Organismo de Evaluación y Fiscalización Ambiental

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ORGANISMO DE EVALUACIÓN Y FISCALIZACIÓN AMBIENTAL - OEFA

2024-2025

Organismo de Evaluación y Fiscalización Ambiental

Organismo de Evaluación y Fiscalización Ambiental

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN

El Estado Peruano, a través de la Política General de Gobierno aprobada por Decreto Supremo N° 042-2023-PCM establece entre otras disposiciones que, las entidades públicas hacen uso intensivo de las tecnologías digitales y datos para el cumplimiento de la Política General de Gobierno, en el marco del proceso nacional de transformación digital.

Asimismo, de acuerdo a lo establecido en el Artículo 3° del Decreto Legislativo N° 1412, Ley de Gobierno Digital (en adelante, ***la Ley de Gobierno Digital***), el gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. En este contexto, la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno y Transformación Digital, viene impulsando el proceso de transformación digital en las entidades de la administración pública coadyuvando a la generación de valor público de cara al ciudadano mediante la prestación de servicios digitales que garanticen la disponibilidad, integridad y confidencialidad de la información.

De igual manera, el Reglamento de la Ley de Gobierno Digital aprobado mediante Decreto Supremo N°029-2021-PCM en su Artículo 105° establece que las entidades públicas tienen entre sus obligaciones implementar y mantener un Sistema de Gestión de Seguridad de la Información (en adelante, ***el SGSI***). Asimismo, en su Artículo 109° se precisan algunas disposiciones para la definición del alcance, diseño, implementación, operación y mejora del SGSI.

Adicionalmente, el Artículo 4° del Decreto Supremo Nº 085-2023-PCM que aprueba la Política Nacional de Transformación Digital al 2030 establece que las entidades de la administración pública implementan la Política Nacional de Transformación Digital al 2030, en el marco de sus funciones y competencias, de tal manera de contribuir al cumplimiento de los objetivos de la Política Nacional de Transformación Digital, entre los cuales están el garantizar la disponibilidad de servicios públicos digitales inclusivos, predictivos y empáticos, así como consolidar la seguridad y confianza digital en la sociedad con la ciudadanía.

Bajo este contexto, a través de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD se dispone la implementación del SGSI utilizando la NTP ISO/IEC 27001 vigente, debiendo las entidades de la administración pública formular y aprobar el Plan SGSI, y registrarlo en la Plataforma Facilita Perú.

El *Plan de implementación del Sistema de Gestión de Seguridad de la Información en el Organismo de Evaluación y Fiscalización Ambiental - OEFA, 2024-2025* (en adelante, ***el Plan SGSI***) establece el marco de la implementación del SGSI bajo el estándar NTP ISO/IEC 27001:2022, contemplando los objetivos, el alcance, los recursos, el cronograma de actividades, el mecanismo de monitoreo, entre otros; a desarrollarse durante el periodo 2024 - 2025, y está orientado a contribuir al logro de los Objetivos Estratégicos Institucionales establecidos en el Plan Estratégico Institucional (en adelante, ***el PEI***) así como del Sistema de Gestión Integrado (en adelante, ***el SGI***) del Organismo de Evaluación y Fiscalización Ambiental - OEFA (en adelante, ***el OEFA***).

2. OBJETIVOS DEL PLAN SGSI

Implementar el SGSI bajo la Norma Técnica Peruana NTP ISO/IEC 27001:2022 en el alcance definido en el OEFA con miras a facilitar la prestación de servicios que generen valor público de manera segura, eficaz y que contribuyan al desarrollo de la economía digital y la sociedad del conocimiento.

3. MARCO LEGAL

3.1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
3.2. Ley N° 29733, Ley de Protección de Datos Personales.
3.3. Ley N° 31572, Ley del Teletrabajo.
3.4. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
3.5. Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
3.6. Decreto de Urgencia N° 007-2020-PCM, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
3.7. Decreto Supremo N° 118-2018-PCM, que declara de interés nacional las estrategias, acciones, actividades e iniciativas para el desarrollo del gobierno digital, la innovación y la economía digital en el Perú con enfoque territorial.
3.8. 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, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
3.9. Decreto Supremo N° 157-2021-PCM, Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital. Decreto Supremo que aprueba el Reglamento del Decreto de Emergencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, Decreto Supremo N° 157-2021-PCM.
3.10. Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.
3.11. Decreto Supremo N° 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030.
3.12. Decreto Supremo N.° 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales
3.13. Decreto Supremo N° 013-2017-MINAM, que aprueba el Reglamento de Organización y Funciones del OEFA.
3.14. Decreto Supremo N° 002-2023-TR, Decreto Supremo que aprueba el Reglamento de la Ley N° 31572, Ley del Teletrabajo.
3.15. Resolución del Consejo Directivo N° 00017-2023-OEFA/CD, que aprueba el Plan Estratégico Institucional para el periodo 2023-2028 del Organismo de Evaluación y Fiscalización Ambiental - OEFA.
3.16. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Seguridad de la Información en las Entidades Públicas.
3.17. Resolución Directoral N° 022-2022-INACAL/DN, que aprueba, entre otras, la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ra. Edición. Reemplaza a la NTP-ISO/IEC 27001:2014.

Las referidas normas incluyen sus modificatorias.

4. TÉRMINOS Y DEFINICIONES

4.1. **Confianza digital:** es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

4.2. **Comité de Gobierno y Transformación Digital:** es el mecanismo de gobernanza a nivel institucional para el gobierno y transformación digital en las entidades de la administración pública, responsable de liderar y dirigir el proceso de transformación digital en la entidad.

4.3. **Dueño del proceso:** Director/a, Subdirector/a, Jefe/a y Coordinador/a de un área del OEFA, quien tiene la responsabilidad y la autoridad definidas para diseñar, implementar, controlar y mejorar los procesos a su cargo, con el propósito de asegurar que se cumpla su resultado previsto. Asimismo, es responsable de apoyar en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como coadyuvar en la gestión de incidentes según corresponda.

