MANUAL DE ROLES, RESPONSABILIDADES Y AUTORIDADES ORGANIZACIONALES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI-MA-02

Elaborado por:	Revisado por:	Aprobado por:
.....	.....	.....
Nombre y Firma	Nombre y Firma	Nombre y Firma

ÍNDICE

1. OBJETIVO

Asignar de manera efectiva los roles, las responsabilidades y las autoridades organizacionales para la dirección, gestión y operación del Sistema de Gestión de Seguridad de la información (SGSI), atendiendo al principio de segregación de funciones entre los integrantes de la entidad en aspectos relacionados al SGSI.

2. ALCANCE

Aplica a los directivos y al personal que forman parte de los procesos relacionados con el SGSI, según los roles que se encuentran establecidos para gestionar el SGSI en la entidad.

3. REFERENCIAS NORMATIVAS

- ISO/IEC 27000:2014 "Tecnología de la información. Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información – Visión General y Vocabulario".
- NTP ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”.
- ISO/IEC 27001:2013 "Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de Información - Requisitos".
- Resolución Ministerial Nº 004-2016-PCM. Aprueban 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. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

4. TÉRMINOS Y DEFINICIONES

4.1. Activo de Información: Conocimientos o datos que tienen valor para la SUNAT.

4.2. Confidencialidad: Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, entidades o procesos.

4.3. Disponibilidad: Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

4.4. Integridad: Propiedad de exactitud y totalidad de la información.

4.5. Incidente de Seguridad de la Información: Uno o serie de eventos de seguridad de la información, no deseados o inesperados, que tiene una probabilidad significativa de comprometer operaciones de negocio y amenazar la seguridad de la información.

4.6. Información: Conjunto de datos contenidos en documentos físicos (Papel, Microfichas, Libros, etc.), medios magnéticos (Cintas, Cartridge, Discos), medios ópticos (CD's, CDR, CDRW, DVD, etc.) y medios electrónicos (USB, Disco Duro Externo, etc.).

4.7. Propietario del Activo de Información: Identifica a la persona o la unidad orgánica que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos, tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

4.8. Propietario del Riesgo: Persona o entidad que tiene la responsabilidad y la autoridad para gestionar un riesgo.

4.9. Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.

4.10. Sistema de Gestión de Seguridad de la Información (SGSI): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, mantener y mejorar la seguridad de la información.

4.11. Usuario de la Información: Persona registrada y autorizada a utilizar un sistema de información determinado, bajo un nivel de acceso pre-establecido.

4.12. Revisión por la Dirección: La Alta Dirección (referido al Comité de Gestión de Seguridad de la Información) debe revisar el sistema de gestión de seguridad de la información de la SUNAT a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.

5. ORGANIZACIÓN INTERNA

La SUNAT dirige el SGSI a través del Comité de Gestión de Seguridad de la Información (CGSI), y coordinado por el Oficial de Seguridad de la Información. Los roles y autoridades identificados que soportan el SGSI son:

- Superintendente Nacional.
- Comité de Gestión de Seguridad de la Información (CGSI).
- Oficial de Seguridad de la Información.
- Equipo de Gestión del Riesgo.
- Propietario del Activo.

- Custodio del Activo de Información.
- Propietario del Riesgo.
- Intendentes, Gerentes o Jefes de Áreas.
- Usuarios de la Información.

6. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las responsabilidades de los roles y autoridades del SGSI de la SUNAT, son descritos en los siguientes numerales.

6.1. Superintendente Nacional

Tiene la responsabilidad de presidir el CGSI, a fin de dirigir el gobierno, gestión y operación del SGSI, dando evidencia del liderazgo y compromiso de la Alta Dirección de la SUNAT en la implementación, mantenimiento y la mejora continua del SGSI. El Superintendente Nacional podrá delegar sus responsabilidades en un representante. A continuación, se describen sus principales responsabilidades:

- Asegurar la disponibilidad de los recursos (humanos, de infraestructura, financieros y tecnológicos) para la implementación y operación del SGSI a través de las unidades de organización competentes.
- Establecer el CGSI y designar a sus miembros.
- Liderar la Revisión por la Dirección del SGSI y respaldar los acuerdos que se tomen en la Revisión por la Dirección, para la mejora del SGSI.
- Aprobar roles y responsabilidades de la organización del SGSI.

6.2. Comité de Gestión de Seguridad de la Información (CGSI)

Es un Comité ejecutivo conformado por altos directivos de la entidad, designado para gestionar, supervisar, revisar e informar de manera permanente los aspectos del SGSI. El Comité es presidido por el Superintendente Nacional o su representante, tiene como coordinador al Oficial de Seguridad de la Información y está conformado por titulares o representantes de:

- El Superintendente Nacional o su representante.
- El Intendente Nacional de Administración.

