San Isidro, 16 de Diciembre del 2024

RESOLUCION N° 000151-2024-PROMPERU/GG

Resolución de Gerencia General

VISTOS: Los Memorandos N° 344-2024-PROMPERU/GG-OTI y N° 373-2024-PROMPERU/GG-OTI, y el Informe N° 013-2024-PROMPERU/GG-OTI-BMF de la Oficina de Tecnologías de la Información; los Informe N° 097-2024-PROMPERU/GG-OPP y N° 105-2024-PROMPERU/GG-OPP de la Oficina de Planeamiento y Presupuesto; y los Informes N° 543-2024-PROMPERU/GG-OAJ y N° 569-2024-PROMPERU/GG-OAJ de la Oficina de Asesoría Jurídica;

CONSIDERANDO:

Que, según el artículo 2 de la Ley N° 30075, Ley de Fortalecimiento de la Comisión de Promoción del Perú para la Exportación y el Turismo – PROMPERÚ, la entidad es competente para formular, aprobar y ejecutar estrategias y planes de promoción de bienes y servicios exportables, así como de turismo interno y receptivo, promoviendo y difundiendo la imagen del Perú en materia turística y de exportaciones, de conformidad con las políticas, estrategias y objetivos sectoriales;

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, el Reglamento del Decreto Legislativo N° 1412, aprobado por Decreto Supremo N° 029-2021-PCM, señala, en el numeral 109.1 del artículo 109, que el Sistema de Gestión de Seguridad de la Información (SGSI), comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación;

Que, asimismo, el numeral 109.3 del artículo 109 del referido Reglamento del Decreto Legislativo N° 1412, establece que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación;

Que, con Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, se dispone que el Plan de implementación del Sistema de Gestión de Seguridad de la Información es el instrumento que establece, como mínimo, los objetivos, actividades, recursos, responsables y plazos para implementar un Sistema de Gestión de Seguridad de la Información, en un periodo máximo de tres (03) años,

y precisa que éste es aprobado por la máxima autoridad administrativa o la que haga sus veces en una entidad pública;

Que, de acuerdo con el artículo 17 del Decreto Supremo N° 004-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, se podrá disponer en el mismo acto administrativo que tenga eficacia anticipada a su emisión, sólo si fuera más favorable a los administrados, y siempre que no lesione derechos fundamentales o intereses de buena fe legalmente protegidos a terceros y que existiera en la fecha a la que pretenda retrotraerse la eficacia del acto el supuesto de hecho justificativo para su adopción;

Que, mediante el Acta de Reunión N° OTI-AREU-BMF-2024-09-06, el Comité de Gobierno y Transformación Digital, acuerda la aprobación del Plan de implementación del Sistema de Gestión de Seguridad de la Información;

Que, con Informe N° 013-2024-PROMPERU/GG-OTI-BMF, la Oficina de Tecnologías de la Información sustenta la aprobación del Plan de implementación del Sistema de Gestión de Seguridad de la Información, indicando que el mismo tiene como alcance los procesos misionales y de soporte: M01. Promoción del Turismo, M02. Promoción de las Exportaciones, M03. Promoción de inversiones empresariales y S05. Gestión de tecnologías de la información y comunicación (OTI), así como que, con este se dará inicio a las actividades contempladas en las cláusulas de las NTP ISO 27001:2022; siendo que, con Memorando N° 373-2024-PROMPERU/GG-OTI, la referida Oficina sustenta la eficacia anticipada del indicado Plan;

Que, a través del Informe N° 097-2024-PROMPERU/GG-OPP, complementado con Informe N° 105-2024-PROMPERU/GG-OPP, la Oficina de Planeamiento y Presupuesto emite opinión, señalando que el referido Plan se encuentra conforme con lo establecido en la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD y contiene la versión vigente del Mapa de Procesos de la Entidad;

De conformidad con lo dispuesto en el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; el Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas; el literal g) del artículo 15 del Texto Integrado del Reglamento de Organización y Funciones de la Comisión de Promoción del Perú para la Exportación y el Turismo – PROMPERÚ, aprobado por Resolución de Presidencia Ejecutiva N° 060-2019-PROMPERU/PE; y, la Resolución de Presidencia Ejecutiva N° 174-2024-PROMPERU/PE;

Con el visto bueno de la Oficina de Tecnologías de la Información, la Oficina de Planeamiento y Presupuesto, y la Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo 1.– Aprobar el Plan de implementación del Sistema de Gestión de Seguridad de la Información de la Comisión de Promoción del Perú para la

Exportación y el Turismo – PROMPERÚ, que en Anexo forma parte integrante de la presente Resolución, con eficacia anticipada al 2 de octubre de 2024.