4.4. **Economía digital:** es la innovación y transformación de la economía basada en el uso estratégico de las tecnologías digitales, redes de datos o comunicación y plataformas digitales. Produce beneficios económicos para la sociedad.

4.5. **Equipo Técnico y Multidisciplinario para la implementación y mantenimiento del SGSI (Equipo SGSI):** es el equipo encargado de realizar la implementación y mantenimiento del SGSI en la entidad, el cual es liderado por el/la Oficial de Seguridad y Confianza Digital. Está conformado por profesionales de la Oficina de Tecnologías de la Información tales como: el/la Oficial de Seguridad y Confianza Digital, el/la Gestor/a de Calidad, el/la Gestor/a de Infraestructura y Comunicaciones, el/la Gestor/a de Soporte Técnico, el/la Supervisor/a de Proyectos de Desarrollo de Sistemas y el/la Coordinador/a de Soluciones Tecnológicas, quienes poseen diversos conocimientos y habilidades, en especial, en materia de gestión de tecnologías de la información, gestión de seguridad de la información, gestión de riesgos, gobierno digital, gestión por procesos, entre otros.

4.6. **Oficial de Datos Personales:** es el rol responsable de velar por el cumplimiento de las normas en materia de protección de datos personales en su entidad. Dicho rol es ejercido por un/a servidor/a civil designado/a por la máxima autoridad administrativa de la entidad, el mismo que puede recaer en el/la titular de la oficina de asesoría jurídica de la entidad o en el/la titular de la oficina de tecnologías de la información de la misma, o quienes hagan sus veces.

4.7. **Oficial de Seguridad y Confianza Digital:** rol responsable de coordinar la implementación, operación, mantenimiento y mejora continua del SGSI en la entidad. Dicho rol recae en un/a servidor/a civil de la entidad que cuente con el conocimiento experiencia profesional y formación, de acuerdo con lo establecido en la Directiva Nº 001-2023-PCM/SGTD.

4.8. **Riesgo de seguridad de la información:** efecto de la incertidumbre sobre los objetivos de seguridad de la información de la entidad pública.

4.9. **Riesgo de seguridad digital:** efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan[1].

---

1 Literal g del artículo 3 del Decreto de Urgencia N° 007-2020.

4.10. **Seguridad digital:** es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno.

4.11. **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

4.12. **Sistema de Gestión Integrado (SGI):** conjunto de elementos interrelacionados que tienen por objetivo dirigir y fortalecer la gestión institucional de manera articulada y alineada conjuntamente con los requisitos del Sistema de Gestión de Calidad (SGC), Sistema de Gestión Antisoborno (SGAS), y el Sistema de Gestión de la Seguridad de la Información (SGSI).

4.13. **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.

4.14. **Transformación Digital:** es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intenso de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

5. ALINEAMIENTO ESTRATÉGICO DEL PLAN SGSI

El PEI para el periodo 2023-2028 Modificado del Organismo de Evaluación y Fiscalización Ambiental - OEFA, es el principal documento de gestión que define la estrategia y la línea de acción de la Entidad que define la cadena de valor de la fiscalización ambiental, la cual contribuirá a contar con un ambiente sano y a generar bienestar en la sociedad; planteando la misión unificada de toda la Entidad hacia el futuro, materializada en los retos y compromisos asumidos para poder alcanzar dicho cambio.

A continuación, se detalla el alineamiento del Plan SGSI con los del PEI:

Cuadro N° 1: Objetivos Estratégicos Institucionales vs Objetivos del Plan SGSI

Objetivo Estratégico Institucional del PEI 2023 - 2028 Modificado	Actividad Estratégica	Objetivo del Plan SGSI
OEI.04. Incrementar los niveles de transformación digital.	AEI.04.04. Seguridad de la información fortalecida en el OEFA	Implementar el SGSI bajo la Norma Técnica Peruana NTP ISO/IEC 27001:2022 en el alcance definido en el OEFA con miras a facilitar la prestación de servicios que generen valor público de manera segura, eficaz y que contribuyan al desarrollo de la economía digital y la sociedad del conocimiento.

Cabe señalar que el OEFA cuenta con un SGI que mantiene una política integrada. A continuación, se presenta la vinculación de los objetivos del Plan SGSI con la Política del SGI:

Cuadro N° 2: Política SGI y Objetivos SGSI vs Objetivos del Plan SGSI

Compromiso de la Política del SGI asociado al SGSI	Objetivos del SGSI[2]	Objetivo del Plan SGSI
Cumplir con los requisitos legales, de antisoborno, calidad, seguridad de la información u otros aplicables a los Sistemas de Gestión del OEFA.	Asegurar el cumplimiento normativo en materia de seguridad y confianza digital.	Implementar el SGSI bajo la Norma Técnica Peruana NTP ISO/IEC 27001:2022 en el alcance definido en el OEFA con miras a facilitar la prestación de servicios que generen valor público de manera segura, eficaz y que contribuyan al desarrollo de la economía digital y la sociedad del conocimiento.
Promover la mejora continua del sistema de gestión integrado del OEFA que permita incrementar el cumplimiento de nuestros objetivos institucionales.	Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información.	
Proteger los activos de información del OEFA de amenazas internas o externas, deliberadas o accidentales, con la finalidad de mantener la continuidad de nuestros servicios a través de la seguridad de la información de los procesos que forman parte del Sistema de Gestión de Seguridad de la Información del OEFA.	Preservar la confidencialidad, integridad y disponibilidad de la información del OEFA.	
	Fortalecer la cultura de seguridad de la información en los servidores, funcionarios y colaboradores en el OEFA.	