- El Jefe de la Oficina Nacional de Planeamiento y Estudios Económicos.
- El Intendente Nacional de Sistemas de Información.
- El Intendente Nacional de Asesoría Legal Interna.
- El Intendente Nacional de Estrategias y Riesgos.
- El Oficial de Seguridad de la Información.

Los roles y responsabilidades del Comité incluyen aspectos tales como:

- Responsabilidad ejecutiva del proceso global de implementación y operación del SGSI, a partir de la información que brinde el Oficial de Seguridad de Información.
- Aprobar los cambios, resultado de las revisiones de los riesgos residuales, así como de los criterios de evaluación y aceptación de riesgos.
- Realizar revisiones de los indicadores de desempeño del SGSI, según el procedimiento definido.
- Dirigir las Reuniones de Revisión del SGSI por la Dirección, para analizar los temas, y determinar acuerdos y acciones a tomar para la mejora del SGSI sobre la base del análisis realizado.
- Promover la gestión de seguridad de la información en los procesos y cultura organizacional, a través del Oficial de Seguridad de Información.
- Gestionar la asignación de personal y recursos necesarios para la implementación del SGSI.
- Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, de conformidad con los requisitos del SGSI.
- Evaluar el desempeño del SGSI y reportarlo a la Alta Dirección.
- Revisar y aprobar la documentación relativa al SGSI exigida por la NTP ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, según los niveles de aprobación definidos en el procedimiento de control de la información documentada del SGSI:
  - Política, alcance y objetivos de seguridad.
  - Metodologías y Manual del SGSI.
  - Manual de Roles, Responsabilidades y Autoridades Organizacionales del SGSI.

  - Manual de Políticas Específicas.
  - Planes de Trabajo y Gestión.
- Revisar y aprobar el programa anual de auditorías y la propuesta de programación de capacitación para el personal sobre el SGSI, propuesto por el Oficial de Seguridad de Información.
- Otras responsabilidades que le asigne el Superintendente Nacional en el ámbito de su competencia y aquellas concordantes con la Seguridad de la Información.

6.3. Oficial de Seguridad de la Información

Es el coordinador del CGSI y principal responsable operativo de la implementación del SGSI en la SUNAT.

Tiene como responsabilidades:

- Implementar y operar el proceso del SGSI.
- Promover y coordinar la ejecución de todas las actividades relacionadas con el proceso de implementación del SGSI.
- Gestionar el control de documentos, como: versiones, almacenamiento, retención, conservación, recuperación, acceso, distribución, vigencia y disposición. Asimismo, gestiona los documentos externos.
- Elaborar la propuesta de la Política de Seguridad de la Información.
- Elaborar el programa anual de auditorías y el programa de capacitación del SGSI.
- Elaborar, implementar y monitorear los indicadores de desempeño del SGSI.
- Elaborar la documentación relativa al SGSI exigida por la NTP ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, según los niveles de elaboración definido en el procedimiento de control de la información documentada del SGSI.
- Liderar y desarrollar los talleres de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información.
- Gestionar el programa de concientización y sensibilización en Seguridad de la Información.

- Coordinar la Revisión del SGSI por la Dirección, generar la información de entrada para la revisión, apoyar al CGSI en el análisis de la información, registrar los resultados y realizar el seguimiento de los acuerdos generados.
- Reportar y comunicar al CGSI, sobre temas relacionados a:
  - Los indicadores de desempeño del Sistema de Gestión de Seguridad de la Información.
  - Los avances de la implementación del SGSI y sus controles.
  - El incumplimiento de las directivas y procedimientos de Seguridad de la Información.
  - La gestión del tratamiento de los incidentes de Seguridad de la Información.
- Recibir, evaluar, priorizar y derivar los incidentes que han sido reportados, notificando al personal de la SUNAT por las faltas o incumplimientos. De ser reiterativo, elevar a la Intendencia Nacional de Recursos Humanos los incidentes suscitados. Asimismo, gestionar los incidentes comunicando periódicamente al Comité de Gestión de Seguridad de la Información.
- Colaborar con los propietarios del activo, custodios del activo de información, propietarios del riesgo, intendentes, gerentes o jefes de áreas para el cumplimiento de las responsabilidades de éstos.
- Otras funciones que le asigne el CGSI en el ámbito de su competencia y aquellas concordantes con la Seguridad de la Información.

6.4. Equipo de Gestión de Riesgos

Es el conjunto de especialistas en los activos de información del proceso. Sus responsabilidades son:

- Conocer la metodología de gestión de riesgos de Seguridad de la Información.
- Participar activamente de los talleres de gestión de riesgos de Seguridad de la Información:
  - Identificación de activos de información.
  - Identificación de riesgos.
  - Análisis de riesgos.
  - Evaluación de riesgos.
  - Tratamiento de riesgos.
- Proponer controles a ser evaluados dentro del marco de plan de tratamiento de riesgos.