Artículo 2.- Registrar el presente Plan en la Plataforma Facilita Perú, para conocimiento y evaluación del Centro Nacional de Seguridad Digital.

Artículo 3.- El responsable de actualización de la información del Portal de Transparencia de PROMPERÚ, en un plazo no mayor de cinco (5) días calendario contados desde el día siguiente de ser notificado de la presente Resolución, deberá hacer la publicación correspondiente en el Portal de Transparencia de la Entidad.

Regístrese y comuníquese.

Firmado digitalmente
ANGEL WILDER NAVARRO DIAZ
Gerente General (e)

PLAN DE TRABAJO PARA IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROMPERU

CONTENIDO

1. OBJETIVO 4
2. ALCANCE 4
3. MARCO LEGAL 4
4. GLOSARIO DE TÉRMINOS 5
5. DEFINICIONES 5
6. ALCANCE 5
7. DIAGNÓSTICO 6
8. ANÁLISIS CONTEXTUAL DE LA ORGANIZACIÓN 7
9. MAPA DE PROCESOS DE PROMPERU 8
10. DOCUMENTACIÓN DEL SGSI 9
11. RIESGOS IDENTIFICADOS PARA LA IMPLEMENTACIÓN DEL SGSI 11
12. ACCIONES PREVIAS Y PERMANENTES 12
13. HERRAMIENTAS DE APOYO AL SGSI 12
14. METODOLOGIA 13
15. CRONOGRAMA DE ACTIVIDADES 13
16. RECURSOS Y PRESUPUESTOS 13
17. MONITOREO Y EVALUACIÓN 13

INTRODUCCIÓN

La Presidencia del Consejo de Ministros – PCM, a través de la Secretaría de Gobierno y Transformación Digital, ente rector del Sistema Nacional de Transformación Digital, mediante Resolución N° 003-2023- PCM/SGTD, establece disposiciones para la adecuada implementación y mantenimiento del Sistema deGestión y Seguridad de la Información en todas las entidades públicas, para lo cual hacen uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI). Las entidades públicas aseguran que el SGSI establezca como alcance mínimo a los procesos misionales y aquellos relevantes para su operación y funcionamiento.

Asimismo, de tales disposiciones se desprende que, las entidades públicas que hayan implementado un SGSI, deben registrar el plan de actividades o documento(s) de planificación utilizados para la operación o mantenimiento del referido SGSI.

Al respecto, la Comisión de Promoción del Perú para la Exportación y el Turismo (en adelante, PROMPERÚ) tiene como propuesta de implementación del SGSI a los procesos misionales y uno de soporte determinados por el siguiente alcance:

- M01.Promoción del Turismo
- M02. Promoción de las Exportaciones
- M03. Promoción de inversiones empresariales
- S05. Gestión de tecnologías de la información y comunicación (OTI)

En ese sentido, el Plan de implementación del Sistema de Gestión de Seguridad de la Información para la PROMPERÚ, es un instrumento que contribuirá al logro de los objetivos estratégicos institucional de la Entidad, teniendo como objetivos primarios:

- Preservar la confidencialidad, integridad y disponibilidad de la información de la entidad pública.
- Fortalecer la cultura de seguridad de la información en los servidores, funcionarios y colaboradores de la entidad pública.
- Asegurar el cumplimiento normativo en materia de seguridad y confianza digital.
- Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información.

PLAN DE TRABAJO PARA IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROMPERU

1. OBJETIVO

Implementar el SGSI que permita gestionar las vulnerabilidades y amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información en PROMPERÚ.

2. ALCANCE

Comprende todos los requisitos constituidos en las cláusulas de la ISO/IEC 27001, requeridas para la implementación del SGSI para la PROMPERÚ.