6. CONTEXTO DE LA ENTIDAD

Mediante la Segunda Disposición Complementaria Final del Decreto Legislativo N° 1013, Decreto Legislativo que aprueba la Ley de Creación, Organización y Funciones del Ministerio del Ambiente, se crea el OEFA como un organismo público técnico especializado, con personería jurídica de derecho público interno adscrito al Ministerio del Ambiente, encargado de la fiscalización, la supervisión, el control y la sanción en materia ambiental que corresponde.

A través de la Ley N° 29325, Ley del Sistema Nacional de Evaluación y Fiscalización Ambiental, se otorga al OEFA la calidad de Ente Rector del citado sistema, el cual tiene por finalidad asegurar el cumplimiento de las obligaciones ambientales fiscalizables por parte de los administrados, así como supervisar y garantizar que las funciones de evaluación, supervisión y fiscalización ambiental a cargo de las diversas entidades del Estado se realicen de forma independiente, imparcial, ágil y eficiente.

El análisis del contexto que orienta el desarrollo del Plan SGSI contempla la evaluación de: *(i)* la regulación en materia de seguridad de la información; y, *(ii)* la gestión de la seguridad de la información en la entidad.

6.1. Regulación en materia de seguridad de la información y gobierno digital

La Secretaría de Gobierno y Transformación Digital (en adelante, ***la SGTD***) como ente rector del Sistema Nacional de Transformación Digital, ha establecido los compromisos prioritarios[3] para cumplimiento de la legislación en materia de seguridad y gobierno digital en ruta hacia la transformación digital. Estas acciones específicas están relacionadas a la designación de roles para la gestión digital, planificación y estrategia, así como la ejecución de lo planificado.

A continuación, se presenta el estado de cumplimiento de los compromisos priorizados por la SGTD así como de la normativa vinculada a seguridad de la información y gobierno digital, clasificada por ámbito de aplicación:

---

[2] Objetivos del SGSI acorde al Artículo 1, numeral 1.2 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.

[3] Compromisos priorizados por la SGTD en el portal institucional de la Presidencia del Consejo de Ministros: https://www.gob.pe/39072-como-implementar-el-gobierno-digital-en-las-entidades-publicas

Cuadro N° 3: Estado de cumplimiento de la regulación de seguridad de la información y gobierno digital

Ámbito	Nº	Acciones y compromisos	Priorizado por la SGTD	Estado de cumplimiento
Gestión estratégica	1	Incorporar la transformación digital en el Plan Estratégico Institucional.	SI	COMPLETADO
	2	Desplegar la Estrategia Digital.	SI	COMPLETADO
Roles y responsabilidades	3	Designar al Líder de Gobierno y Transformación Digital. (conforme el Decreto Supremo Nº 033-2018-PCM y la Resolución de Secretaría de Gobierno Digital N° 004-2018-PCM/SEGDI)	SI	COMPLETADO
	4	Constituir el Comité de Gobierno y Transformación Digital. (conforme la Resolución Ministerial Nº 119-2018-PCM y la Resolución Ministerial Nº 087-2019-PCM)	SI	COMPLETADO
	5	Designar al Oficial de Seguridad y Confianza Digital. (conforme el Decreto Supremo N° 029-2021-PCM, el artículo 5 de la Resolución Ministerial N° 166-2017-PCM y la Resolución de la Secretaría de Gobierno y Transformación Digital N° N° 002-2023-PCM/SGTD)	SI	COMPLETADO
	6	Conformar el Equipo de Respuestas ante Incidentes de Seguridad Digital. (conforme el Decreto de Urgencia N°007-2020 y Decreto Supremo Nº 029-2021-PCM)	SI	COMPLETADO
	7	Designar al Responsable del Software Público. (conforme el Decreto Supremo N° 051-2018-PCM)	SI	COMPLETADO
	8	Designar al Oficial de Datos Personales. conforme el Decreto Supremo N° 29-2021-PCM y la Resolución de Secretaría de Gobierno y Transformación Digital N° 001-2022-PCM/SGTD)	NO	COMPLETADO
	9	Designar al Oficial de Gobierno de Datos. (conforme el Decreto Supremo N° 29-2021-PCM y la Resolución de Secretaría de Gobierno y Transformación Digital N° 001-2022-PCM/SGTD)	NO	COMPLETADO
Gobierno y transformación digital	10	Elaborar el Plan de Gobierno Digital. (conforme la Resolución de Secretaría de Gobierno Digital Nº 005-2018-PCM/SEGDI)	SI	COMPLETADO
	11	Incorporar el sitio web institucional a la Plataforma.GOB.PE[4]	SI	COMPLETADO
	12	Implementar el Modelo de Gestión Documental. (conforme el artículo 8 del Decreto Legislativo N° 1310, la Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI y sus modificatorias)	SI	COMPLETADO
	13	Publicar en la Plataforma Nacional de Datos Abiertos. (conforme el Decreto Legislativo N°1412 Ley de Gobierno Digital y el Decreto Supremo N° 029-2021-PCM)	SI	COMPLETADO
	14	Incorporar información en la Plataforma GeoPerú. (conforme el Decreto Legislativo N°1412 Ley de Gobierno Digital y el Decreto Supremo N° 029-2021-PCM)	SI	COMPLETADO
	15	Implementar el Sistema de Gestión de Seguridad de la Información. (Conforme el Decreto Supremo Nº 029-2021-PCM y la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD)	SI	EN PROCESO
	16	Formular el Plan de Transición al Protocolo IPV6. (conforme el Decreto Supremo Nº 081-2017- PCM)	SI	COMPLETADO
	17	Implementar la Mesa de Partes Digital. (conforme el Decreto Supremo N° 205-2020-PCM)	SI	COMPLETADO
	18	Publicar el TUPA de la entidad en Gob.pe (conforme el Decreto Supremo N° 033-2018-PCM y el Decreto Legislativo N° 1452 que modifica la Ley N° 27444)	SI	COMPLETADO
	19	Responder la Encuesta Nacional de Activos Digitales. (conforme la Resolución Ministerial N° 310-2013-PCM y el Decreto Supremo Nº 029-2021-PCM)	SI	COMPLETADO
	20	Publicar y consumir los servicios de la PIDE[5]. (conforme el Decreto Supremo Nº 083-2011-PCM y sus complementarios, Decreto Legislativo Nº 1246, Decreto	SI	COMPLETADO

4 Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano.
5 PIDE: Plataforma de Interoperabilidad del Estado.

