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

SGSI-MA-02

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

El presente documento aplica a todos los colaboradores y personal bajo modalidades formativas y terceros vinculados con la institución que forman parte del alcance del SGSI y a quienes se les haya asignado roles en el marco de la seguridad de la información.

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 la información. Requisitos.
- Resolución Ministerial Nº 004-2016-PCM, que aprueba el uso obligatorio de la NTP-ISO/IEC 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial Nº 004-2016-PCM.
- Resolución Ministerial N° 119-2018-PCM, que crea el Comité de Gobierno Digital, así como se establecen las funciones del mismo, su alcance, y los lineamientos de gestión y planificación en Gobierno Digital.
- Resolución Ministerial N° 087-2019-PCM, que modifica los artículos 1 y 2 de la Resolución Ministerial N° 119-2018-PCM, que crea el Comité de Gobierno Digital, así como se establecen las funciones del mismo, su alcance, y los lineamientos de gestión y planificación en Gobierno Digital.
- Resolución de Superintendencia N° 084-2019/SUNAT, que conforma el Comité de Gobierno Digital de la Superintendencia Nacional de Aduanas y de Administración Tributaria y deja sin efecto la conformación del Comité de Gestión de Seguridad de la Información de la SUNAT.

- Resolución de Superintendencia N° 142-2019/SUNAT, que modifica conformación del Comité de Gobierno Digital y designa Líder de Gobierno Digital de la Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT.

4. DEFINICIONES

4.1. **Activo de Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, equipamiento informático, edificios, personas, etc.) que tenga valor para la organización.

4.2. **Comité de Gobierno Digital:** Comité ejecutivo conformado por catorce (14) miembros (funcionarios), designados mediante resolución de la superintendencia nacional, encargados de gestionar, supervisar, revisar e informar, permanentemente, el estado de la implementación y operación del SGSI. De acuerdo con el artículo 4 de la Resolución Ministerial N° 087-2019-PCM, toda referencia que se efectúe al Comité de Gestión de Seguridad de la Información debe entenderse realizada al Comité de Gobierno Digital.

4.3. **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a personas , entidades o procesos no autorizados.

4.4. **Custodio del Activo de Información**: Persona o entidad que tiene la responsabilidad de mantener un adecuado nivel de protección de los activos de información en base a las especificaciones coordinadas con el Propietario del Activo de Información.

4.5. **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona, entidad o proceso autorizado.

4.6. **Equipo de Gestión de Riesgos:** Es el conjunto multidisciplinario de especialistas de la institución, que se conforma previo al inicio de las actividades de gestión de riesgos y con la finalidad de llevar a cabo dicha gestión. Entre sus miembros se debe considerar al Oficial de Seguridad de la Información, al Custodio del Activo de información, al Propietario del Activo de Información, al Propietario del Riesgo, al personal de la Gerencia de Seguridad de la Información y del proceso del cual se quiere evaluar los riesgos, entre otros que se consideren necesarios. Los miembros indicados pueden designar a sus representantes.

4.7. **Evento de Seguridad de la Información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de

la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

4.8. Integridad: Propiedad de la información relativa a su exactitud y completitud.

4.9. Incidente de Seguridad de la Información: Un sólo evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

4.10. Oficial de Seguridad de la Información: Es el responsable operativo de la implementación y mantenimiento del SGSI. Es designado mediante resolución de la superintendencia nacional.

4.11. Propietario del Activo de Información: Persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, recepción, desarrollo, mantenimiento, uso y seguridad de los activos. Tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

4.12. Propietario del Riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

4.13. Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información cualquiera sea su formato y soporte. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y confiabilidad también pueden estar involucradas.

4.14. Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

5. ORGANIZACIÓN INTERNA

La SUNAT dirige el SGSI a través del Comité de Gobierno Digital, presidido por el Superintendente Nacional o su representante, en coordinación con el Oficial de Seguridad de la Información. Los roles y autoridades identificados que soportan el SGSI son los siguientes:

- **Superintendente Nacional**.

- **Comité de Gobierno Digital**.
- **Oficial de Seguridad de la Información**.
- **Equipo de Gestión de Riesgos**.
- **Propietario del Activo de Información**.
- **Custodio del Activo de Información**.
- **Propietario del Riesgo**.
- **Intendentes, Gerentes o Jefes de las UUOO**.
- **Colaboradores, personal bajo modalidades formativas de la SUNAT**
- **Terceros vinculados con la institución**.

