sunarp Superintendencia Nacional de los Registros Públicos	Tipo de documento: **MANUAL**	Código: **MN-001-2024-CGD-SN**	
	Aprobación: **RESOLUCIÓN Nº 00065-2024-SUNARP/GG**		
	Versión: **V.01**	Fecha de aprobación: **18/04/2024**	Páginas: **1/19**

MANUAL DE ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

I. DESCRIPCIÓN

1. Objetivo

[Referencia: ISO 27001[1] cláusula 5.3, A5.2]

Organizar la seguridad de la información en la Sunarp, describiendo claramente la estructura, los roles y sus responsabilidades para la realización de procesos específicos de seguridad de la información y del Sistema de Gestión de Seguridad de la Información (SGSI).

No define, ni regula, otros aspectos de seguridad de la información como el acceso o procesamiento de la información, el acceso o protección de los activos de la información, respuesta en casos de incidentes de seguridad de la información u otros aspectos que serán detallados en documentos complementarios.

2. Alcance

Este documento tiene como alcance todas las Unidades Orgánicas de la Sede Central y Zonas Registrales.

Asimismo, es de obligado cumplimiento para todo el personal que preste servicios en la Sunarp, de manera permanente y/o eventual bajo cualquier modalidad de contrato, incluyendo el personal de entidades externas.

3. Base Legal

a) **Decreto Supremo N° 029-2021-PCM** que aprueba el Reglamento del Decreto Legislativo N° 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, publicado el 19 de febrero de 2021.

b) **Decreto Legislativo Nº 1412** que aprueba la Ley de Gobierno Digital, publicada el 13 de setiembre del 2018.

c) **Resolución Ministerial Nº 119-2018-PCM** que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, publicada el 10 de mayo de 2018.

d) **Resolución Ministerial Nº 087-2019-PCM** que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, modificando los artículos 1 y 2 de la Resolución Ministerial N° 119-2018-PCM y dejando sin efecto los artículos 2, 5 y 5-A de la Resolución Ministerial N° 004-2016-PCM, publicada el 19 de marzo de 2019.

e) **Resolución Directoral N° 022-2022-INACAL/DN** de la Dirección de Normalización del Instituto Nacional de Calidad – INACAL, publicada el 12 de enero del 2023, que entre otras normas, aprobó:

- NTP-ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la

[1] **NTP ISO/IEC 27001:2022** de Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición.
La Norma Técnica Peruana NTP-ISO/IEC 27001:2022 es la adopción nacional del estándar internacional ISO/IEC 27001:2022, por lo que en adelante se les denominará **ISO 27001**, indistintamente.

información. Requisitos. 3ª Edición. Reemplaza a la NTP-ISO/IEC 27001:2014.

- NTP-ISO/IEC 27002:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición. Reemplaza a la NTP-ISO/IEC 27002:2017.
- NTP-ISO/IEC 27005:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición. Reemplaza a la NTP-ISO/IEC 27005:2018.

f) **Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD** que aprueba la Directiva Nº 001-2023-PCM/SGTD que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital, publicada el 8 de setiembre de 2023.

g) **Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD** que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, publicada el 8 de setiembre de 2023.

h) **Resolución de la Superintendencia Nacional de los Registros Públicos Nº 048-2022-SUNARP/SN** que aprueba la actualización de la Política del Sistema Integrado de Gestión – SIG de la Superintendencia Nacional de los Registros Públicos publicada el 11 de abril de 2022.

i) **Resolución de la Gerencia General de los Registros Públicos N° 210-2022-SUNARP/GG** que aprueba la Directiva DI-002-2022-UOM-OPPM, denominada “Directiva que regula la emisión de los documentos normativos de la Sunarp”, publicada el 4 de julio de 2022.

j) **Marco de referencia y consulta**

- **NTP ISO/IEC 27001:2022** de Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición.

  La Norma Técnica Peruana NTP-ISO/IEC 27001:2022 es la adopción nacional del estándar internacional ISO/IEC 27001:2022, por lo que en adelante se les denominará **ISO 27001**, indistintamente.

- **NTP ISO/IEC 27002:2022** de Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición.

  La Norma Técnica Peruana NTP-ISO/IEC 27002:2022 es la adopción nacional del estándar internacional ISO/IEC 27002:2022, por lo que en adelante se les denominará **ISO 27002**, indistintamente.

- **NTP ISO/IEC 27005:2022** de Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición.

  La Norma Técnica Peruana NTP-ISO/IEC 27005:2022 es la adopción nacional del estándar internacional ISO/IEC 27005:2022, por lo que en adelante se les denominará **ISO 27005**, indistintamente.