Ámbito	Nº	Acciones y compromisos	Priorizado por la SGTD	Estado de cumplimiento
		Supremo Nº 051-2017-PCM y Decreto Supremo Nº 067-2017-PCM)		
	21	Solicitar acceso al Portal de Transparencia Estándar de la entidad.	SI	COMPLETADO
	22	Conversión integral de procedimientos administrativos a plataformas o servicios digitales. (conforme la Directiva N° 001-2021-PCM/SGD)	NO	EN PROCESO

Fuente: Elaboración propia

6.2. Gestión de la Seguridad de la Información

Los responsables en la gestión de la seguridad de la información en el OEFA son los siguientes:

a) **El/La Presidente/a del Consejo Directivo (PCD)**, quien como responsable de la implementación del SGSI aprueba la política y objetivos para implementar, operar, mantener y mejorar el SGSI.
Cabe indicar que, a través de Resolución de Presidencia del Consejo Directivo N° 068-2019-OEFA/PCD, modificada por las Resoluciones de Presidencia del Consejo Directivo N° 030-2020-OEFA/PCD y 00048-2022-OEFA/PCD se aprueba la *"Política Integrada del Sistema de Gestión Integrado del Organismo de Evaluación y Fiscalización Ambiental - OEFA"*, la misma que tiene entre sus compromisos:

- Fortalecer el Sistema Nacional de Evaluación y Fiscalización Ambiental (SINEFA).
- Desarrollar acciones de fiscalización eficientes, predecibles y orientadas a resultados, considerando el enfoque preventivo, de priorización de riesgos y responsivo.
- Cumplir con los requisitos legales, de antisoborno, calidad, seguridad de la información u otros aplicables a los Sistemas de Gestión del OEFA.
- Promover la mejora continua del sistema de gestión integrado del OEFA que permita incrementar el cumplimiento de nuestros objetivos institucionales.
- Proteger los activos de información del OEFA de amenazas internas o externas, deliberadas o accidentales, con la finalidad de mantener la continuidad de nuestros servicios a través de la seguridad de la información de los procesos que forman parte del Sistema de Gestión de Seguridad de la Información del OEFA.

b) **El/La Gerente/a General (GEG)** es responsable de informar semestralmente a el/la Titular de la entidad los avances y dificultades en la implementación u operación del SGSI.

c) **El Comité de Gobierno y Transformación Digital (CGTD)** es responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI. Asimismo, a solicitud de el/la PCD o el/la GEG emite opinión y recomendaciones sobre la gestión estratégica del SGSI. Sin perjuicio de lo indicado la entidad puede solicitar opinión a un órgano consultivo vinculado a la gestión de riesgos de la entidad. Conformado mediante la Resolución de Presidencia del Consejo Directivo N° 071-2018-OEFA/PCD y sus modificatorias.

d) **El/La Oficial de Seguridad y Confianza Digital (OSCD)** es responsable de coordinar la implementación, operación, mantenimiento y mejora continua del SGSI en la entidad. Designado/a mediante Resolución de Presidencia del Consejo Directivo N° 00020-2022-OEFA/PCD y sus modificatorias.

e) **El/La Oficial de Datos Personales (ODP),** designado/a mediante la Resolución de Gerencia General N° 020-2021-OEFA/GEG, tiene entre sus funciones velar por el cumplimiento de la aplicación de las medidas de seguridad, conforme a la clasificación de los datos personales que administra el OEFA, así como comunicar y colaborar con la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos ante la identificación de incidentes de seguridad digital que hayan afectado los datos personales en el OEFA.

f) **El Equipo de Respuestas ante Incidentes de Seguridad Digital** es responsable de la gestión de incidentes de seguridad digital que afectan los activos de la entidad. Conformado mediante Resolución de Gerencia General N° 00092-2022-OEFA/GEG.

g) **El Equipo SGSI** es responsable de realizar la implementación y mantenimiento del SGSI en la entidad.

h) **El/La Jefe/a de la Oficina de Tecnologías de la Información** es responsable de informar al OSCD todo incidente de seguridad digital crítico que afecte los procesos y servicios que brinda la entidad, de forma inmediata. Asimismo, articula con el OSCD la implementación de controles de seguridad de la información y coordina con el Equipo de Respuestas ante Incidentes de Seguridad Digital la gestión de incidentes de seguridad digital.

i) **El/La Jefe/a de la Oficina de Planeamiento y Presupuesto** es responsable de orientar al OSCD para asegurar una adecuada articulación con los instrumentos de gestión institucional comprendidos en los sistemas administrativos de presupuesto público, planeamiento estratégico, programación multianual y gestión de inversiones, así como; modernización de la gestión pública.

j) **Los dueños de procesos y responsables de las unidades de organización del OEFA** son responsables de la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como también coadyuvar en la gestión de incidentes según corresponda.