3. MARCO LEGAL

- 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.
- ISO/IEC 27000:2014 "Tecnología de la información. Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Visión general y vocabulario".
- ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requisitos. 2a. Edición".
- Resolución Ministerial N° 041-2017-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 12207:2016.
- Decreto Legislativo N°1412 que aprueba la Ley de Gobierno Digital.
- Decreto de Urgencia N° 006-2020 Crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020 Aprueba el marco de Confianza Digital y establece medidas para su fortalecimiento.
- Resolución Ministerial N° 087-2019-PCM publicada el 22 de marzo de 2019, se modificó el artículo 1 de la Resolución Ministerial N° 119-2018-PCM, estableciendo los integrantes debían conformar el Comité de Gobierno Digital en cada entidad, así mismo establece que toda referencia que se efectúe al Comité de Gestión de Seguridad de la Información debe entenderse realizada al Comité de Gobierno Digital.
- Decreto Supremo N° 029-2021-PCM Aprueba el reglamento de la Ley de Gobierno Digital.
- Decreto Supremo N° 157-2021-PCM que aprueba el reglamento del Sistema Nacional de Transformación Digital.
- Mediante Resolución Directoral N° 022-2022-inacal/DN se aprueba la NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición Reemplaza a la NTP-ISO/IEC 27001:2014.

4. GLOSARIO DE TÉRMINOS

- OSCD: Oficial de Seguridad y Confianza Digital
- CGD: Comité de Gobierno Digital
- SGSI: Sistema de Gestión de Seguridad de la Información
- CNSD: Centro Nacional de Seguridad Digital
- SGTD: Secretaria General de Transformación Digital

5. DEFINICIONES

Se utilizarán los términos y definiciones de la Norma ISO/IEC 27000:2014, tales como:

- Confidencialidad. - Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.
- Integridad. - Propiedad de exactitud y lo completo.
- Disponibilidad. - Propiedad de ser accesible y utilizable por petición de una entidad autorizada.
- 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.

6. ALCANCE

6.1. Ámbito de aplicación

El presente plan aplica para los siguientes procesos misionales:

- M01. Promoción del Turismo
- M02. Promoción de las Exportaciones
- M03. Promoción de inversiones empresariales

Y el presente proceso de soporte

- S05. Gestión de tecnologías de la información y comunicación (OTI)

6.2. Actores claves involucrados

Los principales actores involucrados en el Plan de Implementación del SGSI, son los miembros del Comité de Gobierno Digital y los usuarios de los procesos misionales en el alcance del SGSI.

6.3. Organización para la implementación del SGSI

Para dar inicio a la implementación del SGSI, es necesario establecer el equipo de trabajo, y llevar a cabo reuniones con el Comité de Gobierno Digital para informar los avances. Entre los miembros de la organización del SGSI tenemos a los siguientes:

- **Patrocinador:** Esta función será desempeñada por el Titular de la entidad
- **Coordinador:** Gestionará las acciones necesarias para la implementación del SGSI y realizará las coordinaciones con los directores y/o jefes de los Órganos para la adopción de las medidas aprobadas por el Comité de Gobierno Digital. Esta función será desempeñada por el Oficial de Seguridad y Confianza Digital.
- **Comité de Gobierno Digital:** Conformado por funcionarios de PROMPERÚ aprobado con resolución de presidencia N° 000138-2023-PROMPERU/PE. Quienes brindan apoyo en el marco de sus funciones a efectos de contribuir en alcanzar los objetivos.
- **Equipo de Trabajo**: Ayudará en diversos aspectos de la implementación del SGSI, a tomar decisiones sobre diversos temas que requieren un enfoque multidisciplinario y a realizar tareas preestablecidas. Está conformado por personal que forma parte del alcance en la implementación del SGSI.

7. DIAGNÓSTICO

- ✓ PROMPERÚ no cuenta actualmente con un SGSI, tal cual lo establece la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, siendo esto de uso obligatorio para las entidades de la Administración Pública.
- ✓ El no contar con el SGSI aprobado implica el no cumplimiento de uno de los compromisos de Gobierno Digital, sobre la que ejerce supervisión y control la PCM en su calidad de ente rector, tarea que lo ejecuta a través del CNSD de la SGTD.
- ✓ El SGSI como herramienta de gestión facilita la gestión de riesgos de seguridad digital, específicamente los de seguridad de la información, como tal, su no implementación dificulta la administración de riesgos que son propios del entorno digital de PROMPERÚ, así como de toda infraestructura tecnológica de la que se sirve o con la que interactúan los diferentes procesos misionales de la entidad.
- ✓ En PROMPERU se produce y se gestiona información inherente a la misión institucional, los cuales se guardan en distintos medios y formatos, de los que no se tiene el control respectivo a nivel de activo y su grado de sensibilidad (criticidad).
- ✓ Matriz FODA a continuación se presenta el siguiente cuadro, evidenciando las fortalezas, oportunidades, debilidades y amenazas encontradas:

ANALISIS DE CONTEXTO INTERNO Y EXTERNO (FODA)

Fortalezas	Debilidad
✓ Alto compromiso de la Alta Dirección ✓ Alta Dirección firma los documentos de seguridad ✓ Presupuesto para iniciativas de seguridad a los procesos de negocio ✓ Existe un comité de Gobierno y Transformación Digital ✓ Existe coordinación directa entre el oficial de seguridad y confianza digital y la Alta Dirección ✓ Dentro del PEI se ha incluido aspectos de protección de seguridad de la información ✓ Existe asistencia aceptable a las charlas de sensibilización en seguridad de la información ✓ Se tiene plataforma tecnológica actualizada (no existe tecnología legacy) ✓ Buen clima laboral ✓ Se realizan simulacros de sismo con la participación del personal.	✓ Falta de comunicación entre los líderes de los procesos y el Oficial de seguridad y confianza digital ✓ Falta de configuraciones y actualizaciones a las políticas de seguridad de los equipos de infraestructura ✓ No se Apoya en la capacitación permanente del personal responsable ✓ Posibilidad de conflicto de interés dado que el Oficial depende del jefe de TI ✓ Alta rotación de personal ejecutivos

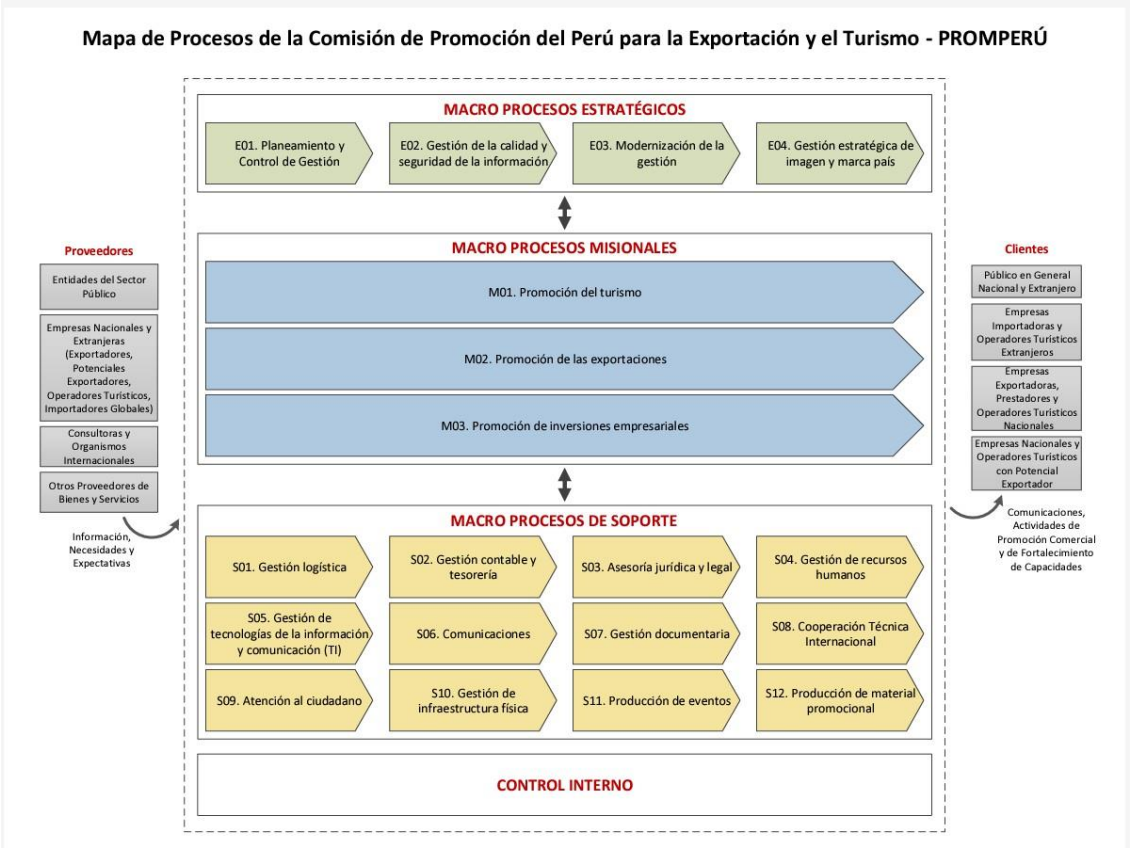
Oportunidad	Amenazas
✓ Presupuesto para adquirir componentes de energía de contingencia en las sedes principales. ✓ Realización de Ethical Hacking para subsanar las vulnerabilidades ✓ Posibilidad de ampliar el alcance del SGSI	Aspecto político: ✓ Cambios en la alta Dirección Aspecto económico ✓ Falta de presupuesto para proyectos de protección de datos personales Aspecto tecnológico: ✓ Hackers que puedan aprovechar en Páginas webs tecnológicas (ocurrió en 2023 un incidente grave) ✓ Activación de malware en ellos equipos de usuarios finales que ingresan con sus equipos personales (algunos sin validación de antivirus dado que las licencias se encuentran limitadas) Aspectos legales: ✓ Sanciones y multas por incumplimiento de la ley de protección de datos personales (no se tiene implementado o registrado ningún banco de datos).