4. Antecedentes

a) **Resolución Nº 270-2014-SUNARP/SN** del 31 de octubre de 2014, publicado el 4 de noviembre de 2014, se aprobó el documento de gestión interna denominado "Política del Sistema de Gestión de la Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos", y el documento denominado "Organización de la Seguridad de la Información" cuyos textos se adjuntaban a la resolución.

b) **Acta de Reunión N° 007-2019-SUNARP/CGD** del 23 de mayo de 2019, que, entre otros documentos, aprobó el "MU-001-SGSI-CGD Manual de Roles y Responsabilidades" v.01.

5. Definiciones

a) **Activo de información**: Todo aquello, tangible o intangible, que presenta valor para la organización y, por lo tanto, se debe proteger. Pueden ser activos de información activos de software (por ejemplo, las aplicaciones registrales), documentos (por ejemplo, títulos registrales), activos físicos, servicios, personal, imagen de la compañía y reputación.

Este término en las nuevas normas se generaliza para denominarse «fuente de riesgo» siendo el elemento que sólo o con otros puede originar un riesgo.

b) **Custodio del activo de información**: Persona responsable de la seguridad de información del activo durante el uso y custodia del mismo.

c) **Información:** La información es un activo que, al igual que otros activos comerciales importantes, es esencial para el negocio de una organización y, en consecuencia, debe protegerse adecuadamente. La información se puede almacenar en muchas formas, incluyendo: forma digital (por ejemplo, archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo, en papel), así como información no representada en forma de conocimiento de los empleados. La información puede transmitirse por diversos medios, incluidos: mensajería, comunicación electrónica o verbal. Cualquiera que sea la forma que adopte la información o el medio por el que se transmita, siempre necesita una protección adecuada.

d) **Propietario del activo de información**: Persona responsable de la gestión, producción, mantenimiento, uso y seguridad de los activos de la información.

e) **Propietario del proceso:** Unidad de organización quien tiene la responsabilidad y la autoridad definida para diseñar, implementar, controlar y mejorar los procesos a su cargo, con el propósito de asegurar que se cumpla su resultado previsto. También denominado *Dueño del proceso*.

f) **Propietario del riesgo**: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo

g) **Seguridad de la información:** La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información y tiene alcance Institucional. La seguridad de la información implica la aplicación y gestión de controles apropiados que implican la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito y la continuidad del negocio sostenido, y minimizar las consecuencias de los incidentes de seguridad de la información.

h) **SGSI** (Sistema de Gestión de Seguridad de la Información): En un alcance específico aprobado por la alta dirección, un SGSI consta de políticas, procedimientos, directrices y recursos y actividades asociados, gestionados

colectivamente por una organización, en la búsqueda de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. Analizar los requisitos para la protección de los activos de información y aplicar controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la implementación exitosa de un SGSI.

6. Asignación de Roles para la Seguridad de la Información

[Referencia: ISO 27001 5.3, A5.2]

En la Sunarp, la estructura de la organización para la Seguridad de la Información está compuesta básicamente por los siguientes roles[2] o funciones:

a) Superintendente Nacional (SN-SUNARP)
b) Comité de Gobierno Digital (CGD-SUNARP)
c) Auditor Interno del SGSI (AI-SGSI)
d) Gerente General (GG-SUNARP)
e) Jefatura Zonal (JZ-ZR)
f) Oficial de Seguridad y Confianza Digital (OSCD-SUNARP)
g) Jefe de la OTI (OTI-SC)
h) Equipo de Respuesta ante Incidentes de Seguridad de la Información (CSIRT-SUNARP)
i) Jefe UTI - Coordinador de Seguridad y Confianza Digital (UTI-ZR - CSCD)
j) Equipo Zonal de Respuesta ante Incidentes de Seguridad de la Información (CSIRT-ZR)
k) Participante en la seguridad de la información (PSI)
l) Propietario del Activo de la Información (PAI)
m) Custodio del Activo de la Información (CAI)
n) Propietario del Riesgo (PR)
o) Usuarios de la Información (UI)

La estructura organizativa descrita se esquematiza en la siguiente figura:

[2] El Diccionario de la lengua española de la RAE define “rol” como el “papel o función que alguien o algo cumple”.