En el marco de la implementación del SGSI el OEFA cuenta con los siguientes documentos aprobados:

a) Política Integrada del Sistema de Gestión Integrado del OEFA, aprobada mediante Resolución de Presidencia del Consejo Directivo Nº 068-2019-OEFA/PCD, modificada por las Resoluciones de Presidencia del Consejo Directivo N° 030-2020-OEFA/PCD y 00048-2022-OEFA/PCD.
b) Manual del Sistema de Gestión Integrado del OEFA, aprobado mediante Resolución de Gerencia General N° 044-2019-OEFA/GEG, modificada por las Resoluciones de Gerencia General N° 00063-2020-OEFA/GEG; 061 y 070-2021-OEFA/GEG; 030, 064, 082, 000113-2022-OEFA/GEG; y, 00016, 00036 y 00103-2023-OEFA/GEG.
c) Políticas Específicas de Seguridad de la Información del OEFA, aprobadas mediante Resolución de Gerencia General Nº 051-2020-OEFA/GEG, y modificada por la Resolución de Gerencia General N° 00116-2022-OEFA/GEG.
d) Procedimiento PA0306 *"Gestión de riesgos de seguridad de información"* del Manual de Procedimientos *"Tecnologías de la Información"*, aprobado por la Resolución de Gerencia General N° 075-2019-OEFA/GEG, modificado por las Resoluciones de Gerencia General números 051-2021-OEFA/GEG y 0063-2022-OEFA/GEG.

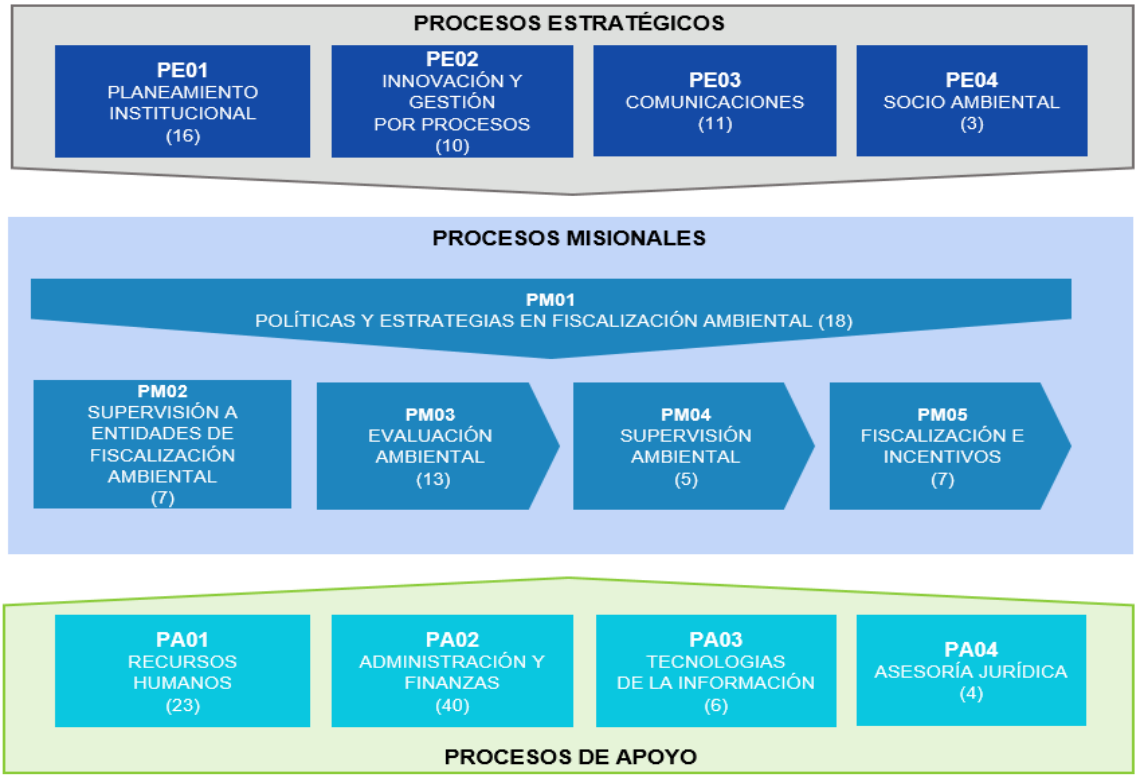
Asimismo, el OEFA mantiene los siguientes documentos:
- Alcance del SGSI aprobado.
- Inventario de activos de información y matrices de riesgos de seguridad de la información de procesos en el alcance del SGSI.
- Declaración de aplicabilidad de controles del SGSI (actualmente conforme al estándar NTP ISO/IEC 27001:2014).

7. MAPA DE PROCESOS

El OEFA mediante la Resolución de Presidencia del Consejo Directivo N° 065-2015-OEFA/PCD, modificada por las Resoluciones de Presidencia del Consejo Directivo números 080-2016-OEFA/PCD y 012-2018-OEFA/PCD, aprueba su Mapa de Procesos, contando con:

- Cuatro (04) procesos estratégicos con cuarenta (40) procedimientos estratégicos.
- Cinco (05) procesos misionales con cincuenta (50) procedimientos misionales.
- Cuatro (04) procesos de apoyo con setenta y tres (73) procedimientos de apoyo.

Imagen N° 1: Mapa de procesos del OEFA



8. ALCANCE DEL SGSI

El alcance inicial del SGSI contempla el proceso misional de **Supervisión Ambiental (PM04)** y dos procedimientos del proceso de apoyo de Tecnologías de la información (**PA0302 Desarrollo y mantenimiento de sistemas de información** y **PA0304 Monitoreo y mantenimiento de la infraestructura de tecnologías de la información**).

Cuadro N° 4: Procesos y procedimientos en el alcance del SGSI - Fase I

Código	Proceso	Procedimiento	Ubicación
PM04	Supervisión Ambiental	Todos	Sede central
PA302	Tecnologías de la información	Desarrollo y mantenimiento de sistemas de información	Sede central

Código	Proceso	Procedimiento	Ubicación
PA304	Tecnologías de la información	Monitoreo y mantenimiento de la infraestructura de tecnologías de la información	Sede central

Posteriormente, los demás procesos misionales se incorporarán en el alcance del SGSI, previo análisis del contexto y disponibilidad de recursos, hasta completar la totalidad de los procesos misionales, de acuerdo al siguiente orden de priorización:

Cuadro N° 5: Procesos en el alcance del SGSI - Fase II

Código	Proceso	Procedimiento	Priorización
PM03	Evaluación Ambiental	Conforme resultado del análisis de contexto y disponibilidad de recursos.	1
PM05	Fiscalización e Incentivos	Conforme resultado del análisis de contexto y disponibilidad de recursos.	1
PM01	Políticas y Estrategias en Fiscalización Ambiental	Conforme resultado del análisis de contexto y disponibilidad de recursos.	2
PM02	Supervisión a Entidades de Fiscalización Ambiental	Conforme resultado del análisis de contexto y disponibilidad de recursos.	2

9. CRONOGRAMA DE ACTIVIDADES

En el Anexo N° 1 se detalla el cronograma de actividades con su respectiva programación y responsables de ejecución.