8. ANÁLISIS CONTEXTUAL DE LA ORGANIZACIÓN

Según las normas de Gobierno Digital, el Comité de Gobierno y Transformación Digital de la entidad, tiene entre otras las funciones siguientes:

a) Gestionar la asignación de personal y recursos necesarios para la implementación del Plan de Gobierno Digital, Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) en sus planes operativos institucionales, Plan Anual de Contrataciones y otros.
b) Promover y gestionar la implementación de estándares y buenas prácticas en gestión y gobierno de tecnologías digitales, interoperabilidad, seguridad digital, identidad digital y datos en la entidad.
c) Elaborar informes anuales que midan el progreso de la implementación del Plan de Gobierno Digital y evalúen el desempeño del Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI).
d) Vigilar el cumplimiento de la normatividad relacionada con la implementación del Gobierno Digital, Interoperabilidad, Seguridad de la Información y Datos Abiertos en las entidades públicas.
e) Gestionar, mantener y documentar el Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad.

9. MAPA DE PROCESOS DE PROMPERU



10. DOCUMENTACIÓN DEL SGSI

Durante la implementación del Sistema de Gestión de Seguridad de la Información SGSI, se redactarán los siguientes documentos, sin perjuicio de otros que consideren pertinentes:

Nº	Norma Técnica Peruana NTP ISO/IEC 27001:2022	Documento	Descripción
1	Clausula 4.1 comprender la organización y su contexto. cláusula 4.2 comprender las necesidades y expectativas de las partes interesadas.	Análisis de contexto y requerimiento de seguridad de las partes interesadas.	Documento que establece el contexto interno y externo de PROMPERÚ y para asegurar que el SGSI está alineado con los objetivos institucionales y cumpla con las obligaciones legales y normativas relacionadas a la seguridad de la información.
2	Clausula 4.3 determinar el alcance del SGSI.	Alcance y límites del SGSI.	Documento que define en forma precisa la ubicación, la tecnología y los activos que forman parte del alcance de la implementación del SGSI.
3	Clausula 5.1 Liderazgo y compromiso de la Alta Dirección. Cláusula 5.2 Política.	Comunicados y apoyo de la Alta Dirección. Política y objetivos de la seguridad de la información.	Documento clave que establece el marco normativo para gestionar la seguridad de la información en PROMPERÚ.
4	Clausula 5.3 Roles, autoridad y responsabilidad organizacionales.	Roles y Responsabilidades del SGSI.	Documento que define la estructura organizacional para la dirección, gestión y operación de la seguridad de la información en PROMPERÚ.
5	Clausula 6.1 Acciones para tratar los riesgos y las oportunidades.	Metodología de la Gestión de Riesgos.	Documento que describe los métodos y parámetros para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información.
6	Clausula 6.1.2 Valoración del Riesgo de Seguridad de la Información.	Cuadro de análisis y evaluación de riesgos.	Documentación resultante del análisis y la evaluación de los riesgos de seguridad de la información.
7		Cuadro de tratamiento de riesgos.	Documentación que establece los controles de seguridad que se deben implementar para cada riesgo inaceptable.
8		Informe sobre el resultado de la gestión de riesgos y el tratamiento de los riesgos.	Documento que incluye los documentos generados en el proceso de gestión de riesgos.
9	Clausula 6.1.3 Tratamiento de riesgos de seguridad de la información.	Declaración de Aplicabilidad.	Documento que contiene los controles del Anexo A de la NTP ISO/IEC 27001:2022 y justifica la inclusión o exclusión de su implementación.
10		Plan de tratamiento de riesgos.	Documento que especifica un plan de trabajo priorizado de los controles que deben implementarse como resultado de la gestión de riesgos. Además de especificar los otros documentos que requieren para evidenciar la conformidad con la NTP ISO/IEC 27001:2022

