RESOLUCIÓN DEL SUPERINTENDENTE NACIONAL DE LOS REGISTROS PÚBLICOS Nº 270 -2014-SUNARP/SN

Lima, 31 OCT. 2014

VISTO, el informe Nº 064-2014-SUNARP-OGTI/SG, de fecha 13 de octubre de 2014, el Acta del Comité de Seguridad de la Información Nº 003-2014-SUNARP/SGSI-CSI, el informe N° 232-2014-SUNARP/OGTI y el Informe Nº 019-2014-SUNARP/OSI;

CONSIDERANDO:

Que, mediante Resolución de Superintendencia Nº 321-2008-SUNARP/SN, se constituyó el Comité de Seguridad de la Información como instancia administrativa encargada de gestionar la seguridad de la información en la Sunarp, teniendo entre otras funciones la de formular, revisar, y aprobar la política de seguridad de la información, así como evaluar y proponer al Superintendente Nacional la política, directivas y responsabilidad generales en materia de seguridad de la información.

Que, mediante Resolución Ministerial Nº 129-2012-PCM, publicado en el Diario Oficial El Peruano con fecha 25 de mayo de 2012, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática, cuyos controles deberán ser implementados de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI Tecnología de la Información";

Que, en tal sentido el Comité de Seguridad de la Información ha formulado la Política del Sistema de Gestión de la Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos, que tiene por objetivo establecer el marco general de gestión para proteger adecuadamente los activos de la información y que define un conjunto de principios, lineamientos y responsabilidades para tal propósito;

Que, la Alta Dirección de la Sunarp como evidencia de su alto compromiso y en cumplimiento de la NTP-ISO/IEC 27001:2008, promueve, patrocina y facilita el proceso de establecimiento, implementación, operación y

mejora continua del Sistema de Gestión de Seguridad de la Información, para lo cual se requiere aprobar la Política de Seguridad de la Información;

Que, de conformidad con la facultad conferida por el literal x) del artículo 9° del Reglamento de Organización y Funciones de la SUNARP, aprobado por Decreto Supremo N° 012-2013-JUS;

SE RESUELVE:

Artículo Primero.- APROBAR 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 presentan en anexo adjunto y que forman parte integrante de la presente resolución.

Artículo Segundo.- DISPONER que lo establecido en la "Política del Sistema de Gestión de la Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos" y en la "Organización de la Seguridad de la Información", a que se refiere el artículo precedente, es de cumplimiento obligatorio por los funcionarios y servidores de la Sunarp.

Artículo Tercero.- DISPONER que el Reglamento de Seguridad de la Información de la Sunarp, aprobado mediante Resolución de Superintendencia N° 060-2010-SUNARP/SN, permanece vigente únicamente en los controles de los Capítulos III al XI del Título III los cuales se supeditan al Sistema de Gestión de la Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos; los títulos, capítulos y artículos derogados se encuentran definidos y establecidos en la documentación del SGSI.

Artículo Cuarto.- DISPONER que la Oficina General de Comunicaciones de la Sede Central, en coordinación con la Escuela de Capacitación Registral, difundan la "Política del Sistema de Gestión de la Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos" y la "Organización de la Seguridad de la Información" que por la presente resolución se aprueba.

Regístrese, comuníquese y publíquese en el portal institucional.

Mario Solari Zerpa
Superintendente Nacional de los Registros Públicos
SUNARP

sunarp
Superintendencia Nacional
de los Registros Públicos

POLÍTICA

del

Sistema de Gestión de Seguridad de la Información

Código: CSI-01-PO

El contenido de este documento está destinado únicamente para uso interno de SUNARP. No debe ser divulgado a terceros sin la autorización de SUNARP.

Elaborado por:	Revisado por:	Aprobado por:
Reymer M. Ricaldi Arauzo **Oficial de Seguridad de la Información**	Dr. Carlos A. Díaz Chunga **Comité de Seguridad de la Información**	Dr. Carlos A. Díaz Chunga **Secretario General**
Firma:	Firma:	Firma:

1. INTRODUCCIÓN

A continuación se desarrolla la Política del Sistema de Gestión de Seguridad de la Información (SGSI) de la Sunarp de acuerdo a lo establecido en la norma NTP ISO/IEC 27001:2008.

Este documento define la orientación ideológica y principios asumidos por nuestra Institución en relación a la seguridad de información, manifestado en la implementación, operación y mejora continua del SGSI.

2. POLÍTICA DEL SGSI

Sunarp tiene la misión de otorgar seguridad jurídica al ciudadano a través del registro y publicidad de derechos y titularidades, brindando servicios eficientes, transparentes y oportunos.

2.1 DECLARACIÓN

La Sunarp reconoce la información registral como un activo vital para la Institución y, con la finalidad de mantener su integridad, confidencialidad y disponibilidad, ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI), bajo el cual gestiona los riesgos de los procesos de Inscripción y Publicidad Registral.

2.2 OBJETIVOS

Considerando el Objetivo Estratégico General y, específicamente, los Objetivos Estratégicos Específicos número 1 y 2 del Plan Estratégico Institucional 2014 – 2017, respondiendo a los requerimientos de la norma NTP ISO/IEC 27001:2008, se enuncian los siguientes objetivos para el Sistema de Gestión de Seguridad de Información:

Objetivo General

Contribuir al fortalecimiento de la Seguridad Jurídica que se brinda a la ciudadanía a través del aseguramiento de tres aspectos fundamentales del proceso de Inscripción y Publicidad Registral: calificación, registro de partidas y asientos, y la publicidad registral.