10. RECURSOS Y PRESUPUESTO

El desarrollo de actividades del Plan SGSI abarca los siguientes recursos:

a) Personal:

- Oficial de Seguridad y Confianza Digital.
- Equipo SGSI.

b) Presupuesto:

El presupuesto contempla el personal dedicado al desarrollo y seguimiento del Plan SGSI, así como las contrataciones de servicios necesarios para garantizar la implementación y mantenimiento de los controles del SGSI, el cual está comprendido en el presupuesto de la OTI, en la actividad operativa "*Implementación de proyectos de tecnologías de la información y comunicación"* con la Tarea "Gestión de Infraestructura y Servicios de TI" del POI Anual 2024 Consistente con el PIA.

En el caso del presupuesto de la/s auditoría/s externa/s de certificación, ampliación de alcance y/o mantenimiento del SGSI corresponde a la OPP, en coordinación con la OTI.

A continuación, se precisa el presupuesto del Plan SGSI:

Cuadro N° 6: Presupuesto del Plan SGSI

Ítems	2024	2025
Personal y obligaciones sociales (Oficial de Seguridad y Confianza Digital)	S/. 96,768.00	S/. 96,768.00
Servicios para implementación del SGSI (consultorías / auditoría interna)	S/. 0.00	S/. 24,000.00
Servicios para la operación del SGSI (análisis de vulnerabilidades, antivirus, custodia de backups, mantenimientos de equipos del centro de datos)	S/. 54,972.45	S/. 92,572.45
Servicios (auditoría externa de certificación, mantenimiento y/o ampliación del alcance)	S/. 22,800.00	S/. 37,000.00
Total	**S/. 174,540.45**	**S/. 250,340.45**

11. MONITOREO Y EVALUACIÓN

A continuación, se detallan las acciones que se realizarán para el seguimiento, monitoreo y evaluación del cumplimiento de los objetivos del Plan SGSI:

- El/La Oficial de Seguridad y Confianza Digital realizará el seguimiento de las actividades planificadas en el cronograma de actividades detalladas en el Anexo 1, e informará de manera trimestral a la Gerencia General el avance, logros, gestión de recursos y/o dificultades en la implementación u operación del SGSI.

- La Gerencia General informará semestralmente a la Presidencia del Consejo Directivo del OEFA el estado del Plan SGSI, así como las dificultades en la implementación u operación del SGSI.

12. ANEXOS

Anexo 1: Cronograma de actividades del Plan SGSI.

Organismo de Evaluación y Fiscalización Ambiental

Anexo 1 - Cronograma de actividades del Plan SGSI

Planificación de actividades							2024											2025										
Fase	N°	Actividad	Medio de prueba	Responsable	Fecha Inicio	Fecha Fin	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
Fase I	1	Planear la implementación del SGSI alcance inicial			22/1/2024	23/4/2024																							
	1.1.	Realizar análisis de brechas del SGSI conforme la NTP ISO/IEC 27001:2022.	Informe	OSCD	22/1/2024	29/1/2024	1																						
	1.2.	1. Evaluar los procedimientos de OTI, determinar e incorporar los ajustes requeridos conforme la NTP ISO 27001:2022.	Correo	OSCD	22/1/2024	29/1/2024	(*)																						
		2. Realizar la evaluación técnica preliminar de la propuesta de actualización del MAPRO “Tecnologías de la información”	Correo	OPP	30/1/2024	1/2/2024		(*)																					
		3. Realizar la evaluación legal preliminar relacionada a la actualización de procedimientos del MAPRO “Tecnologías de la información”.	Correo	OAJ	2/2/2024	6/2/2024		(*)																					
		4. Revisar actualización del MAPRO “Tecnologías de la información”.	Correo	GEG	7/2/2024	9/2/2024		(*)																					
		5. Presentar informe sustentatorio de la modificación del MAPRO OTI.	Informe	OTI	12/2/2024	14/2/2024		1																					
		6. Sustentar actualización del MAPRO “Tecnologías de la información” al Comité de gestión por procesos.	Acta	OTI	15/2/2024	16/2/2024		1																					
		7. Emitir opinión técnica de la modificación del MAPRO “Tecnologías de la información”.	Informe	OPP	19/2/2024	21/2/2024		1																					
		8. Emitir opinión legal de la modificación del MAPRO “Tecnologías de la información”.	Informe	OAJ	22/2/2024	26/2/2024		1																					
		9. Aprobar resolución de actualización MAPRO “Tecnologías de la información”.	Resolución	GEG	27/2/2024	28/2/2024		1																					
	1.3.	Evaluar los procedimientos de áreas de soporte al SGSI (UAB, URH, UFGD), determinar y proponer los ajustes requeridos conforme la NTP ISO 27001:2022.	Informe	OSCD	30/1/2024	12/2/2024		1																					
	1.4	1. Evaluar, determinar e incorporar ajustes a las políticas específicas del SGSI conforme la NTP ISO 27001:2022.	Correo	OSCD	13/2/2024	21/2/2024		(*)																					
		2. Realizar la evaluación técnica preliminar de la propuesta de actualización de las políticas específicas SGSI.	Correo	OPP	22/2/2024	26/2/2024		(*)																					
		3. Realizar la evaluación legal preliminar de la propuesta de actualización de las políticas específicas SGSI.	Correo	OAJ	27/2/2024	29/2/2024		(*)																					
		4. Revisión preliminar de la propuesta de actualización de las políticas específicas SGSI.	Correo	GEG	1/3/2024	4/3/2024			(*)																				