11		Actas de aceptación de propietarios de riesgo.	Actas donde se expresa la conformidad de los propietarios de riesgo para el plan correspondiente.
12	Clausula 6.2 Objetivos de Seguridad de la Información.	Registro de objetivos de seguridad de la información.	Documento que debe ser medible, comunicada, brindar seguimiento y estar disponibles como información documentada.
13	Clausula 7.3 Concientización.	Plan de Concientización en Seguridad de la Información.	Documento que especifica un plan de formación en seguridad de la información.
14	Clausula 7.4 comunicaciones.	Registro de comunicaciones SGSI.	Documento que registra las partes internas y externas para llevar una eficiente comunicación en el marco del SGSI.
15	Clausula 7.5 Información documentada.	Procedimiento para la gestión de documentos y registros.	Documento que establece los lineamientos para la elaboración. Aprobación, distribución y actualización de los documentos y registros relacionados al SGSI.
16	Clausula 9.1 Monitoreo, medición, análisis y evaluación.	Procedimiento de medición y monitoreo del SGSI.	Documento que describe el proceso para evaluar el cumplimiento de los indicadores establecidos para el SGSI.
17	Cláusula 9.2 Auditoría interna.	Procedimiento de auditoría interna.	Documento que describe como se realizará la auditoría interna y se informará el resultado de la misma.
18	Clausula 9.3 Revisión de la gerencia.	Procedimiento de la revisión por la gerencia.	Documento que describe como se realizará la revisión por la Alta Dirección para asegurar la eficacia y efectividad del SGSI.
19	Cláusula 10.1 No conformidades y acción correctiva.	Procedimiento de acciones correctivas del SGSI.	Documento que describe el proceso de implementación de las acciones correctivas y preventivas, así como los formatos a emplear.

11. RIESGOS IDENTIFICADOS PARA LA IMPLEMENTACIÓN DEL SGSI

La implementación del SGSI contribuye al cambio de cultura organizacional en todos los niveles de la Institución.
A continuación, se detalla los principales riesgos que se pueden identificar en la implementación del SGSI y las acciones de mitigación, a fin de lograr el éxito del mismo.

Riesgos	Acciones de Mitigación
Cambio de los funcionarios de Alta Dirección.	La Alta Dirección dará continuidad a la ejecución de los planes aprobados. La Alta Dirección establecerá una política y objetivos de Seguridad de la Información que incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información. La Alta Dirección revisará el sistema de Gestión de Seguridad de la Información a intervalos planificados para asegurar su conveniencia, adecuación y efectividad continua.
Falta de recursos y personal especializado.	La Alta Dirección debe garantizar planificadamente la disposición de recursos que aseguren la implementación integral del SGSI y las necesidades que conlleva.
Falta de compromiso del personal del respecto a importancia de la seguridad de la información.	Se deben formular y llevar a cabo actividades de concientización relacionadas a seguridad de la información en PROMPERU, las cuales deberán ser establecidas en el plan de concientización.

12. ACCIONES PREVIAS Y PERMANENTES

12.1. Para el inicio de la implementación del SGSI

12.1.1. Compromiso de la Alta Dirección: con la finalidad de respaldar al equipo y las medidas aprobadas en el Comité de Gobierno Digital.