Objetivos Específicos

- **Garantizar el acceso a la información registral a través de los mecanismos regulados**
- **Asegurar que la información sustentadora brindada por el usuario, se vea reflejada fielmente en el acto inscrito.**
- **Brindar publicidad, a través de los diferentes mecanismos establecidos por Sunarp, de forma continua a los usuarios.**

2.3 LINEAMIENTOS Y PRINCIPIOS

El Sistema de Gestión de Seguridad de la Información se basa en los siguientes lineamientos y principios:

- La operación del SGSI está enfocada en el robustecimiento de la seguridad de información de los procesos que forman parte de su alcance; para ello, capacita y sensibiliza periódicamente a su personal, promueve la conciencia del valor de la información y comunica los lineamientos de seguridad, roles, responsabilidades y obligaciones de seguridad de información a todas las partes involucradas; asegurando que sean comprendidos y cumplidos por el personal y terceros que tengan un vínculo con la Institución.

- Cada unidad orgánica de Sunarp tiene la responsabilidad de garantizar la integridad, confidencialidad y disponibilidad de la información que produce o utiliza. Para ello, se realiza periódicamente un proceso de gestión de riesgos, a partir del cual se proponen, diseñan e implementan controles para la reducción de riesgos, manteniendo un equilibrio entre la productividad y la seguridad de la información.

- Sunarp asume y exige el cumplimiento de la legislación, normativa y acuerdos suscritos con terceros, que están relacionados a la seguridad de información y que se encuentran vigentes.

- El Comité de Seguridad de la Información debe aprobar los lineamientos y controles del Sistema de Gestión de Seguridad de la Información, proveer los recursos necesarios para su implementación y verificar su eficacia.

- Es de cumplimiento obligatorio por el personal interno y externo de la Sunarp, en caso de incumplimiento se sanciona a los responsables teniendo como referencia al Reglamento Interno de Trabajo, contratos y convenios firmados.

- La política es comunicada a todo el personal de la institución y partes externas; es revisada anualmente y extraordinariamente cuando ocurren cambios significativos en el SGSI, para asegurar su conveniencia, adecuación y eficacia continua.

sunarp
Superintendencia Nacional
de los Registros Públicos

ORGANIZACIÓN
de la
Seguridad de la Información

El contenido de este documento está destinado únicamente para uso interno de SUNARP. No debe ser divulgado a terceros sin la autorización de SUNARP.

Elaborado por:	Revisado por:	Aprobado por:
Reymer M. Ricaldi Arauzo **Oficial de Seguridad de la Información**	Dr. Carlos A. Díaz Chunga **Comité de Seguridad de la Información**	Dr. Carlos A. Díaz Chunga **Secretario General**
Firma:	Firma:	Firma:

Índice

1. INTRODUCCIÓN

El presente documento contiene la estructura organizativa de roles y responsabilidades del Sistema de Gestión de Seguridad de la Información (SGSI) de Sunarp, alineado a lo establecido en la norma NTP ISO / IEC 27001:2008.

Este documento no regula otros aspectos de seguridad de la información, como el acceso a la información y a los sistemas de procesamiento, los planes de mejora y el cumplimiento de sus objetivos, la protección de las infraestructuras críticas y la forma de actuar en casos de emergencia. Estos aspectos serán detallados en disposiciones complementarias.

2. OBJETIVOS

Sunarp busca hacer una distribución efectiva de funciones y responsabilidades para la dirección, gestión y operación de la seguridad de la información en la institución, atendiendo al principio de segregación de funciones entre los integrantes de la Institución en aspectos relacionados a la seguridad, producción, procesamiento y revisión de la información.

3. ALCANCE

La organización interna de seguridad de la información en la Sunarp es de alcance nacional, en todos los procesos y en todas las actividades desarrolladas en la institución y para la institución.

Estas disposiciones son de cumplimiento obligatorio para todo el personal que labore en la Sunarp bajo cualquier modalidad de contrato, así como también a terceros que intervengan en sus operaciones (proveedores e instituciones con las que la Sunarp establezca convenios).

Como marco reglamentario de la implementación se cuenta con la Norma Técnica Peruana "NTP SO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos".

4. ESTRUCTURA ORGANIZATIVA

Las funciones para el mantenimiento y la mejora de la seguridad de la información se asignan a un grupo de responsables que se distribuyen en la Sede Central y en cada una de las Zonas Registrales.

La Sede Central dirige la gestión de la seguridad de la información de forma centralizada a través de la Superintendencia y de un Comité de Seguridad de la Información y, de forma descentralizada, a través de Supervisores de Seguridad de la Información quienes tienen como ámbito de acción a cada una de las Zonas Registrales a las que representan.

El esquema operativo definido está compuesto por los siguientes roles:

a) Superintendente Nacional de los Registros Públicos (SN-SUNARP)

b) Comité de Seguridad de la Información (CSI-SUNARP)

c) Jefes Zonales (J-ZRN°...)

d) Auditor Líder del SGSI (AL-SGSI)

e) Auditores Internos del SGSI (AI-SGSI)

f) Oficial de Seguridad de la Información (OSI-SUNARP)

g) Supervisor de Seguridad de la Información (SSI-ZRN°...)

h) Supervisor Adjunto de Seguridad de la Información (SSIA-ZRN°...)

i) Propietarios de la Información de la Zona Registral

j) Custodio de la Información de la Zona Registral

La estructura organizativa descrita se esquematiza en la siguiente figura:

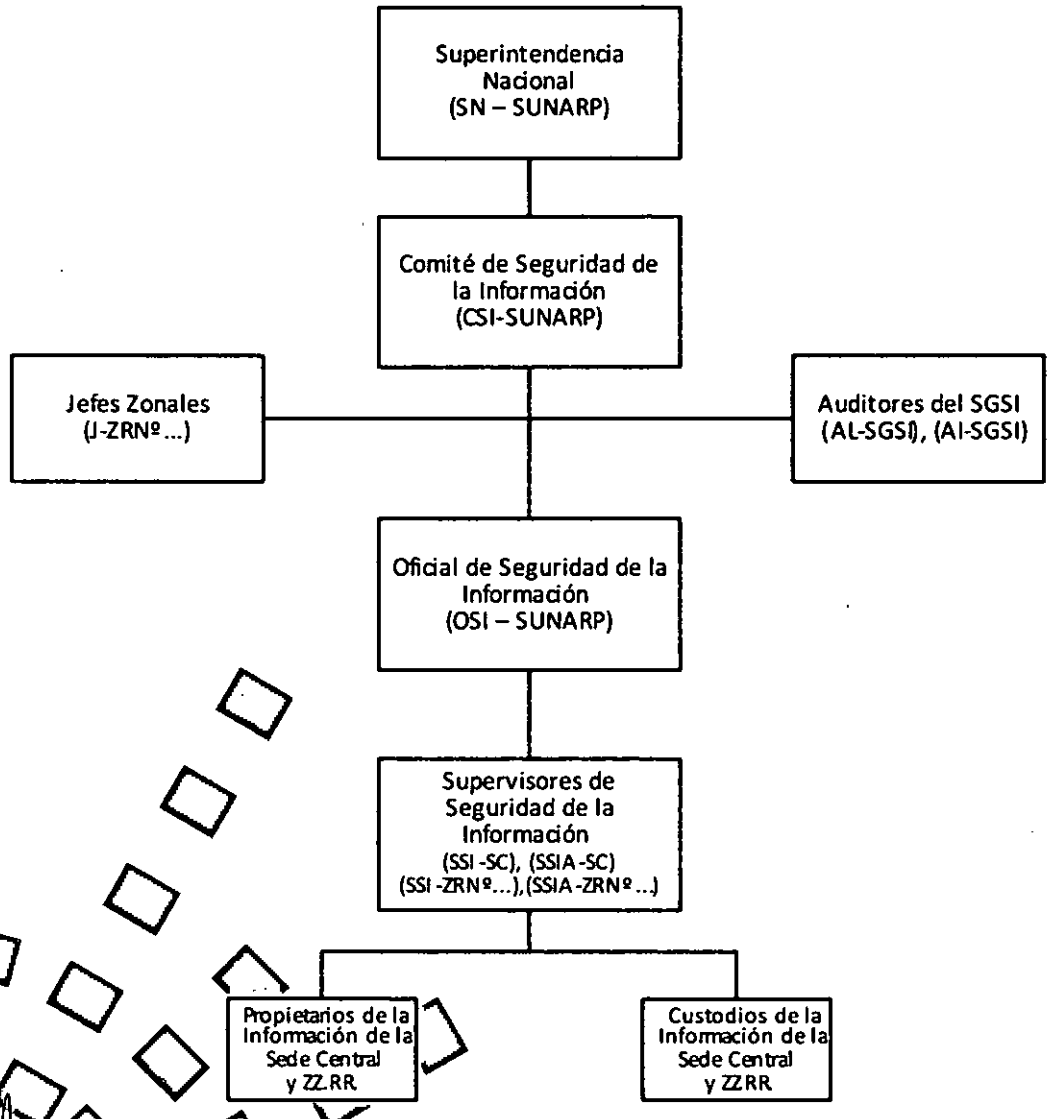

Figura 1. Estructura organizativa de seguridad de la información

5. ROLES Y RESPONSABILIDADES DEL SGSI

Se cuenta con la narrativa de las funciones y responsabilidades de cada uno de los roles involucrados en el ciclo del SGSI.

5.1 Organización central de seguridad de la información

Los responsables de la organización central desempeñan papeles principales en el planeamiento, gestión, operación y mejora de seguridad de la información. Su misión consiste en definir los objetivos y la estrategia corporativa en esa materia, trazar, dirigir y monitorear los planes para hacerla efectiva, así como coordinar, asesorar y prestar servicios de apoyo a los responsables de las organizaciones zonales.

5.1.1 Superintendente Nacional de los Registros Públicos (SN-SUNARP)

El Superintendente Nacional de los Registros Públicos es la máxima autoridad en seguridad de la información de la Institución.

En el SGSI, actúa directamente o a través del Secretario General.

Las responsabilidades del Superintendente Nacional de los Registros Públicos son:

a) Patrocinar el Sistema de Gestión Seguridad de la Información (SGSI) de la Sunarp.

b) Aprobar la política del Sistema de Gestión Seguridad de la Información (SGSI).

c) Aprobar el Plan Estratégico de Seguridad de la Información (PESI), proporcionar los recursos y la autoridad suficientes para llevarlos a cabo.

d) Aprobar la estructura organizativa interna de seguridad de la información.

e) Designar a los miembros del Comité de Seguridad de la Información.

f) Designar al Oficial de Seguridad de la Información.

g) Promover y patrocinar la capacitación y concientización del personal de la Sunarp en materia de seguridad de la información.

h) Llevar a cabo, en el último bimestre del año, la revisión del SGSI. Y, registrar las decisiones.

5.1.2 Comité de Seguridad de la Información (CSI-SUNARP)

El Comité de Seguridad de la Información de la Sunarp es el máximo órgano consultivo de carácter no técnico sobre la seguridad de la información.

Está presidido por el Secretario General.

El Comité de Seguridad de la Información se reunirá 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 mejorarla continuamente.