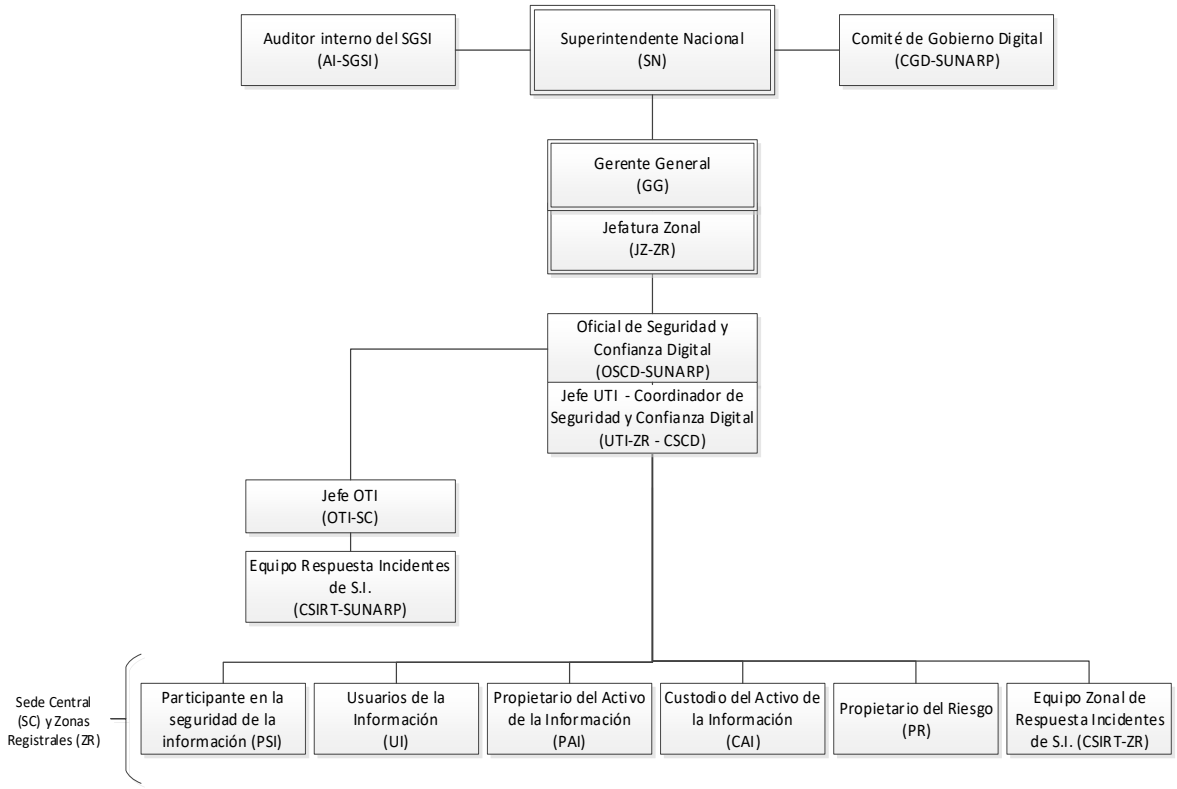

Figura 1. Estructura organizativa de seguridad de la información en la Sunarp

7. Asignación de Responsabilidades para la Seguridad de la Información

Las responsabilidades se han definido para realizar procesos específicos de dirección, gestión, operación, revisión, mejora y participación en seguridad de la información y en el SGSI.

7.1. Superintendente Nacional

El/la Superintendente Nacional de los Registros Públicos (SN) es la máxima autoridad y principal interesado en la seguridad de la información y representa la Alta Dirección de la Sunarp.

Respecto a la seguridad de la información, tiene las siguientes responsabilidades:

a) Evidenciar liderazgo y compromiso con la seguridad de la información[3].

b) Establecer una política y objetivos de seguridad de la información[4].

c) Establecer, asignar, empoderar y comunicar roles y responsabilidades relevantes a la seguridad de la información[5].

d) Revisar el SGSI de la Sunarp a intervalos planificados para asegurar su continua adecuación, conveniencia y efectividad[6].

7.2. Comité de Gobierno Digital

[3] En concordancia con la Cláusula "5.1 Liderazgo y compromiso" de la ISO 27001.
[4] En concordancia con el Artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD y la Cláusula "5.2 Política" de la ISO 27001.
[5] En concordancia con la Cláusula "5.3 Roles, responsabilidades y autoridades organizacionales" de la ISO 27001.
[6] En concordancia con la Cláusula "9.3 Revisión por la Dirección" de la ISO 27001.

El Comité de Gobierno Digital[7] (CGD-SUNARP) es el responsable directivo de la gestión y segundo máximo interesado en la seguridad de la información, complementando a el/la Superintendente Nacional.

Se constituye mediante resolución de Superintendencia Nacional y está integrado por funcionarios y servidores en cumplimiento de la normativa vigente.