Organismo de Evaluación y Fiscalización Ambiental

Anexo 1 - Cronograma de actividades del Plan SGSI

Planificación de actividades							2024											2025											
Fase	N°	Actividad	Medio de prueba	Responsable	Fecha Inicio	Fecha Fin	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
		5. Levantamiento de observaciones de la Políticas Específica de SGSI (en coordinación con OPP y OAJ)	Informe	OSCD	5/3/2024	7/3/2024			1																					
		6. Revisión por el Comité de Gobierno y Transformación Digital.	Acta	CGTD	8/3/2024	14/3/2024			1																					
		7. Elaborar y emitir el informe de sustento de la propuesta de actualización de las políticas específicas SGSI y se adiciona el acta de comité con los acuerdos	Informe	OSCD	15/3/2024	18/3/2024			1																					
		8. Emitir técnica de la propuesta de actualización de Políticas Específicas del SGSI.	Informe	OPP	19/3/2024	21/3/2024			1																					
		9. Emitir opinión legal relacionada a la actualización de Políticas Específicas del SGSI.	Informe	OAJ	22/3/2024	26/3/2024			1																					
		10. Aprobar resolución de actualización de Políticas Específicas del SGSI.	Resolución	GEG	27/3/2024	2/4/2024				1																				
	1.5.	1. Gestionar la actualización de la documentación interna del SGSI en el Manual SGI (definiciones, roles y responsabilidades, objetivos, indicadores, estructura organizativa, procedimientos).	Correo	OSCD	19/3/2024	21/3/2024			(*)																					
		2. Realizar la evaluación técnica preliminar del Manual del SGI.	Correo	OPP	22/3/2024	26/3/2024			(*)																					
		3. Realizar la evaluación legal preliminar del Manual del SGI.	Correo	OAJ	27/3/2024	2/4/2024				(*)																				
		4. Realizar revisión al Manual del SGI.	Correo	GEG	3/4/2024	4/4/2024				(*)																				
		5. Levantar las observaciones del Manual del SGI (en conjunto con OPP y OAJ).	Correo	OSCD	5/4/2024	8/4/2024				(*)																				
		6. Elaborar informe de sustento de la propuesta de actualización del Manual del SGI.	Informe	OSCD	9/4/2024	10/4/2024				1																				
		7. Emitir opinión técnica de la propuesta de actualización del Manual del SGI.	Informe	OPP	11/4/2024	15/4/2024				1																				
		8. Emitir opinión legal de la propuesta de actualización del Manual del SGI.	Informe	OAJ	16/4/2024	18/4/2024				1																				
		9. Aprobar los cambios al Manual SGI.	Resolución	GEG	19/4/2024	23/4/2024				1																				
	2	Ejecutar la implementación del SGSI alcance inicial			5/2/2024	31/12/2024																								
	2.1	Desarrollar charlas de concientización en seguridad de la información (fase I).	Reporte de asistencia	OSCD	05/02/2024	30/10/2024		1		1		1		1		1														

Organismo de Evaluación y Fiscalización Ambiental

Anexo 1 - Cronograma de actividades del Plan SGSI

Planificación de actividades							2024											2025											
Fase	N°	Actividad	Medio de prueba	Responsable	Fecha Inicio	Fecha Fin	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
	2.2	Evaluar y actualizar el inventario de activos de información de los procesos del alcance con asistencia del Equipo SGSI.	Inventario de activos de procesos	Dueño del proceso	05/02/2024	16/02/2024		8																					
	2.3	Realizar el análisis, evaluación y definición del plan de tratamiento de riesgos y oportunidades de seguridad de la información en coordinación con el/la OSCD.	Matriz de riesgos y oportunidades	Dueño del proceso	19/02/2024	05/03/2024			8																					
	2.4	Revisar, dar conformidad de la matriz de riesgos y oportunidades (áreas usuarias) y remitir matrices al OSCD.	Matriz de riesgos y oportunidades aprobada	Dueño del proceso	06/03/2024	08/03/2024			8																					
	2.5	Elaborar informe de sustento de matrices de riesgos y oportunidades de seguridad de la información y presentar al CGTD.	Informe	OSCD	11/03/2024	13/03/2024			1																					
	2.6	Validar las matrices de riesgos y oportunidades del SGSI en sesión de CGTD.	Acta	CGTD	14/03/2024	20/03/2024			1																					
	2.7	Implementar o actualizar los controles específicos conforme el Plan de Tratamiento de riesgos (fase I).	Cuadro seguimiento con evidencia	Responsables de implementación	21/03/2024	31/10/2024										1														
	2.8	Realizar seguimiento de la operación del SGSI conforme los controles NTP ISO/IEC 27001:2022 y elaborar informe de seguimiento de las matrices de riesgos y oportunidades de seguridad de la información (fase I).	Informe	OSCD	15/1/2024	31/12/2024			1			1			1			1												
	3	Verificar la implementación del SGSI alcance inicial			15/03/2024	31/12/2024																								
	3.1	Coordinar, analizar y evaluar resultados de la medición de indicadores del SGSI (fase I)	Memorando	OPP	15/03/2024	31/12/2024			1			1			1			1												
	3.2	Realizar la Auditoría Interna del SGSI (alcance inicial).	Informe de auditoría	OTI	29/04/2024	07/05/2024					1																			
	3.3	Realizar la Revisión por la Dirección, respecto del SGSI (por la Alta Dirección del SGI)	Informe / Acta	OSCD / GEG / OPP /	17/06/2024	28/06/2024						1																		
	4	Actuar y realizar mejoras de la implementación del SGSI alcance inicial			08/05/2024	31/12/2024																								

