



Resolución Ministerial

N° 228-2018-MC

Lima, 12 JUN. 2018

VISTOS; los Memorandos N° SS025-2018-OGETIC/SG/MC y N° 900032-2018/OGETIC/SG/MC de la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones; los Memorandos N° SS041-2018-OGPP/SG/MC y N° 900118-2018/OGPP/SG/MC de la Oficina General de Planeamiento y Presupuesto; el Acta de Reunión de fecha 2 de febrero de 2018, del Comité de Gestión de Seguridad de la Información del Ministerio de Cultura; y,

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 004-2016-PCM de fecha 8 de enero de 2016, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar la seguridad de la información como un componente crucial para dicho objetivo;

Que, a través de la Resolución Ministerial N° 085-2016-MC de fecha 26 de febrero de 2016, se constituye el Comité de Gestión de Seguridad de la Información del Ministerio de Cultura; el mismo que con Acta de Reunión de fecha 2 de febrero de 2018, acordó elevar a la Alta Dirección para su aprobación, la propuesta de "Política y objetivos de Seguridad de la Información" y de los "Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información – SGSI", presentada por la coordinadora del Ministerio de Cultura que hace las veces de Oficial de Seguridad de la Información, designada por Resolución Ministerial N° 509-2017-MC;

Que, el numeral 5.2 de la precitada Norma Técnica Peruana dispone que la Alta Dirección debe establecer una política de seguridad de la información que sea apropiada al propósito de la organización, la cual incluya objetivos de seguridad de la información o proporcione el marco de referencia para fijar los mismos, así como los compromisos de satisfacer requisitos aplicables relacionados a la seguridad de la información, y de mejora continua del sistema de gestión de seguridad de la información; así como, que la precitada política debe estar disponible como información documentada, comunicada dentro de la organización y disponible a las partes interesadas, según sea apropiado;

Que, adicionalmente, en su numeral 5.3, señala que la Alta Dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas, debiendo establecer la responsabilidad y la autoridad para garantizar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de la Norma Técnica Peruana antes citada, y reportar sobre el desempeño del sistema de gestión de seguridad de la información a la Alta Dirección;



Que, a través de los Informes N° 000011-2018-SVH/OGETIC/SG/MC y N° SS0001-2018-SVH/OGETIC/SG/MC, de fechas 28 de febrero y 19 de marzo de 2018, respectivamente; la coordinadora del Ministerio de Cultura que hace las veces de Oficial de Seguridad de la Información, propone la reformulación de los documentos denominados “Política de Seguridad de la Información” y “Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información – SGSI”, que fueron aprobados el 01 de junio de 2016 por el Comité de Gestión de Seguridad de la Información;

Que, mediante el Memorando N° SS025-2018-OGETIC/SG/MC de fecha 21 de marzo de 2018, la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones remite a la Oficina General de Planeamiento y Presupuesto los precitados documentos, para la emisión de opinión técnica; y, con el Memorando N° 900032-2018/OGETIC/SG/MC de fecha 16 de mayo de 2018, brinda conformidad a los proyectos reformulados de “Política de Seguridad de la Información” y “Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información – SGSI”;

Que, con el Memorando N° SS041-2018-OGPP/SG/MC de fecha 27 de marzo de 2018, la Oficina General de Planeamiento y Presupuesto remite el Informe N° SS009-2018-OPL/OGPP/SG/MC de la Oficina de Planeamiento a su cargo, expresando su conformidad con los documentos antes mencionados; asimismo, a través del Memorando N° 900118-2018/OGPP/SG/MC de fecha 30 de mayo de 2018, ratifica la opinión brindada mediante el precitado Informe, donde se da cuenta que dichos proyectos cumplen con lo requerido en la NTP ISO/IEC 27001:2014; motivo por el cual, resulta necesario proceder a su aprobación;

De conformidad con lo dispuesto en la Ley N° 29565, Ley de creación del Ministerio de Cultura; y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo N° 005-2013-MC;

SE RESUELVE:

Artículo Único.- Aprobar los documentos denominados “Política y objetivos de Seguridad de la Información” y “Roles y responsabilidades del Sistema de Gestión de Seguridad de la Información – SGSI” del Ministerio de Cultura, los mismos que en anexo forman parte integrante de la presente resolución.

Regístrese y comuníquese.