El/la Superintendente Nacional, o su representante, preside el Comité de Gobierno Digital para liderar, dirigir, gestionar, mantener y mejorar la seguridad de la información y el SGSI.

Respecto a la seguridad de la información, tiene las siguientes responsabilidades:

a) Liderar y dirigir el proceso de transformación digital en la entidad.[8]

b) Dirigir y supervisar estratégicamente los planes, resultados y recursos del SGSI[9].

c) Dirigir y gestionar la implantación, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI, enfocado en las actividades y riesgos de la Sunarp según el modelo de mejora continua.

d) Revisar y presentar para aprobación de la Superintendencia Nacional la política general, objetivos, directivas, roles y responsabilidades de seguridad de la información.

e) Revisar y aprobar políticas específicas, metodologías, procedimientos, planes, programas, manuales, instructivos, registros y formatos del SGSI. Decidir el criterio para la aceptación de riesgos de seguridad de la información y los niveles de riesgo aceptables.

f) Gestionar la asignación de personal y recursos necesarios para la seguridad de la información y el SGSI en los Planes Operativos Institucionales, Plan Anual de Contrataciones y otros[10].

g) Promover y gestionar la implementación de estándares y buenas prácticas en gestión y seguridad digital[11].

h) Elaborar informes anuales que midan el desempeño y el progreso de la seguridad de la información y del SGSI de la Sunarp.[12]

i) Supervisar el cumplimiento de la normativa relacionada a seguridad de la información.[13]

j) Gestionar y revisar periódicamente la efectividad del SGSI.

k) Atender la respuesta a incidentes de seguridad de la Información que hayan sido escalados a su competencia.

[7] En concordancia con la Resolución Ministerial Nº 087-2019-PCM.
[8] En concordancia con el párrafo b) del Artículo 2 de la Resolución Ministerial Nº 087-2019-PCM.
[9] En concordancia con el Artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.
[10] En concordancia con el párrafo d) del Artículo 2 de la Resolución Ministerial Nº 087-2019-PCM.
[11] En concordancia con el párrafo e) del Artículo 2 de la Resolución Ministerial Nº 087-2019-PCM.
[12] En concordancia con el párrafo f) del Artículo 2 de la Resolución Ministerial Nº 087-2019-PCM.
[13] En concordancia con el párrafo g) del Artículo 2 de la Resolución Ministerial Nº 087-2019-PCM.

l) Aprobar la ejecución de auditorías internas o externas del SGSI a intervalos planificados.

m) Reunirse por lo menos una vez al mes para evaluar la situación institucional en materia de seguridad de la información y el plan de acción para la mejora continua.

n) Emitir opinión y recomendaciones sobre la gestión estratégica del SGSI, a solicitud del Titular de la Entidad o la máxima autoridad administrativa[14].

o) Otras responsabilidades que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

7.3. Auditor Interno del SGSI

El/la Auditor Interno del SGSI (AI-SGSI) es el responsable de determinar la conformidad del SGSI con los criterios de auditoría. Reporta y depende del Comité de Gobierno Digital.

El equipo de auditores internos es designado específicamente para una auditoría por la Gerencia General, a solicitud o propuesta del Comité de Gobierno Digital.

Tiene las siguientes responsabilidades:

a) Planificar, gestionar y llevar a cabo los procesos de auditorías internas en nombre de la Sunarp y en el período planificado.

b) Cumplir el Procedimiento de Auditorías Internas del SGSI.

c) Coordinar y gestionar la ejecución de las auditorías internas.

d) Verificar la eficacia, la eficiencia y la mejora continua del SGSI implementado.

e) Coordinar y gestionar el seguimiento, medición y verificación de la efectividad de la acción correctiva de la no conformidad hallada en el proceso de auditoría.

f) Elaborar oportunamente el informe de auditoría y reportarlo a la alta dirección o al Comité de Gobierno Digital.

g) Informar oportunamente el resultado de la auditoría a los auditados.

h) El Auditor Líder, es quien liderar a los auditores internos.

7.4. Gerente General

El/la Gerente General de la Sunarp (GG-SUNARP) es la máxima autoridad administrativa y también principal interesado en la seguridad de la información y representa la Alta Dirección de la Sunarp.

Respecto a la seguridad de la información, tiene las siguientes responsabilidades[15]:

a) Informar semestralmente al Titular de la entidad, los avances y dificultades en la implementación u operación del SGSI, así como el

[14] En concordancia con el Artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.