Los integrantes del Comité de Seguridad de la Información de la Sunarp son designados por resolución de Superintendencia Nacional.

Las funciones del Comité de Seguridad de la Información son las siguientes:

a) Informar a la Superintendente Nacional la situación Institucional en materia de seguridad de la información.

b) Proponer al Superintendente Nacional la designación del Oficial de Seguridad de la Información.

c) Designar a los miembros del Comité Consultivo de Seguridad de la Información.

d) Patrocinar y participar en la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión Seguridad de la Información (SGSI), enfocado en las actividades y riesgos de la Sunarp según el modelo PDCA:

Fase	Actividades
Establecimiento del SGSI	Definir y aprobar el alcance y límites del SGSI; definir y proponer a la Superintendencia Nacional la política del SGSI; definir, aprobar y proponer directivas, roles y responsabilidades generales en materia de seguridad de la información; definir y aprobar el enfoque de evaluación del riesgo; definir y aprobar los riesgos identificados; definir y aprobar el análisis y evaluación de riesgos; definir y aprobar opciones de tratamiento del riesgo; definir y aprobar los objetivos de control y controles propuestos para el tratamiento de riesgos; definir y aprobar los riesgos residuales propuestos; autorizar la implementación y operación del SGSI; definir y aprobar el documento de declaración de aplicabilidad.
Implantación y operación del SGSI	Definir y aprobar el plan de tratamiento de riesgos; garantizar la implementación del plan de tratamiento de riesgos y los controles seleccionados; definir y aprobar las métricas de efectividad de los controles seleccionados; patrocinar programas de capacitación y concientización; garantizar la operación del SGSI; aprobar recursos para el SGSI; garantizar la operación de mecanismos de detección y respuesta a incidentes de seguridad.
Monitoreo y revisión del SGSI	Evaluar la ejecución de procedimientos de monitoreo y control; patrocinar y participar en la revisión de la efectividad del SGSI (regularmente, por lo menos una vez al año); evaluar la revisión de la efectividad de los controles; revisar la evaluación de riesgos, el nivel de riesgos residual y el riesgo aceptable a intervalos planificados (por lo menos dos veces al año); evaluar los resultados de las auditorías internas y externas a intervalos planificados (por lo menos una vez al año); emprender una revisión gerencial del SGSI a intervalos planificados (por lo menos una vez al año); garantizar la actualización de los planes de seguridad con los resultados del monitoreo y revisión; registrar acciones y eventos que podrían afectar el funcionamiento o efectividad del SGSI.

Fase	Actividades
Mantenimiento y mejora del SGSI	Garantizar que las mejoras identificadas en las revisiones gerenciales y en las auditorías se implementen en el SGSI; garantizar que las acciones preventivas y correctivas se hayan ejecutado; comunicar las acciones y resultados a todas las partes interesadas, garantizar que las mejoras alcancen sus objetivos planificados.

Cuadro 1. Participación del Comité de Seguridad de la Información

e) Definir y evaluar el Plan Estratégico Institucional de Seguridad de la Información, garantizando que las metas de seguridad de la información sean identificadas y cumplidas, y que la seguridad de la información sea parte del proceso de planificación institucional.

f) Aprobar la memoria anual sobre el estado de seguridad de la información en la Sunarp y decidir sobre las propuestas de actuación incluidas.

g) Definir, evaluar y garantizar que la continuidad del negocio se gestione.

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

i) Resolver en última instancia los conflictos entre el resto de responsables cuando las intervenciones mediadoras del Oficial de Seguridad de la Información no hubieran sido suficientes.

j) Garantizar el cumplimiento de las exigencias legales en materias de seguridad de la información y de protección de datos personales.

k) Patrocinar auditorías internas y externas del SGSI a intervalos planificados (por lo menos una vez al año).

l) Promover y disponer la difusión y el apoyo a la seguridad de la información al interior de la Sunarp.

m) Iniciar planes y programas para mantener la conciencia en seguridad de la información entre el personal de la Sunarp.

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

o) Las demás funciones que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

5.1.3 Jefes Zonales

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 Jefe Zonal, como funcionario de mayor jerarquía y responsabilidad en la Zona Registral, es también el máximo responsable 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.

Las funciones de los Jefes Zonales en la organización de la Seguridad de la Información Institucional son las siguientes:

a) Informar trimestralmente al Comité de Seguridad de la Información la situación de la Zona Registral en materia de seguridad de la información.

b) Designar los Supervisores de Seguridad de la Información, principal y adjunto e informar la designación al Comité de Seguridad de la Información.

c) Patrocinar y participar en la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión Seguridad de la Información (SGSI) de la Sunarp en sus respectivas Zonas Registrales, según el modelo PDCA:

Fase	Actividades
Establecimiento del SGSI	Liderar y monitorear el proceso de identificación de los activos de información; liderar y monitorear el proceso de identificación de los riesgos; liderar y monitorear el proceso de análisis y evaluación de riesgos; proponer opciones de tratamiento del riesgo; proponer objetivos de control y controles para el tratamiento de riesgos; proponer los riesgos residuales.
Implantación y operación del SGSI	Liderar y monitorear la implementación el plan de tratamiento de riesgos y los controles seleccionados; proponer, implementar y monitorear programas de capacitación y concientización; auspiciar la operación del SGSI; solicitar y gestionar los recursos del SGSI; monitorear los mecanismos de detección y respuesta a incidentes de seguridad de la Información.
Monitoreo y revisión del SGSI	Supervisar el cumplimiento de las políticas y controles de seguridad de la información ejecutando procedimientos de monitoreo y control; revisar la efectividad de los controles implementados; revisar los riesgos, el nivel de riesgos residual y el riesgo aceptable a intervalos planificados (por lo menos dos veces al año); apoyar auditorías internas y auditorías externas del SGSI a intervalos planificados; registrar acciones y eventos que podrían afectar el funcionamiento o efectividad del SGSI. Evaluar los incidentes y vulnerabilidades de seguridad de la información a fin de identificar los controles a implementar.
Mantenimiento y mejora del SGSI	Implementar las mejoras identificadas en las revisiones y en las auditorias del SGSI; ejecutar las acciones preventivas y correctivas; gestionar y monitorear que las acciones y resultados del mantenimiento y mejora se comuniquen a todas las partes interesadas; gestionar y monitorear que las mejoras alcancen sus objetivos planificados

Cuadro 2. Participación de los Jefes Zonales en la Seguridad de la Información

d) Participar y garantizar que la continuidad del negocio se gestione.