6. RESPONSABILIDADES DEL SGSI

6.1. Superintendente Nacional

- Asegurar la disponibilidad de los recursos necesarios (humanos, de infraestructura, financieros y tecnológicos) para la implementación y operación del SGSI.
- Definir y aprobar la estructura del Comité de Gobierno Digital y designar a sus miembros.
- Designar al Oficial de Seguridad de la Información de la institución.
- Presidir o designar a su representante para presidir el Comité de Gobierno Digital, con la finalidad de dirigir el gobierno, la gestión y la operación del SGSI y respaldar los acuerdos que se tomen para la mejora continua.

6.2. Comité de Gobierno Digital

- Gestionar, mantener y documentar el SGSI de la entidad, con apoyo del Oficial de Seguridad de la Información, vigilando el cumplimiento de la normatividad relacionada a seguridad de la información.
- Realizar las revisiones de los indicadores de desempeño del SGSI, que permitan la elaboración de informes anuales, asegurando que el SGSI alcance los resultados previstos.
- Efectuar la revisión del SGSI, asegurando una gestión eficaz y el cumplimiento de los requisitos del SGSI, promoviendo la mejora continua.

- Promover, comunicar y fomentar la gestión de la seguridad de la información, los requisitos de seguridad y la gestión de riesgos en los procesos y en la cultura organizacional.
- Gestionar la asignación de personal y recursos necesarios para la implementación y operación del SGSI.
- Revisar y aprobar la documentación relativa al SGSI según los niveles de revisión y aprobación definidos en el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01).
- 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

- Promover y coordinar la ejecución de todas las actividades relacionadas con el proceso de implementación y operación del SGSI.
- Gestionar el control de documentos, como: versiones, almacenamiento, retención, conservación, recuperación, acceso, distribución, vigencia y disposición. Asimismo, gestiona los documentos externos.
- Elaborar, implementar y monitorear los indicadores de desempeño del SGSI.
- Elaborar, revisar y aprobar la documentación relativa al SGSI según los niveles de elaboración, revisión y aprobación definidos en el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01).
- Liderar y desarrollar los talleres de análisis, evaluación y tratamiento de riesgos de seguridad de la información.
- Gestionar el programa de concientización y sensibilización en Seguridad de la Información.
- Gestionar el tratamiento de los incidentes de seguridad de la información tomando en cuenta lo definido en el Procedimiento para el Registro y Atención de Incidentes y Vulnerabilidades de Seguridad de la Información vigente.

- Promover y coordinar la ejecución de las actividades relacionadas con la implementación del SGSI.
- Coordinar la revisión del SGSI por el Comité de Gobierno Digital, generando la información de entrada para la revisión, apoyando en el análisis de la información, registrando los resultados y realizando el seguimiento de los acuerdos generados.
- Reportar y comunicar al Comité de Gobierno Digital, según corresponda, sobre temas relacionados a:
  - Los indicadores de desempeño del SGSI.
  - 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.
- Colaborar y orientar a los Propietarios del Activo de Información, Custodios del Activo de Información, Propietarios del Riesgo, Intendentes, Gerentes o Jefes de las UUOO para el cumplimiento de sus responsabilidades relacionadas al SGSI.

6.4. Equipo de Gestión de Riesgos

- Conocer la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01).
- Participar activamente de los talleres de gestión de riesgos de seguridad de la información y en las fases definidas en la Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01).
- Proponer controles a ser evaluados dentro del marco del 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 del Riesgo.

6.5. Propietario del Activo de Información

- Asegurar y mantener la confidencialidad, integridad y disponibilidad de los activos de información bajo su control.
- Realizar, en coordinación con el Oficial de Seguridad de la Información, la clasificación de los activos de información, de acuerdo con los estándares establecidos en la institución, así como etiquetar dichos activos, con el objetivo de asegurar el adecuado tratamiento de sus riesgos y establecer un nivel de protección adecuado.
- Apoyar activamente en las actividades de análisis, evaluación y tratamiento de los riesgos de seguridad de la información, así como en la elaboración del inventario de activos.

