de información físicos de accesos indebidos o no autorizados.

4.7. Usuarios

Es el personal del Ministerio de Cultura indistintamente del régimen laboral, modalidad de contratación o nivel jerárquico, las personas naturales o jurídicas que prestan servicios en el Ministerio, así como las personas y entidades públicas o privadas que utilizan la información del Ministerio. Tienen como responsabilidades:

- Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información, ciberseguridad y protección de la privacidad.
- Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
- Utilizar la información del Ministerio de Cultura únicamente para los propósitos autorizados.
- Participar en los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información, ciberseguridad y protección de la privacidad.
- Reportar cualquier incidente, potencial incidente u oportunidades de mejora del SGSI del Ministerio.
- No divulgar o utilizar información contenida en los sistemas, plataformas, aplicativos y otros recursos informáticos que se hayan facilitado en un entorno de trabajo remoto, presencial o mixto, para propósitos ajenos a sus funciones; realizando una adecuada utilización y manteniendo la debida confidencialidad y protección de datos.
- Hacer uso de los sistemas, plataformas, aplicativos y otros recursos informáticos del Ministerio desde un equipo con antivirus actualizado.

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.03

4.8. Auditor

Es el/la responsable de liderar y/o preparar y/o llevar a cabo el proceso de auditoría interna o auditoría externa de certificación, para determinar el grado en el cual el SGSI cumple con los requisitos de la Norma NTP ISO/IEC 27001:2022. Puede liderar un grupo de auditores y tiene como responsabilidades:

- a) Convocar y realizar la reunión de apertura y cierre de auditoría de acuerdo con el plan de auditoría.
- b) Planificar y dirigir todas las actividades de la auditoría.
- c) Revisar la documentación y evidencias de cumplimiento dentro del alcance del SGSI.
- d) Llevar a cabo las reuniones de relevamiento de información con el personal involucrado en el alcance, para corroborar o extender sus indagaciones.
- e) Mantener imparcialidad, objetividad y ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo (de ser una auditoría interna).
- f) Otras funciones en el ámbito de su competencia.

4.9. Auditado

Es el personal del Ministerio de Cultura indistintamente del régimen laboral, modalidad de contratación o nivel jerárquico, las personas naturales o jurídicas que prestan servicios en el Ministerio, así como las personas y entidades públicas o privadas que utilizan la información del Ministerio; que se encuentran sujetas a una revisión por parte del auditor o equipo de auditores. Tienen como responsabilidad proporcionar al auditor o equipo auditores la información necesaria y objetiva para asegurar un proceso de auditoría eficiente y eficaz.