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

f) Garantizar el cumplimiento de las exigencias legales en materias de seguridad de la información y de protección de datos personales.

g) Patrocinar auditorías internas y externas del SGSI a intervalos planificados.

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

i) Iniciar planes y programas para mantener la concientización en seguridad de la información entre el personal de la Zona Registral.

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

k) Proponer mejoras o iniciativas en materia de seguridad de la información al Comité o al Oficial de Seguridad de la Información en materia de gestión de riesgos, activos de información, procesamiento de la información, mejoras al SGSI, entre otros.

l) Ser "embajadores" de seguridad de la información para influenciar las opiniones de una forma positiva y, recoger las necesidades y expectativas de los trabajadores.

m) Reunirse mensualmente, y cada vez que lo requiera, con los Supervisores de Seguridad de la Información, a fin de analizar y evaluar la seguridad de la información y emitir informes al Comité de Seguridad de la Información.

n) Participar de las reuniones convocadas por el Comité de Seguridad de la Información.

o) Analizar las buenas prácticas de controles de seguridad a fin de proponer al Oficial de Seguridad su estandarización en todas las Zonas Registrales.

p) Opinar sobre el Sistema de Gestión de Seguridad de la Información.

q) Apoyar en el cumplimiento de las exigencias legales en materias de seguridad de la información y de protección de datos personales.

r) Apoyar en la definición de la estrategia de capacitación y concientización en materia de seguridad de la información.

s) Apoyar en la elaboración del análisis y evaluación de la situación Institucional en materia de seguridad de la información y contribuir en el plan de actuación para mejorarlo continuamente.

t) Facilitar el conocimiento y la aplicación de la normativa y de las medidas de seguridad en las distintas instancias de la Sunarp, buscando conseguir un clima positivo y de participación.

u) Las demás funciones que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

El Comité Consultivo de Seguridad de la Información de la Sunarp estará integrado por los siguientes miembros:

Integrante	Rol
Jefe de Zona Registral Nro I – Piura	Máximo responsable zonal
Jefe de Zona Registral Nro II – Chiclayo	Máximo responsable zonal
Jefe de Zona Registral Nro III – Moyobamba	Máximo responsable zonal
Jefe de Zona Registral Nro IV – Iquitos	Máximo responsable zonal
Jefe de Zona Registral Nro V – Trujillo	Máximo responsable zonal
Jefe de Zona Registral Nro VI – Pucallpa	Máximo responsable zonal
Jefe de Zona Registral Nro VII – Huaraz	Máximo responsable zonal
Jefe de Zona Registral Nro VIII – Huancayo	Máximo responsable zonal
Jefe de Zona Registral Nro IX – Lima	Máximo responsable zonal
Jefe de Zona Registral Nro X – Cuzco	Máximo responsable zonal
Jefe de Zona Registral Nro XI – Ica	Máximo responsable zonal
Jefe de Zona Registral Nro XII – Arequipa	Máximo responsable zonal
Jefe de Zona Registral Nro XIII - Tacna	Máximo responsable zonal
Jefe de Zona Registral Nro XIV - Ayacucho	Máximo responsable zonal

Cuadro 3: Jefes Zonales participantes en la Seguridad de la Información de Sunarp

5.1.4 Auditor Líder del SGSI

El Auditor Líder es quien debe liderar a los auditores internos y además es el responsable de lo siguiente:

a) Planificar y gestionar las auditorías internas en el período planificado.

b) Tomar conocimiento de los resultados de auditorías anteriores.

c) Asegurarse que los Auditores Internos mantienen sus habilidades y competencias.

d) Elaborar los informes y reportes finales de las auditorías internas.

e) Coordinar la ejecución de las auditorías internas.

f) Realizar la reunión de Apertura.

g) Requerir el informe de los auditores internos de forma oportuna.

h) Coordinar y gestionar con los Auditores Internos, el seguimiento, medición y verificación de la efectividad de las No Conformidades levantadas en los procesos de auditorías.

i) Reportar al área auditada los resultados de la auditoría.

j) Coordinar con los auditores internos el programa de auditoría para cada zona registral a nivel nacional y la sede central.

k) Realizar la Reunión de Cierre de acuerdo al Plan de Auditoría Interna, coordinando y acordando con cada zona los plazos para levantar las No Conformidades detectadas.

l) Mantener y salvaguardar los documentos correspondientes a la auditoria para entregar dichos documentos junto al informe final de auditoría y asegurar la confidencialidad permanente.

m) Verificar que el SGSI implementado se mantiene de manera eficaz.

n) Cumplir el Procedimiento de Auditoría Interna **(CSI-03-P)**

o) En caso necesario, realizar las funciones del auditor interno del SGSI.