12.1.2. Análisis de brechas de seguridad de la Información: con la finalidad de determinar la distancia que existe entre la organización actual de la seguridad de la información y lo establecido en la ISO/IEC 27001.

12.1.3. Fortalecimiento de capacidades del coordinador del plan en los siguientes temas:

- COBIT 5 FUNDATIONS.
- ISO 27001.
- ISO 31000.
- ISO 27032.
- ETHICAL HACKING.

12.2. Durante la implementación del SGSI

12.2.1. Realización de Ethical Hacking: en intervalos anuales para determinar vulnerabilidades o intrusión a los sistemas informáticos.

12.2.2. Evaluación a los proveedores: enfocados proveedores que brindan servicio de almacenamiento de información, seguridad perimetral, software telefonía y otros de redes y comunicaciones.

12.2.3. Auditoria informática especializada: que permita establecer indicadores de cumplimiento y de gestión.

12.2.4. Implementación de proyectos de prevención de riesgos: Herramientas y/o servicios que permitan cubrirnos de lo posibles riesgos de seguridad de la información a los que estamos expuestos como entidad.

12.2.5. Fortalecimiento de capacidades de los participantes claves en los siguientes temas:

- Seguridad de la Información.
- Ethical hacking.
- Protección de datos personales.
- Informática forense.
- Ciberseguridad.

13. HERRAMIENTAS DE APOYO AL SGSI

- Todos los documentos se crearán empleando herramientas ofimáticas, dado que no se cuenta con una aplicación que automatice el Sistema de Gestión de Seguridad de la Información.
- Se creará una carpeta compartida en el DRIVE de GSUITE donde se almacenará las actas y los documentos generados durante la implementación del SGSI. Todos los miembros del equipo tendrán acceso a esos documentos en modo lectura. Solo el coordinador de la implementación del SGSI está autorizado a editar los datos.
- Se empleará la intranet y el correo institucional como plataforma o medio de comunicaciones para uso interno y para desplegar la concientización de seguridad de la información.

14. METODOLOGIA

Para la implementación del SGSI se empleará la metodología PDCA (Plan-Do-Check-Act), también llamada ciclo de DEMING, que impulsa al mejoramiento continuo de procesos y consiste en los siguientes pasos:

- Planear (PLAN): Reconocer una oportunidad y planificar el cambio.
- Hacer (DO): Probar el cambio.
- Verificar (CHECK): Revisar la prueba, analizar los resultados e identificar lo aprendido.
- Actuar (ACT): tomar acción basada en las lecciones aprendidas. Si el cambio fue exitoso, incorporar lo aprendido, de lo contrario intentar un plan diferente.

15. CRONOGRAMA DE ACTIVIDADES

El detalle de las actividades para la implementación está detalladas en el Anexo N°01 Cronograma de implementación SGSI, del presente documento.

16. RECURSOS Y PRESUPUESTOS

El presupuesto para la ejecución del plan de implementación del SGSI debería ser facilitado por la Oficina de Planeamiento y Presupuesto previo análisis y debería incorporarse al POI 2024.

De acuerdo a experiencias de otras entidades, de lo que se ha podido investigar en procesos de convocatorias similares, el presupuesto estimado asciende a S/40 mil soles.

17. MONITOREO Y EVALUACIÓN

Las actividades de monitoreo y evaluación serán llevadas a cabo al término de la implementación según el cronograma del presente Plan. Para el monitoreo se utilizará recursos propios y al personal de la Entidad, siendo liderado por el Oficial de Seguridad y Confianza Digital para el ejercicio de las evaluaciones se coordinaría una auditoría interna o externa de ser oportuno.

ANEXO

Anexo N° 01 Cronograma de implementación SGSI.

ANEXO 01 Cronograma de implementación SGSI.