PATRICIA BALBUENA PALACIOS
MINISTRA DE CULTURA





PERÚ

Ministerio de Cultura

POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

[SGSI-POLI-001]

Elaborado por: Oficial de Seguridad de la Información	Revisado por: Comité de Gestión de Seguridad de la Información	Aprobado por: Titular del pliego
		
Fecha: 02/02/2018	Fecha: 01/03/2018	Fecha: 12/06/2018

PATRICIA BALBUENA PALACIOS
MINISTRA DE CULTURA

 PERÚ Ministerio de Cultura	POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: SGSI-POLI-001
	USO PÚBLICO	POLÍTICA VERSIÓN: V.01

HOJA DE CONTROL DE CAMBIOS

Versión	Justificación	Texto modificado	Aprobador
01	Versión inicial	-	Titular del pliego



 PERÚ Ministerio de Cultura	POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: SGSI-POLI-001
	USO PÚBLICO	POLÍTICA VERSIÓN: V.01

1. DECLARACIÓN

El Ministerio de Cultura es un organismo del Poder Ejecutivo con personería jurídica de derecho público que constituye pliego presupuestal del Estado, ejerciendo competencias y funciones sobre las áreas programáticas de acción referidas al patrimonio cultural de la nación, material e inmaterial; la creación cultural contemporánea y artes vivas; la gestión cultural e industrias culturales; y, la pluralidad étnica y cultural de la nación. Reconoce a la información como un activo de vital importancia para el cumplimiento de la misión y objetivos estratégicos institucionales, por lo que se compromete a:

- Establecer los mecanismos necesarios para preservar la integridad, confidencialidad y disponibilidad de la información en concordancia con los requerimientos regulatorios, legales y contractuales vigentes.
- Identificar y tratar los riesgos de seguridad de la información que son relevantes para la Institución, mediante una adecuada gestión de riesgos.
- Dar respuesta efectiva y tomar acciones correctivas ante incidentes relacionados con la seguridad de la información.
- Asegurar el aprovisionamiento de los recursos requeridos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
- Fortalecer la toma de conciencia y promover una cultura en seguridad de la información en todo el personal.
- Establecer medidas de continuidad en torno a los activos de información del Ministerio de Cultura.
- Mejorar continuamente el Sistema de Gestión de Seguridad de la Información.

2. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

La presente política tiene como objetivo establecer el marco general de gestión para proteger adecuadamente la información del Ministerio de Cultura, definiendo los lineamientos generales que aseguren el tratamiento adecuado de los riesgos que conduzcan al fortalecimiento de una cultura en seguridad de la información.

Para la gestión de la seguridad de la información, se han establecido los siguientes objetivos:

- Asegurar la disponibilidad de la información y la continuidad de los servicios tecnológicos.
- Establecer medidas de seguridad de la información para proteger los activos de información contra las amenazas que afecten la confidencialidad, integridad y disponibilidad de la información.
- Generar conciencia de la necesidad de seguridad de la información en todo el personal del Ministerio de Cultura.

 PERÚ Ministerio de Cultura	POLÍTICA Y OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: SGSI-POLI-001
	USO PÚBLICO	POLÍTICA VERSIÓN: V.01

3. ALCANCE

La presente política es de cumplimiento obligatorio para todo el personal del Ministerio de Cultura, indistintamente de su régimen laboral, modalidad de contratación o nivel jerárquico; así como por las personas naturales o jurídicas que prestan servicios o tengan acceso a la información del Ministerio.

4. SANCIONES

El personal o personas que incumplan las disposiciones contenidas en la presente Política, incurrirán en falta disciplinaria que se sancionará de acuerdo a lo dispuesto en la Ley N° 27815, Ley del Código de Ética de la Función Pública y lo establecido en el Reglamento General de la Ley N° 30057, Ley del Servicio Civil, aprobado mediante Decreto Supremo N° 040-2014-PCM.

5. REVISIONES

La presente política se revisará por lo menos una vez al año, cuando ocurran cambios significativos que afecten al Sistema de Gestión de Seguridad de la Información o cuando el Comité de Gestión de Seguridad de la Información lo vea pertinente para asegurar su conveniencia, adecuación y eficacia continua.

6. DIFUSIÓN

La comunicación de los documentos que componen la seguridad de la información se efectúa de manera que el contenido de la documentación sea accesible y comprensible para todo el personal comprendido en esta Política.





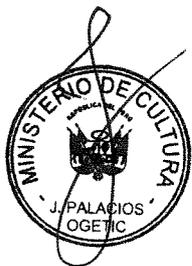
PERÚ

Ministerio de Cultura

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

[SGSI-DOC-003]

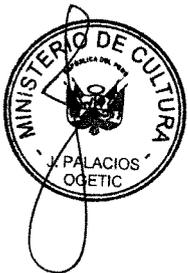
Elaborado por: Oficial de Seguridad de la Información	Revisado por: Comité de Gestión de Seguridad de la Información	Aprobado por: Titular del pliego
 Fecha: 02/02/2018	 Fecha: 01/03/2018	 PATRICIA BALBUENA PALACIOS MINISTRA DE CULTURA Fecha: 12/06/2018



 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.01

HOJA DE CONTROL DE CAMBIOS

Versión	Justificación	Texto modificado	Aprobador
001	Versión inicial	-	Titular del pliego



Contenido

1. OBJETIVO.-	4
2. ALCANCE	4
3. ESTRUCTURA ORGANIZACIONAL	4
4. ROLES Y RESPONSABILIDADES	4
4.1. Comité de Gestión de Seguridad de la Información	4
4.2. Oficial de Seguridad de la Información	4
4.3. Propietarios de la Información	5
4.4. Custodios de la Información	5
4.5. Usuarios	5
4.6. Auditor Líder	6
4.7. Auditor Interno	6
4.8. Auditado	6