5.1.5 Auditores Internos del SGSI

El Auditor Interno es el responsable de gestionar, preparar y llevar a cabo los procesos de Auditoría Interna institucionales en todas las zonas registrales a nivel nacional y Sede Central, para determinar el grado en el cual el Sistema de Seguridad de la Información cumple con los requisitos de la norma ISO 27001:2008.

Las funciones del Auditor Interno son las siguientes:

a) Elaborar conjuntamente con el Auditor Líder, el Programa Anual de Auditorías del SGSI para el año en curso en todo Sunarp.

b) Llevar a cabo la auditoría interna conforme al programa anual en la Sede Central o Zona Registral designada.

c) Revisar la documentación y otras evidencias de cumplimiento, para los procesos dentro del alcance del SGSI.

d) En caso necesario, realizar la reunión de Apertura.

e) Llevar a cabo las reuniones de relevamiento de información con el personal involucrado, para corroborar o extender sus indagaciones.

f) Recoger evidencias objetivas del área auditada a través de entrevistas, observación de actividades y revisión de registros con la finalidad de verificar la implementación del SGSI, y su efectividad.

g) Verificar que el SGSI es conforme con la norma y con los requisitos del SGSI, según corresponda.

h) Informar al área auditada sobre los hallazgos durante el proceso de auditoría. Y, esperar respuesta antes de emitir el informe de auditoría.

i) Redactar las no conformidades encontradas en el formato Solicitud de Acción Correctiva haciendo referencia a la cláusula de la ISO 27001:2008.

j) Elaborar el Informe de Auditoría Interna hacia el Auditor Líder.

k) Presentar el Informe de Auditoría Interna General al Auditor Líder del SGSI, anexando las Solicitudes de Acciones Correctivas de ser necesario.

l) En caso necesario, realizar la Reunión de Cierre de acuerdo al Plan de Auditoría Interna, coordinando y acordando con cada zona los plazos para levantar las No Conformidades detectadas.

5.1.6 Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información tiene la responsabilidad completa de la gestión de la Seguridad de la Información asegurando el correcto manejo de los activos de información. Coordina, implementa y controla las medidas técnicas y organizativas necesarias para garantizar la seguridad de la información y evitar su alteración, pérdida, procesamiento o acceso no autorizado.

El Oficial de Seguridad de la Información requerirá la colaboración de otros órganos u oficinas de la Sunarp en la medida en que fuera necesaria la participación de sus profesionales para cumplir sus funciones.

Las funciones del Oficial de Seguridad de la Información son las siguientes:

a) Informar a la Superintendencia Nacional y al Comité de Seguridad de la Información la situación Institucional en materia de seguridad de la información.

b) Coordinar con los propietarios de los activos de la información sus requerimientos de seguridad, la ejecución de los procesos de análisis y evaluación de riesgos. Promover y colaborar en el mantenimiento, difusión y aplicación de la política de seguridad de la información, así como en la redacción de las normas, procedimientos y guías de buenas prácticas que la desarrollen.

c) Asesorarse con el Comité Consultivo de Seguridad de la Información en materia de procesos que se realizan en la Sunarp, activos de información importantes y procesamientos de la información.

d) Realizar la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), enfocado en las actividades y riesgos de la Sunarp según el modelo PDCA:

Fase	Actividades
Establecimiento del SGSI	Participar en la definición del alcance y límites del SGSI; formular, revisar y proponer la política del SGSI; elaborar y proponer directivas, roles y responsabilidades generales en materia de seguridad de la información; proponer el enfoque de evaluación del riesgo; liderar el proceso de identificación de los activos de información; liderar el proceso de identificación de los riesgos; liderar el proceso de análisis y evaluación de riesgos; proponer opciones de tratamiento del riesgo; proponer objetivos de control y controles para el tratamiento de riesgos; proponer los riesgos

Fase	Actividades
	residuales; gestionar la implementación y operación del SGSI; preparar y proponer el documento de declaración de aplicabilidad.
Implantación y operación del SGSI	Formular y proponer el plan de tratamiento de riesgos; implementar el plan de tratamiento de riesgos y los controles seleccionados; proponer e implementa métricas de efectividad de los controles seleccionados; proponer e implementar programas de capacitación y concientización; gestionar la operación del SGSI; solicitar y gestionar los recursos del SGSI; gestionar mecanismos de detección y respuesta a incidentes de seguridad de la Información.
Monitoreo y revisión del SGSI	Supervisar el cumplimiento de las políticas y controles de seguridad de la información ejecutando procedimientos de monitoreo y control; revisar regularmente (por lo menos dos veces al año) la efectividad del SGSI; revisar la efectividad de los controles implementados; revisar la evaluación de riesgos, el nivel de riesgos residual y el riesgo aceptable a intervalos planificados (por lo menos dos veces al año); realizar auditorías internas y apoyar auditorías externas del SGSI a intervalos planificados (por lo menos una vez al año); apoyar en la revisión gerencial del SGSI a intervalos planificados; actualizar los planes de seguridad con los resultados del monitoreo y revisión; registrar acciones y eventos que podrían afectar el funcionamiento o efectividad del SGSI. Evaluar los incidentes y vulnerabilidades de seguridad de la información a fin de identificar los controles a implementar.
Mantenimiento y mejora del SGSI	Implementar las mejoras identificadas en las revisiones gerenciales y en las auditorias del SGSI; ejecutar las acciones preventivas y correctivas; elaborar y actualizar el Plan de Seguridad de la Información; gestionar que las acciones y resultados del mantenimiento y mejora se comuniquen a todas las partes interesadas; gestionar que las mejoras alcancen sus objetivos planificados