[15] En concordancia con el Artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.

cumplimiento de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.

b) Asegurar el cumplimiento de las políticas, objetivos, planes, procedimientos y marco normativo en materia de seguridad y confianza digital en la entidad pública.

7.5. Jefatura Zonal

La Sunarp, en su estructura organizativa cuenta con Zonas Registrales que son Órganos Desconcentrados que tienen por finalidad dirigir, promover y coordinar las actividades de las Oficinas Registrales dentro del ámbito de su competencia territorial, con el fin de cautelar que los servicios registrales sean brindados en forma eficiente y oportuna, dentro del marco legal correspondiente.

El/la Jefe Zonal (JZ-ZR), como funcionario de mayor jerarquía y responsabilidad en la Zona Registral, es también el máximo responsable y principal interesado de la seguridad de la información en su ámbito de acción debiendo tener un amplio conocimiento de los procesos, los activos de la información, los riesgos y la situación Institucional en materia de seguridad de la información.

Respecto a la seguridad de la información, tiene las siguientes responsabilidades:

a) Informar trimestralmente a la Gerencia General, los avances y dificultades en materia de Seguridad de la información de la Zona Registral a la que pertenece.

b) Asegurar el cumplimiento de las políticas, objetivos, planes, procedimientos y marco normativo en materia de seguridad y confianza digital en la Zona Registral.

c) Evidenciar liderazgo y compromiso con la seguridad de la información en la zona registral.

d) Proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad de la información.

e) Reunirse mensualmente, y cada vez que lo requiera, con los Coordinadores de Seguridad y Confianza Digital, a fin de analizar y evaluar la seguridad de la información y emitir informes a la Gerencia General o al Comité de Gobierno Digital (CGD-SUNARP).

f) Establecer, asignar, empoderar y comunicar roles y responsabilidades relevantes a la seguridad de la información en la zona registral.

g) Las demás funciones que se le encarguen en el ámbito de su competencia y aquellas concordantes con la materia.

7.6. Oficial de Seguridad y Confianza Digital

El/la Oficial de Seguridad y Confianza Digital (OSCD-SUNARP), o quien haga las veces, es un rol estratégico para la gestión digital en la entidad pública, reporta y depende de la Gerencia General, y actúa de conformidad con lo establecido en el marco legal de seguridad y confianza digital[16].

[16] En cumplimiento de lo establecido en el párrafo 3.2 del Artículo 3 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.

Es designado mediante resolución de Superintendencia Nacional a propuesta del Comité de Gobierno Digital.

El Oficial de Seguridad y Confianza Digital (OSCD-SUNARP) debe ser competente en la materia[17] y, para el cumplimiento de sus responsabilidades, está facultado a requerir la colaboración de otros órganos, unidades orgánicas u oficinas de la Sunarp en la medida necesaria.

Tiene las siguientes responsabilidades[17]:

a) Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

b) Coordinar con las unidades de organización de la entidad las acciones orientadas a implementar y/o mantener el SGSI, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

c) Formular y proponer políticas, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.

d) Promover la conformación y adecuada operación del equipo de respuestas ante incidentes de seguridad de la información.

e) Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.

f) Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.

g) Comunicar al CNSD los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.

h) Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.

i) Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la entidad pública e informarlos a la máxima autoridad administrativa.

j) Informar a la máxima autoridad administrativa acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la entidad, y sobre la aplicación efectiva de las normas en materia de seguridad de la

[17] En cumplimiento de lo establecido en la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, que aprueba la Directiva N° 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.

información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

k) Coordinar con el CNSD acciones de sensibilización y capacitación para los funcionarios y servidores civiles de la entidad sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

l) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la entidad, respectivamente.

m) Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.

n) Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las unidades de organización de la entidad su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.

o) Coordinar con el responsable de la unidad de organización de planeamiento y presupuesto de la entidad pública para asegurar una adecuada articulación con los instrumentos de gestión institucional comprendidos en los sistemas administrativos de presupuesto público, planeamiento estratégico, programación multianual y gestión de inversiones.

p) Liderar a los CSCD designados en la entidad pública para la adecuada implementación de la seguridad de la información.

q) Otras responsabilidades que le sean asignadas por el Titular de la entidad, Comité de Gobierno y transformación Digital o Gerencia General.

7.7. Jefe de la OTI

El/la Jefe de la Oficina de Tecnologías de la Información (OTI-SC) es designado mediante resolución de la Superintendencia Nacional.

Respecto a la seguridad de la información, tiene las siguientes responsabilidades[18]:

a) Informar al Oficial de Seguridad y Confianza Digital (OSCD) todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata.

b) Articular con el OSCD la implementación de controles de seguridad de la información y coordina con el Equipo de Respuestas ante Incidentes de Seguridad Digital la gestión de incidentes de seguridad digital.