6.6. Custodio del Activo de Información

- Velar por la protección de los activos de información bajo su custodia y/o responsabilidad en coordinación con el Propietario del Activo de Información.
- Apoyar la implementación de los controles propuestos para la protección de los activos de información asignados para su custodia, según los planes de tratamiento de riesgos de seguridad de la información.
- Participar en las actividades de análisis, evaluación y tratamiento de riesgos de seguridad de la información.

6.7. Propietario del Riesgo

- Participar y/o delegar al personal que participará en las actividades de análisis, evaluación y tratamiento de los riesgos de seguridad de la información de la institución.
- Revisar y aprobar la Matriz de Riesgos de Seguridad y el Plan de Tratamiento de Riesgos de seguridad de la información, asegurando la eficacia de los controles a implementar.
- Evaluar y aceptar el riesgo residual de seguridad de los activos de información, y revisarlos periódicamente; así como los criterios de evaluación y aceptación de riesgos.

- Contribuir a la implementación de los controles de seguridad de la información que mitiguen los riesgos bajo su responsabilidad, reportando su avance cuando sea requerido.
- Gestionar la existencia del capital y recursos necesarios para la implementación de los controles.
- Brindar información oportuna y pertinente y disponer recursos para la elaboración de indicadores y métricas, así como en la ejecución de auditorías, revisiones y mejoras al SGSI, cuando sea requerido.

6.8. Intendentes, Gerentes o Jefes de las UUOO

- Reforzar la difusión, de manera adecuada, de 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, los procedimientos y toda normativa, control o disposición establecida en la entidad, sobre seguridad de la información, como parte del SGSI.
- Promover la participación del personal a su cargo en las actividades de concientización y sensibilización en seguridad de la información.
- Autorizar el acceso a las instalaciones, a documentos e información relevantes, y la disposición del personal a su cargo, para la ejecución de las actividades de medición de indicadores, auditorías, revisiones o investigación y solución de incidentes y vulnerabilidades de seguridad de la información.
- Gestionar los accesos otorgados al personal a su cargo, según los lineamientos establecidos en la institución.
- Aprobar planes de acción para la atención de no conformidades, observaciones u oportunidades de mejora, producto de auditorías, revisiones por la dirección u otros.
- Gestionar las acciones correctivas, correcciones o mejoras bajo su responsabilidad, y reportarlo cuando sea requerido.

6.9. Colaboradores de la SUNAT, personal bajo modalidades formativas

- Conocer y cumplir las políticas, procedimientos y toda normativa, control o disposición establecida en la entidad, sobre seguridad de la información, como parte del SGSI.
- Utilizar la información y sus activos únicamente para los propósitos autorizados por la SUNAT.
- Reportar inmediatamente, a través de los canales de comunicación establecidos en la institución, cualquier vulnerabilidad o evento que identifique o del que sospeche que comprometa o pueda comprometer las operaciones y afectar la seguridad de la información de la SUNAT.
- Proporcionar toda la información requerida y disponer de su tiempo para atender las consultas o reuniones solicitadas con la finalidad de resolver el incidente o vulnerabilidad reportada.
- Participar en las charlas de concientización y sensibilización en seguridad de la información promovidas por el personal a cargo del SGSI y la INRH.
- Proponer mejoras para el SGSI dentro del ámbito de su competencia.
- Reportar no conformidades u observaciones que sean identificadas durante el desempeño de sus labores diarias.

6.10. Terceros vinculados con la institución

- Conocer y cumplir las políticas, procedimientos y toda normativa, control o disposición establecida en la entidad, sobre seguridad de la información, como parte del SGSI.
- Utilizar la información y sus activos provistos como parte de los servicios brindados, únicamente para los propósitos autorizados por la SUNAT.
- Cumplir con lo estipulado en las cláusulas incluidas en contratos u órdenes de servicio, que están referidas a salvaguardar la confidencialidad, integridad y disponibilidad de la información de la institución.
- Brindar las facilidades necesarias para que la SUNAT verifique el cumplimiento de las condiciones y aspectos de seguridad de la información incluidos en contratos u órdenes de los servicios brindados.

7. CONTROL DE CAMBIOS

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial del documento	01	25/01/2019	Oficial de Seguridad de la Información
Modificación del rol de Usuarios por el de Colaboradores de la SUNAT y personal bajo modalidades formativas y terceros vinculados con la institución. Actualización de definiciones y otros.	02	22/03/2023	Oficial de Seguridad de la Información