Organismo de Evaluación y Fiscalización Ambiental

Anexo 1 - Cronograma de actividades del Plan SGSI

Planificación de actividades							2024											2025										
Fase	N°	Actividad	Medio de prueba	Responsable	Fecha Inicio	Fecha Fin	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
	4.1	Implementar acciones correctivas y de mejora de la fase I.	Cuadro de seguimiento	Equipo SGSI	08/05/2024	31/12/2024												1												
	5	Certificar el SGSI - alcance inicial			01/07/2024	25/07/2024																								
	5.1	Realizar la Auditoría Externa para la certificación del SGSI (alcance inicial).	Informe de auditoría	OPP / OTI	01/07/2024	25/07/2024							1																	
Fase II	6	Planear la ampliación del alcance del SGSI			03/01/2025	12/02/2025																								
	6.1	Realizar el análisis, evaluación y actualización del contexto del SGSI.	Acta de reunión	Equipo SGSI	03/01/2025	09/01/2025													1											
	6.2	Coordinar, evaluar y elaborar sustento para la ampliación del alcance del SGSI.	Informe	OSCD	10/01/2025	17/01/2025													1											
	6.3	Evaluar, priorizar y dar conformidad a la ampliación del alcance del SGSI	Acta	CGTD	20/01/2025	24/01/2025													1											
	6.4	1. Elaborar informe de sustento para la actualización del Manual del SGI (alcance SGSI).	Informe	OSCD	27/01/2025	29/01/2025													1											
		2. Emitir opinión técnica de la propuesta de actualización del Manual del SGI.	Informe	OPP	30/1/2025	04/02/2025														1										
		3. Emitir opinión legal de la propuesta de actualización del Manual del SGI.	Informe	OAJ	05/02/2025	07/02/2025														1										
		4. Aprobar actualización del Manual SGI.	Resolución	GEG	10/02/2025	12/02/2025														1										
	7	Operar el SGSI en el alcance actualizado			03/02/2025	31/12/2025																								
	7.1	Capacitar al personal de los nuevos procesos en el alcance del SGSI respecto al procedimiento de gestión de riesgos de seguridad de la información.	Acta de reunión	OSCD	03/02/2025	12/02/2025														2										
	7.2	Desarrollar charlas de concientización en seguridad de la información (fase II).	Reporte de asistencia	OSCD	17/02/2025	12/12/2025														1		1		1		1		1		1
	7.3	Identificar, evaluar y/o actualizar el inventario de activos de información de los procesos del alcance SGSI actualizado con asistencia del Equipo SGSI.	Inventario de activos de procesos	Dueño del proceso	13/02/2025	21/02/2025														10										
		Realizar el análisis, evaluación y definición del plan de tratamiento de riesgos y oportunidades de seguridad de la información en coordinación con el/la OSCD.	Matriz de riesgos y oportunidades	Dueño del proceso	24/02/2025	11/03/2025															10									

Organismo de Evaluación y Fiscalización Ambiental

Anexo 1 - Cronograma de actividades del Plan SGSI

Planificación de actividades							2024											2025										
Fase	N°	Actividad	Medio de prueba	Responsable	Fecha Inicio	Fecha Fin	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
		Revisar, dar conformidad de la matriz de riesgos y oportunidades (áreas usuarias) y remitir matrices al OSCD.	Matriz de riesgos y oportunidades aprobada	Dueño del proceso	12/03/2025	14/03/2025															10									
		Elaborar informe de sustento de matrices de riesgos y oportunidades de seguridad de la información y presentar al CGTD.	Informe	OSCD	17/03/2025	21/03/2025															1									
		Revisar y validar las matrices de riesgos y oportunidades del SGSI en sesión de CGTD.	Acta	CGTD	24/03/2025	28/03/2025															1									
		Implementar o actualizar los controles específicos conforme el Plan de Tratamiento de riesgos (fase II).	Cuadro seguimiento con evidencia	Responsables de implementación	01/04/2025	30/09/2025																					1			
	7.4	Realizar seguimiento de la operación del SGSI conforme los controles NTP ISO/IEC 27001:2022 y elaborar informe de seguimiento de las matrices de riesgos y oportunidades de seguridad de la información (fase II).	Informe	OSCD	03/03/2025	30/12/2025															1			1			1			1
	8	Verificar la operación del SGSI conforme el alcance del SGSI actualizado			17/03/2025	31/12/2025																								
	8.1	Coordinar, analizar y evaluar resultados de la medición de indicadores del SGSI	Memorando	OPP	17/03/2025	31/12/2025															1			1			1			1
	8.2	Realizar la Auditoría Interna del SGSI.	Informe	OSCD	20/5/2025	30/05/2025																	1							
	8.3	Realizar la Revisión por la Dirección, respecto del SGSI (por la Alta Dirección del SGI)	Informe / Acta	GEG / OPP	16/06/2025	30/6/2025																		1						
	9	Actuar y realizar mejoras en el alcance del SGSI actualizado			02/06/2025	31/12/2025																								
	9.1	Implementar acciones correctivas y de mejora identificadas en la fase II.	Cuadro de seguimiento	Responsables de implementación	02/06/2025	31/12/2025																								1
	10	Certificar el SGSI en el alcance actualizado			01/07/2025	31/07/2025																								

Organismo de Evaluación y Fiscalización Ambiental

Anexo 1 - Cronograma de actividades del Plan SGSI

Planificación de actividades							2024											2025											
Fase	N°	Actividad	Medio de prueba	Responsable	Fecha Inicio	Fecha Fin	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
	10.1	Realizar la Auditoría Externa de seguimiento y/o ampliación de certificación en el alcance del SGSI aprobado.	Informe de auditoría	OPP	01/07/2025	31/07/2025																			1					

Leyenda:
(*) La cantidad programada para las actividades con medio de prueba "correo" es variable (uno o más correos).