7.8. Equipo de Respuesta ante Incidentes de Seguridad de la Información

[18] En concordancia con el Artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.

El Equipo de Respuesta ante Incidentes de Seguridad de la Información (CSIRT-SUNARP) es conformado mediante resolución de Superintendencia Nacional y sus miembros son designados por el Jefe de la OTI.

El Equipo de Respuesta ante Incidentes de Seguridad Digital de carácter institucional es responsable de la gestión de incidentes de seguridad digital que afectan los activos de la entidad pública. Dicho Equipo forma parte de los órganos o unidades orgánicas de Tecnologías de la Información de la entidad y por lo tanto reporta y depende de la Jefatura OTI.

Tiene las siguientes responsabilidades[19]:

a) Comunicar al Centro Nacional de Seguridad Digital los incidentes 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 y red de confianza.

d) Asegurar acciones de investigación y cooperación efectiva, eficiente y segura con el Centro Nacional de Seguridad Digital.

e) Gestionar los recursos y medidas necesarias para asegurar la efectiva atención 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 con otros Equipos de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital.

h) Los miembros de apoyo participarán en la ejecución de funciones, a requerimiento del Líder del "Equipo de Respuestas ante Incidentes de Seguridad Digital de la Sunarp", conforme corresponda a la naturaleza de sus competencias, debiendo el Jefe de la Oficina de Tecnologías de la Información informar a la Gerencia General, en forma trimestral, sobre la ejecución de las funciones asignadas al citado Equipo.

7.9. Jefe UTI - Coordinador de Seguridad y Confianza Digital

El Jefe UTI - Coordinador de Seguridad y Confianza Digital **(UTI-ZR - CSCD)** es un rol estratégico para la gestión digital en la Zona Registral, reporta y depende de la Jefatura Zonal, y actúa en conformidad con lo establecido en el marco legal de seguridad y confianza digital[20].

El UTI-ZR - CSCD actúa en conformidad con lo establecido en el marco legal de seguridad y confianza digital[21].El UTI-ZR - CSCD coordina y articula con el OSCD-SUNARP la implementación, operación, mantenimiento y mejora

[19] Basado en la "Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital", guía del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, disponible en https://www.gob.pe/institucion/pcm/informes-publicaciones/2986553-guia-para-la-conformacion-e-implementacion-de-equipos-de-respuestas-ante-incidentes-de-seguridad-digital.

[20] En cumplimiento de lo establecido en el párrafo 3.2 del Artículo 3 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.

[21] En cumplimiento de lo establecido en el párrafo 3.2 del Artículo 3 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD.

continua de la seguridad de la información de la Zona Registral a la que pertenece[22].

El UTI-ZR - CSCD, para el cumplimiento de sus responsabilidades, está facultado a requerir la colaboración de otros órganos, unidades orgánicas u oficinas de la Zona Registral en la medida necesaria.

Tiene las siguientes responsabilidades:

a) Reunirse por lo menos una vez al mes con el Jefe Zonal para evaluar la situación de la Zona Registral en materia de seguridad de la información y el plan de acción para la mejora continua.

b) Promover y disponer la difusión y el apoyo a la seguridad de la información al interior de la Zona Registral.

c) Promover y difundir la Política de Seguridad de la Información e impulsar planes y programas de capacitación y concientización en materia de seguridad de la información entre el personal de la Zona Registral.

d) Supervisar el cumplimiento de la normativa relacionada a seguridad de la información y de protección de datos personales.

e) Informar al Oficial de Seguridad y Confianza Digital (OSCD) todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata.

f) Articular con el OSCD la implementación de controles de seguridad de la información y coordinar con el Equipo de Respuestas ante Incidentes de Seguridad Digital la gestión de incidentes de seguridad digital. Dirigir y aplicar la Gestión de Riesgos de seguridad de la información e impulsar y monitorear la implementación del Plan de Tratamiento de Riesgos.

g) Dar seguimiento a los incidentes de seguridad de la información, evaluar riesgos y eventuales impacto.

h) Coordinar la respuesta a incidentes de seguridad de la información con el equipo zonal de respuesta a incidentes en primera instancia y con el CSIRT-Sunarp en segunda instancia o en caso no cuente con el equipo zonal.

i) Otras responsabilidades que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

7.10. Equipo Zonal de Respuesta ante Incidentes de Seguridad de la Información

El Equipo Zonal de Respuesta ante Incidentes de Seguridad de la Información (CSIRT-ZR) es optativo y la decisión de conformarlo depende de la disponibilidad del recurso humano.