	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.01

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 Gestión de Seguridad de la Información
- Oficial de Seguridad de la Información
- Propietarios de la Información
- Custodios de la Información
- Usuarios
- Auditor Líder
- Auditor Interno
- Auditado

4. ROLES Y RESPONSABILIDADES

4.1. Comité de Gestión de Seguridad de la Información

La Resolución Ministerial N° 166-2017-PCM, modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM, e incorpora el artículo 5-A “De las funciones del Comité de Gestión de Seguridad de la Información”, estableciendo lo siguiente:

- a) Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información.
- b) Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información.
- c) Promover la gestión de seguridad de la información en los procesos y cultura organizacional.
- d) Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información.
- e) Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información.
- f) Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información.
- g) Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

4.2. Oficial de Seguridad de la Información

Coordinador del plan de implementación del SGSI en el Ministerio de Cultura. Tiene como responsabilidades:

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.01

- a) Participar en la creación y revisión de las políticas, lineamientos, metodologías, procedimientos y planes referidos a la seguridad de la información.
- b) Supervisar el cumplimiento de las políticas, procedimientos y controles de seguridad de la información.
- 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 su gestión al Comité de Gestión de Seguridad de la Información.
- e) Dar seguimiento a los incidentes de seguridad de la información, evaluar riesgos y eventuales impactos.
- f) Evaluar, coordinar y monitorear la implementación de los controles relacionados al SGSI.
- g) Supervisar y apoyar en la difusión de los temas de seguridad de la información.
- h) Supervisar la ejecución de las actividades que se deriven de los informes de las auditorías en seguridad de la información.

4.3. Propietarios de la Información

Son los 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 las actividades de análisis, evaluación y tratamiento de riesgos.
- b) Revisión periódica de la clasificación y etiquetado de la información con el propósito de verificar que cumpla con los requerimientos de la Entidad.
- c) Sugerir y apoyar en la elaboración de lineamientos y procedimientos de seguridad de la información dentro de sus respectivas áreas y procesos.
- d) Revisar periódicamente los niveles de acceso a los sistemas de información a su cargo.
- e) Supervisar y verificar la aplicación de los controles de seguridad con el custodio de la información.

4.4. Custodios de la Información

Son los encargados 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 tiene como responsabilidades:

- a) Administrar los controles relevantes a la seguridad de la información, 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, otros).
- b) Cumplir con los controles implementados para la protección de los activos de información asignados para su custodia.
- c) Colaborar en la investigación de los incidentes de seguridad de la información.
- d) Identificar oportunidades de mejora y comunicarlas al Oficial de Seguridad de la Información.

4.5. Usuarios

Es el personal del Ministerio de Cultura indistintamente del régimen laboral, modalidad de contratación o nivel jerárquico; así como por las personas naturales o jurídicas que

 PERÚ Ministerio de Cultura	ROLES Y RESPONSABILIDADES DEL SGSI	CODIGO: SGSI-DOC-003
	USO PÚBLICO	DOCUMENTO VERSIÓN: V.01

prestan servicios, quienes utilizan la información en actividades habituales y se encuentran obligados a respetar las normas establecidas por la Institución. Tienen como responsabilidades:

- a) Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información.
- b) Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
- c) Utilizar la información del Ministerio de Cultura únicamente para los propósitos autorizados.
- d) Participar en los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
- e) Reportar cualquier incidente, potencial incidente u oportunidades de mejora de seguridad de la información.

4.6. Auditor Líder

Es el encargado de encabezar al equipo de auditores internos. Tiene como responsabilidades:

- a) Convocar y realizar la reunión de apertura de auditoría.
- b) Realizar la reunión de cierre de acuerdo al plan de auditoría.
- c) Planificar y dirigir todas las actividades de la auditoría.
- d) Ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.

4.7. Auditor Interno

Es el responsable de preparar y llevar a cabo el proceso de auditoría interna para determinar el grado en el cual el sistema de gestión de seguridad de la Información cumple con los requisitos de la Norma Técnica Peruana ISO/IEC 27001:2014. Tiene como responsabilidades:

- a) Revisar la documentación y evidencias de cumplimiento dentro del alcance del SGSI.
- b) Llevar a cabo las reuniones de relevamiento de información con el personal involucrado, para corroborar o extender sus indagaciones.
- c) Mantener imparcialidad, objetividad y ser independiente del área o proceso comprendido dentro del alcance de la auditoría, no auditar su propio trabajo.
- e) Otras funciones en el ámbito de su competencia

4.8. Auditado

El auditado es cualquier personal del Ministerio de Cultura que se encuentra sujeto a una revisión por parte del equipo de auditores. Tiene como responsabilidad proporcionar al equipo auditor la información necesaria y objetiva para asegurar un proceso de auditoría eficiente y eficaz.