Cuadro 4: Participación del Oficial de Seguridad

e) Elaborar y proponer el Plan Estratégico Institucional de Seguridad de la Información, identificando objetivos estratégicos y asegurando que la seguridad de la información sea parte del proceso de planificación institucional. Asimismo, dirigir las actividades proyectadas en los planes estratégicos, controlando su grado de ejecución y eficacia.

f) Proponer la estructura organizativa de Seguridad de la Información.

g) Gestionar la continuidad del negocio.

h) Habilitar los canales de comunicación y participación oportuna, para todo el personal que labore en la Sunarp, con el objetivo de:

- Atender la respuesta a incidentes de seguridad de la Información.
- Intervenir en la gestión de las alertas, incidencias y problemas de seguridad que por su relevancia pudieran afectar o suponer un grave riesgo para la Sunarp y sus activos de información.
- Atender las cuestiones relativas a la seguridad de la información, la protección de datos personales y a la aplicación de las medidas de seguridad procedentes de quienes intervengan en el procesamiento de la información o desde cualquier instancia de la Sunarp.
- Mediar en los conflictos relacionados con asuntos de su competencia que sean sometidos a su consideración.

i) Gestionar el cumplimiento de las exigencias legales en materias de seguridad de la información y de protección de datos personales.

j) Realizar la difusión y apoyar la seguridad de la información al interior de la Sunarp. Informar a los distintos responsables sobre la adecuación, viabilidad e impacto de las actuaciones en materia de seguridad de la información, pudiendo proponer nuevas iniciativas o la modificación de las existentes.

k) Asesorar, coordinar e interactuar con los funcionarios de la Sunarp en materia de seguridad de la información.

l) Informar sobre la idoneidad de las tecnologías, productos y servicios utilizados por la Sunarp desde el punto de vista de la seguridad.

m) Definir la estrategia de capacitación y entrenamiento. Así como preparar los planes y programas de capacitación y concientización en materia de seguridad de la información.

n) Elaborar el análisis y evaluación de la situación Institucional en materia de seguridad de la información y proponer el plan de actuación para mejorarlo continuamente.

o) Identificar y proponer los cambios en seguridad de la información en respuesta a los cambios del ambiente organizacional, circunstancias del entorno, condiciones legales o cambios en el ambiente técnico.

p) Facilitar el conocimiento y la aplicación de la normativa y de las medidas de seguridad en las distintas instancias de la Sunarp, buscando conseguir un clima positivo y de participación.

q) Comunicar al Comité Consultivo de Seguridad de la Información las amenazas, incidentes y debilidades emergentes.

r) Establecimiento de las condiciones mínimas contractuales, técnicas y legales, para la seguridad de la información y la protección de datos personales por parte de terceros, así como el control de su cumplimiento y eficacia.

s) Homologar el procesamiento, en especial las aplicaciones informáticas y servicios de información, respecto a los requisitos de seguridad exigibles.

t) Elaborar la memoria anual sobre el estado de seguridad de la información en la Sunarp, que incluirá apartados dedicados a riesgos y mejoras.

u) Organizar los documentos de seguridad y realizar los controles de calidad correspondientes.

v) Las demás funciones que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

5.1.7 Supervisores de Seguridad de la Información

El Supervisor de Seguridad de la Información es designado por el Jefe de la Zona Registral y tiene la responsabilidad completa de la gestión de Seguridad de la Información en la Zona Registral asegurando el correcto manejo de los activos de información.

El Supervisor de Seguridad de la Información actuará en coordinación con el Oficial de Seguridad de la Información.

El Supervisor de Seguridad de la Información requerirá la colaboración de otras áreas funcionales de la Zona Registral en la medida en que fuera necesaria la participación de sus profesionales para cumplir sus funciones.

Las funciones del Supervisor Zonal de Seguridad de la Información son las siguientes:

a) Informar a la Jefatura Zonal la situación Institucional y de la Zona Registral en materia de seguridad de la información.

b) Coordinar con los propietarios de los activos de la información sus requerimientos de seguridad, la ejecución de los procesos de análisis y evaluación de riesgos. Promover y colaborar en el mantenimiento, difusión y aplicación de la política de seguridad de la información.

c) Coordina, implementa y controla las medidas técnicas y organizativas necesarias para garantizar la seguridad de la información y evitar su alteración, pérdida, procesamiento o acceso no autorizado.

d) Apoyar en la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión Seguridad de la Información (SGSI), enfocado en las actividades y riesgos de la Sunarp según el modelo PDCA:

- En el establecimiento del SGSI
- En la implantación y operación del SGSI
- En el monitoreo y revisión del SGSI
- En el mantenimiento y mejora del SGSI

e) Gestionar la continuidad del negocio en la Zona Registral.

f) Facilita, a través de los canales establecidos, la comunicación y participación oportuna de todo el personal que labore en la Zona Registral, con el objetivo de:

- Atender, en primera instancia, la respuesta a incidentes de seguridad de la Información. Intervenir en la gestión de las alertas, incidencias y problemas de seguridad que por su relevancia pudieran afectar o suponer un riesgo para la Sunarp y sus activos de información.

- Atender, en primera instancia, las cuestiones relativas a la seguridad de la información, la protección de datos personales y a la aplicación de las medidas de seguridad procedentes de quienes intervengan en el procesamiento de la información o desde cualquier instancia de la Sunarp.

- Escalar al Oficial de Seguridad de la Información, las atenciones que no pueda resolver. cuya relevancia así lo requiera o que considere necesario hacerlo.