El Equipo Zonal de Respuesta ante Incidentes de Seguridad de la Información es conformado por la Jefatura Zonal mediante resolución y sus miembros son designados por el Jefe de la UTI.

El Equipo Zonal de Respuesta ante Incidentes de Seguridad Digital es responsable de la gestión de incidentes de seguridad digital que afectan los

[22] En cumplimiento de lo establecido en el párrafo 8.2 de la Directiva N° 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital aprobado con Resolución N° 002-2023-PCM/SGTD.

activos de la Zona Registral a la que pertenece. Dicho Equipo forma parte de Unidad de Tecnologías de la Información y por lo tanto reporta y depende de la Jefatura UTI.

Tiene las siguientes responsabilidades[23]:

a) Comunicar al CSIRT-SUNARP los incidentes de seguridad digital y las alertas tempranas, avisos e información sobre riesgos e incidentes 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) Gestionar los recursos y medidas necesarias para asegurar la efectiva atención de incidentes de seguridad digital.

d) Coordinar y colaborar con otros Equipos Zonales de Respuestas ante Incidentes de Seguridad Digital, con la finalidad de fortalecer la seguridad digital en la Sunarp.

7.11. Participante en la seguridad de la información

El Participante (PSI) es el rol ineludible que concierne a todo el personal de la Sunarp, así como también al personal de instituciones y contratistas que intervengan en sus operaciones. Este rol es básico, generalizado y no inhibe a otros roles. Existe en la Sede Central y en las Zonas Registrales.

Tiene las siguientes responsabilidades:

a) Promover, difundir, cumplir y hacer cumplir las políticas, la normatividad y los controles de seguridad de la información.

b) Participar activamente en la preservación de la seguridad de la información (confidencialidad, integridad, confidencialidad).

c) Participar en la capacitación y concientización de seguridad de la información.

d) Reportar amenazas o vulnerabilidades de los activos de la información o de sus controles a la Mesa de Ayuda (o a quien haga las veces).

e) Reportar eventos o incidentes de seguridad de la información, real o potencial a la Mesa de Ayuda (o a quien haga las veces).

f) Colaborar con los otros roles.

g) Identificar no conformidades y oportunidades de mejora en la seguridad de la información.

h) Apoyar en el cumplimiento de las actividades de elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI.

i) Otras responsabilidades que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

7.12. Propietario del Activo de la Información

[23] Basado en la "Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital", guía del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, disponible en https://www.gob.pe/institucion/pcm/informes-publicaciones/2986553-guia-para-la-conformacion-e-implementacion-de-equipos-de-respuestas-ante-incidentes-de-seguridad-digital.

El Propietario del Activo de la Información (PAI) tiene la responsabilidad y autoridad para gestionar el activo de la información por lo que también es denominado *Responsable del Activo de la información*. Existe en la Sede Central y en las Zonas Registrales.

El Propietario del Activo de la información (PAI) debe conocer y entender el valor del activo y asumir voluntariamente su responsabilidad contribuyendo así al logro de los objetivos estratégicos de la organización. Debe tener capacidad para la toma de decisiones respecto al activo.

El Propietario del Activo de la información es identificado en la Matriz de Activos de la Información.

En la Sede Central, el Comité de Gobierno Digital aprueba la Matriz de Activos de la Información.

En las Zonas Registrales, el Jefe Zonal aprueba la Matriz de Activos de la Información.

Tiene las siguientes responsabilidades:

a) Participar en la designación de los miembros del equipo de trabajo para la valoración y tratamiento de riesgos de seguridad de la información. Apoya y participa activamente de estas actividades.

b) Revisar y dar la conformidad a la Matriz de Riesgos, el Plan de Tratamiento de Riesgos y la aceptación del riesgo residual correspondiente.

c) Informar al OSCD/CSCD, según corresponda, todo incidente de seguridad de la información que afecte los activos de la información a su cargo, de forma inmediata.

d) Articular con el OSCD/CSCD, según corresponda, la implementación de controles de seguridad de la información.

e) Es responsable de gestionar la implementación de los controles de seguridad de la información en los activos de la información que gestiona.

f) Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI.

g) Respecto a los activos de la información que gestiona:

- Que los activos estén inventariados y clasificados adecuadamente;
- Definir los niveles de acceso y privilegios de los usuarios y autorizar su asignación. Revisar periódicamente los accesos y privilegios otorgados. Que se cumpla las políticas aplicables de control de acceso.
- Que se cumpla las políticas aplicables cuando el activo es eliminado o destruido
- Determinar la seguridad de la información que los custodios deben implementar.
- Gestionar recursos.
- Estar informado sobre la integridad, confidencialidad y disponibilidad.
- Estar informado de los eventos o incidentes de seguridad de la información y tomar acción sobre ellos.

h) Otras responsabilidades que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

7.13. Custodio del Activo de la Información

El Custodio del Activo de la Información (CAI) brinda protección al activo de la información. Existe en la Sede Central y en las Zonas Registrales.