- Identificar oportunidades relacionadas a la seguridad de la información.
- Revisar los riesgos residuales; así como los criterios de evaluación y aceptación de riesgos, en coordinación con el Propietario de Riesgos.

6.5. Propietario del Activo de Información

El propietario del activo es quien tiene la responsabilidad de la producción, desarrollo, mantenimiento, uso y seguridad del activo de información, según corresponda. Sus responsabilidades son:

- Realizar la valorización de los activos de información a su cargo.
- Realizar la clasificación de los activos de información con el objetivo de asegurar el adecuado tratamiento de sus riesgos.
- Apoyar activamente en las actividades de identificación, análisis, evaluación y tratamiento de los riesgos de Seguridad de la Información.

6.6. Custodio del Activo de Información

El custodio del activo de información es responsable de mantener los niveles de protección adecuados en base a las especificaciones dadas por el propietario del riesgo. Sus responsabilidades son:

- Velar por la protección de los activos de información bajo su custodia y/o responsabilidad.
- Apoyar la implementación de los controles propuestos para la protección de los activos asignados para su custodia, según el plan de tratamiento de riesgos.
- Participar en las actividades de identificación, análisis, evaluación y tratamientos de riesgos de Seguridad de la Información, incluidos los relacionados a tecnología, de ser el caso.

6.7. Propietario del Riesgo

El propietario del riesgo es quien tiene la responsabilidad y autoridad para gestionar (seguimiento y control) el riesgo del activo de información. Sus responsabilidades son:

- Participar y/o delegar al personal que participará en las actividades de identificación, análisis, evaluación y tratamiento de los riesgos de Seguridad de la Información.
- Contribuir a la implementación de los controles de Seguridad de la Información que estén relacionados a sus responsabilidades.
- Revisar y aprobar la Matriz de Riesgos, Plan de Tratamiento de Riesgos y los riesgos residuales de seguridad de la información.
- Evaluar y aceptar el riesgo residual de seguridad del activo de información, y revisarlos periódicamente; así como los criterios de evaluación y aceptación de riesgos.
- Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI, cuando sea requerido.

Las responsabilidades del propietario de riesgo serán desarrolladas a partir de la información de los riesgos comunicados por el Oficial de Seguridad de la Información.

6.8. Intendentes, Gerentes o Jefes de Áreas

Los Intendentes, Gerentes o Jefes de Áreas son responsables de la difusión de la Política de Seguridad de la Información. Sus responsabilidades específicas son:

- Difundir de manera adecuada la Política de Seguridad de la Información, asegurando su correcto entendimiento en el personal a su cargo.
- Promover el cumplimiento de la Política de Seguridad de la Información.
- Facilitar el acceso a las instalaciones y documentos relevantes para la ejecución de las actividades de medición de indicadores, auditorías o revisiones.
- De ser el caso, con respecto a observaciones, no conformidad o mejora, producto de auditorías, acciones correctivas, revisiones por la dirección u otros:
  - Aprobar el plan de acción para la atención de la no conformidad, observación u oportunidad de mejora.
  - Gestionar las acciones correctivas o de mejora bajo su responsabilidad.
  - Reportar al Oficial de Seguridad de la Información, los avances en la realización de las acciones correctivas o de mejora, cuando sea requerido.

Las responsabilidades de los intendentes, gerentes o jefes de áreas serán desarrolladas a partir de la información de los riesgos comunicados por el Oficial de Seguridad de la Información.

6.9. Usuarios de la Información

En general cumplir con todas las disposiciones sobre Seguridad de la Información, y de manera particular:

- Cumplir con las políticas y procedimientos de Seguridad de la Información.
- Usar la información solamente para los propósitos autorizados por la SUNAT.
- Cumplir con los controles establecidos en las políticas y procedimientos definidos por la SUNAT.
- Informar de inmediato cualquier evento, vulnerabilidad, o incidente real o potencial a la Seguridad de la Información.
- Colaborar y disponer de su tiempo para atender las consultas o reuniones solicitadas por el Jefe de la Oficina de Seguridad Informática o el Especialista, con la finalidad de resolver el incidente.
- Participar en las charlas de concientización y sensibilización en Seguridad de la Información.
- Elaborar propuestas de mejora para el SGSI dentro del ámbito de su competencia.
- Reportar la no conformidad, observación u oportunidad de mejora detectada.

7. CONTROL DE CAMBIOS

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial	01	25/01/2019	Oficial de Seguridad de la Información