- Registrar lo actuado en una bitácora e informar al Oficial de Seguridad de la Información. En los casos que no pueda resolver.

g) Cumplir las exigencias legales en materias de seguridad de la información y de protección de datos personales.

h) Realizar la difusión y apoyar la seguridad de la información al interior de la Zona Registral. Informar a los distintos responsables sobre la adecuación, viabilidad e impacto de las actuaciones en materia de seguridad de la información, pudiendo proponer nuevas iniciativas o la modificación de las existentes.

i) Informar sobre la idoneidad de las tecnologías, productos y servicios utilizados por la Zona Registral desde el punto de vista de la seguridad.

j) Elaborar el análisis y evaluación de la situación Institucional en materia de seguridad de la información de la Zona Registral y proponer las medidas para mejorarlo continuamente.

k) Identificar y proponer los cambios en seguridad de la información en respuesta a los cambios del ambiente organizacional, circunstancias del entorno, condiciones legales o cambios en el ambiente técnico.

l) Facilitar el conocimiento y la aplicación de la normativa y de las medidas de seguridad en las distintas instancias de la Zona Registral, buscando conseguir un clima positivo y de participación.

m) Comunicar al Oficial de Seguridad de la Información las amenazas, incidentes y debilidades emergentes.

n) Organizar los documentos de seguridad y realizar los controles de calidad correspondientes.

o) Las demás funciones que se le encarguen, y otras necesarias para cumplir con las disposiciones normativas en materia de seguridad de la información.

p) Participar con sus homólogos de otras Zonas Registrales y con el responsable de la seguridad de la información en la elaboración de los planes de seguridad corporativos, en la gestión de los planes vigentes y en la valoración de sus resultados.

q) Realizar un informe anual para el Jefe Zonal, con copia al Oficial de Seguridad de la Información, sobre el cumplimiento de los planes previstos, la efectividad de los controles aplicados, los nuevos riesgos detectados, y posibles cambios y mejoras.

r) En caso de ausencia del Supervisor Adjunto de Seguridad de la Información, es el único responsable.

5.1.8 Supervisor Adjunto de Seguridad de la Información

a) El Supervisor de Seguridad de la Información Adjunto tiene las mismas funciones que el Supervisor de Seguridad de la Información y participa plenamente en todas las actividades, asumiendo solidariamente la responsabilidad.

b) En caso de ausencia del Supervisor de Seguridad de la Información es el único responsable.

5.1.9 Propietarios de la Información de la Zona Registral

El Propietario de la Información de la Zona Registral es una persona designada por cada proceso de la organización y/o aplicación especializada; esta persona es llamada también como "responsable de la información" o "propietario de los activos de información" para todos los asuntos o temas de seguridad de la información relacionadas con el procesamiento de datos dentro de este proceso de la organización en particular.

El Propietario de la Información, o propietario del proceso, es responsable para la delegación de tareas y manejo de la información dentro de los procesos de la organización a la que han sido designados.

Las funciones del Propietario de la Información de la Zona Registral son las siguientes:

a) Identificar y clasificar los activos de su propiedad. Revisar periódicamente la clasificación de la información con la finalidad de verificar el cumplimiento de los requerimientos de seguridad de la Institución.

b) Autorizar el procesamiento de la información que está bajo su responsabilidad.

c) Valorar los riesgos de la información que está bajo su responsabilidad, o que se sometan a su consideración, y ordenar las actuaciones pertinentes. En caso de asumir riesgos, compartir riesgos o evitar riesgos, las acciones necesarias deben ser adoptadas desde el enfoque de seguridad de la organización.

d) Verificar que los controles o medidas de seguridad aplicados sean consistentes con la clasificación realizada.

e) Autorizar los accesos a la información que está bajo su responsabilidad.

Autorizar los accesos a los activos de información de su propiedad. Determinar los criterios y niveles de acceso. Revisar periódicamente los niveles de acceso de los usuarios.

f) De ser necesario, designar un responsable funcional para cada procesamiento diferenciado que tendrá la misión de hacer que el procesamiento de la información consiga los objetivos declarados, ciñéndose a ellos y cumpliendo los niveles exigibles de calidad, seguridad y eficiencia, tanto en condiciones normales como en situaciones excepcionales.

g) Determinar los periodos de retención de los activos de información (electrónica e impresa).

h) Autorizar la comunicación de información a terceros.

i) En coordinación con el Oficial de Seguridad de la Información, revisar y evaluar los resultados de la implementación de controles aplicados a los activos de su propiedad. Los procedimientos de resolución de incidencias y los planes de contingencia deberán formar parte de la coordinación.

j) Conseguir los elementos técnicos, materiales, humanos y organizativos necesarios para realizar el procesamiento.

k) Controlar la calidad y la eficiencia del procesamiento dentro de un ciclo de mejora continua.

l) Informará diligentemente de las alertas, incidencias o problemas de seguridad que detecte mediante los procedimientos de comunicación establecidos al efecto.

m) Designar a los Propietarios de la Información de la Zona Registral.

5.1.10 Custodios de la Información de la Zona Registral

El Custodio de los Activos de Información de la Zona Registral es el responsable del resguardo y de asegurar el buen uso de los activos de información; asimismo, del monitoreo del cumplimiento de los controles de seguridad en los activos que se encuentren bajo su administración.

Las funciones del Custodio de la Información de la Zona Registral son las siguientes:

a) Dar acceso a los usuarios de acuerdo con las especificaciones establecidas por los propietarios.

b) Administrar los accesos físicos o lógicos a los activos de información que permanecen bajo su custodia.

c) Cumplir con los controles implementados para la protección de los activos asignados para su custodia.

d) Administrar los procedimientos de respaldo, recuperación y restauración de información.

e) Reportar incidentes y debilidades de seguridad de la información.

f) En caso de identificar oportunidades de mejora, son comunicarlas a los responsables de Seguridad de la Información inmediatos.