CRONOGRAMA DE IMPLEMENTACIÓN SGSI ISO 27001

ACTIVIDADES		FECHA INICIO	FECHA FIN	RESPONSABLE	AVANCE (%)	2024			2025			
						M10	M11	M12	M01	M02	M03	M04
FASE I: PLANEAR					**25**	**MESES**						
1	Elaborar y aprobar el contexto externo e interno, partes interesadas y sus pertinencias.	**2/10/2024**	**31/10/2024**	PROVEEDOR /OSCD	**2**							
2	Elaborar y aprobar el alcance del Sistema de Gestión de Seguridad de la Información.	**2/10/2024**	**31/10/2024**	PROVEEDOR /OSCD	**2**							
3	Elaborar, actualizar y aprobar las Políticas de seguridad de la información.	**2/10/2024**	**31/12/2024**	PROVEEDOR /OSCD	**2**							
4	Elaborar y aprobar los objetivos de seguridad de la información.	**2/10/2024**	**31/10/2024**	PROVEEDOR /OSCD	**1**							
5	Elaborar y aprobar los indicadores de procesos relacionados a seguridad de la información.	**1/11/2024**	**30/11/2024**	PROVEEDOR /OSCD	**1**							
6	Elaborar y aprobar el Inventario de activos de información.	**1/11/2024**	**30/11/2024**	PROVEEDOR /OSCD	**2**							
7	Identificar, analizar y evaluar riesgos y oportunidades de seguridad de la información.	**1/11/2024**	**31/12/2024**	PROVEEDOR /OSCD	**2**							
8	Elaborar y aprobar el plan de tratamiento de riesgos y oportunidades de seguridad de la información.	**1/11/2024**	**31/12/2024**	PROVEEDOR /OSCD	**2**							
9	Elaborar y aprobar el documento de Declaración de Aplicabilidad.	**1/11/2024**	**31/12/2024**	PROVEEDOR /OSCD	**1**							
10	Elaborar y aprobar la matriz de comunicación de los Sistemas de Gestión	**2/10/2024**	**30/11/2024**	PROVEEDOR /OSCD	**1**							
11	Elaborar y aprobar el Programa de Sensibilización del SGSI	**1/12/2024**	**31/1/2025**	PROVEEDOR /OSCD	**2**							
12	Elaborar y aprobar el Programa de auditoría.	**1/1/2025**	**31/1/2025**	PROVEEDOR /OSCD	**1**							
13	Elaborar y aprobar el Formato de contacto de autoridades y grupos de interés.	**1/12/2024**	**31/1/2025**	PROVEEDOR /OSCD	**1**							
14	Elaborar y aprobar la Matriz RACI.	**1/12/2024**	**31/1/2025**	PROVEEDOR /OSCD	**1**							
15	Elaborar y aprobar la Matriz de requisitos legales y contractuales.	**1/12/2024**	**31/1/2025**	PROVEEDOR /OSCD	**1**							
16	Elaborar y aprobar el Manual de Seguridad de la Información	**1/12/2024**	**31/1/2025**	PROVEEDOR /OSCD	**1**							

FASE II: HACER					**50**							
17	Gestionar y/o realizar la implementación de controles de seguridad de la información e	**1/11/2024**	**28/2/2025**	PROVEEDOR /OSCD	**15**							
18	Implementar los manuales, protocolos y procedimientos en el marco del SGSI.	**1/11/2024**	**28/2/2025**	PROVEEDOR /OSCD	**5**							
19.1	Plan de recuperación antes desastres	**1/11/2024**	**28/2/2025**	PROVEEDOR /OSCD	**3**							
19.2	Plan de continuidad operativa	**1/11/2024**	**28/2/2025**	PROVEEDOR /OSCD	**2**							
FASE III: REVISIÓN					**75**							
20	Revisar la conformidad de los requisitos de la NTP ISO/IEC 27001:2022	**1/1/2025**	**28/2/2025**	PROVEEDOR /OSCD	**15**							
21	Auditoría interna	**1/1/2025**	**28/2/2025**	PROVEEDOR /OSCD	**5**							
22	Realizar la revisión con la alta dirección.	**1/1/2025**	**28/2/2025**	PROVEEDOR /OSCD	**5**							
FASE IV: ACTUAR					**100**							
23	Establecer e implementar acciones correctivas para las No Conformidades u oportunidad	**1/2/2025**	**28/2/2025**	PROVEEDOR /OSCD	**12.5**							
24	Tratamiento de los hallazgos de auditoría interna	**1/2/2025**	**28/2/2025**	PROVEEDOR /OSCD	**12.5**							
CERTIFICACIÓN INTERNACIONAL												
25	Certificación en la ISO 27001:2022	**1/3/2025**	**30/4/2025**	CASA CERTIFICADORA								

HOJA DE CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO O REVISIÓN	RESPONSABLE