El Custodio del Activo de la información es identificado cuando se elabora la Matriz de Activos de la Información.

Tiene las siguientes responsabilidades:

a) Proteger al activo de la información que tiene en custodia en atención de la normatividad, lo requerido por el Propietario del Activo de la Información y las buenas prácticas.

b) Informar semestralmente al Propietario sobre el Activo de la Información.

c) Gestionar proactivamente la custodia del activo de la información a su cargo.

d) Informar al OSCD/CSCD, según corresponda, todo incidente de seguridad de la información que afecte los activos de la información a su cargo, de forma inmediata.

e) Articular con el OSCD/CSCD, según corresponda, la implementación de controles de seguridad de la información.

f) Otras responsabilidades que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

7.14. Propietario del Riesgo

El Propietario del Riesgo de seguridad de la información (PR) tiene la responsabilidad y autoridad para gestionar el riesgo del activo de la información, que se le ha asignado. Existe en la Sede Central y en las Zonas Registrales.

El Propietario del Riesgo de seguridad de la información (PR) debe entender el valor de gestionar los riesgos y asumir voluntariamente su responsabilidad contribuyendo así al logro de los objetivos estratégicos de la organización. Existe en la Sede Central y en las Zonas Registrales.

El Propietario del Riesgo es identificado en la Matriz de Riesgos de seguridad de la información.

En la Sede Central, el Comité de Gobierno Digital aprueba la Matriz de Riesgos.

En las Zonas Registrales, el Sub Comité de Riesgos aprueba la Matriz de Riesgos.

Tiene las siguientes responsabilidades:

a) Participar activamente en la elaboración, revisión y conformidad del Plan de Tratamiento de Riesgos y la aceptación del riesgo residual correspondiente. Es corresponsable de la conformidad mencionada.

b) Es corresponsable de gestionar recursos y de la implementación de los controles de seguridad de la información en los riesgos a su cargo.

c) Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI.

d) Velar que el riesgo que gestiona esté controlado.

e) Informar al OSCD/CSCD, según corresponda, todo incidente de seguridad de la información que afecte los activos de la información, de forma inmediata.

f) Articular con el OSCD/CSCD, según corresponda, la implementación de controles de seguridad de la información.

g) Otras responsabilidades que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

7.15. Usuarios de la Información

El Usuario de la Información (UI) utiliza adecuadamente el activo de la información y la información. Existe en la Sede Central y en las Zonas Registrales.

El Usuario de la Información es identificado cuando se elabora la Matriz de Activos de la Información.

Tiene las siguientes responsabilidades:

a) Utilizar adecuadamente la información y el activo de la información a los cuales se le ha otorgado acceso y está autorizado de acuerdo con el cargo vigente que desempeña.

b) Informar al OSCD/CSCD, según corresponda, todo incidente de seguridad de la información que afecte los activos de la información, de forma inmediata.

c) Articular con el OSCD/CSCD, según corresponda, la implementación de controles de seguridad de la información.

d) Otras responsabilidades que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

8. Disposiciones complementarias

8.1. **Propietario del documento**: Comité de Gobierno Digital (CGD)

Los aspectos no contemplados en la presente Directiva, serán resueltos por el Comité de Gobierno Digital.

Las modificaciones o mejoras serán canalizados al Oficial de Seguridad y Confianza Digital (OSCD-SUNARP).

8.2. **Clasificación del documento**: USO INTERNO

8.3. **Distribución**: COPIA NO CONTROLADA

CONTROL DE CAMBIOS

Ítem	Descripción del cambio	Código / Versión	Fecha
---	Elaboración inicial del documento	MN- -CGD-SN	08/03/2024

Firmado digitalmente por:
RONDON CHAVEZ Jorge Luis FAU 20267073580 hard
Motivo: Doy Visto Bueno del Documento
Fecha: 2024/04/18 16:03:16-0500

Firmado digitalmente por:
RICALDI ARAUZO Reymer Melchor FAU 20267073580 hard
Motivo: Doy Visto Bueno del Documento
Fecha: 2024/04/18 16:08:45-0500