REF.: DEJA SIN EFECTO LA RESOLUCIÓN EXENTA N° 32, DE 2023, QUE APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE OBRAS PÚBLICAS Y APRUEBA POLÍTICA GENERAL DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MINISTERIO DE OBRAS PÚBLICAS (2025)

SUBSECRETARIA OO. PP.
OFICINA DE PARTES
19 DIC 2025
TRAMITADO

Santiago. 19 DIC 2025

Resolución SOP [Ex] Nº: 414

VISTOS:

Lo dispuesto en el DFL N°1/19.653 del 2000, de la Secretaría General de la Presidencia que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, la Ley 19.880 que establece las Bases de los procedimientos Administrativos que rigen los actos de los órganos de la Administración del Estado, las atribuciones que me confiere el DFL MOP N° 850/97, que fija el texto refundido, coordinado y sistematizado de la Ley 15.840 de 1964, la Ley N° 19.628, sobre protección de la vida privada, la Ley N° 21.719, sobre protección y tratamiento de datos personales, la Ley N° 20.285, sobre acceso a la información pública, la Ley N° 21.663, Ley Marco de Ciberseguridad, el Decreto N° 12 de 2025, del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, que aprueba la actualización de la Política Nacional de Inteligencia Artificial, que orienta el desarrollo ético, responsable e inclusivo de esta tecnología, la Resolución Exenta SOP N° 121, de 23 de mayo de 2025 y sus modificaciones, y la Resolución N°36 de 2024, que fija normas sobre exención del trámite de toma de razón de la Contraloría General de la República.

CONSIDERANDO:

1. Que, corresponde al Ministerio de Obras Públicas velar por la correcta administración, gestión, protección y continuidad operativa de los activos de información que soportan el cumplimiento de sus funciones públicas, en conformidad con lo dispuesto en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

2. Que, la Ley N° 19.880 establece la obligación de que los órganos de la Administración ajusten su actuación a procedimientos que garanticen la transparencia, eficiencia y eficacia en el ejercicio de sus potestades, lo que incluye el manejo y la preservación de la información bajo su responsabilidad.

3. Que, en virtud del DFL MOP N° 850/1997, corresponde a esta Cartera la planificación, estudio, proyección, construcción, conservación, explotación y regulación de la infraestructura pública fiscal, funciones que requieren sistemas, plataformas y activos digitales seguros, íntegros y disponibles para asegurar la continuidad del servicio público.

4. Que, la evolución tecnológica, el aumento de amenazas en el ciberespacio y la dictación de nueva normativa, especialmente la Ley N° 21.663, Ley Marco de Ciberseguridad, así como estándares internacionales como NCH-ISO/IEC 27001:2023, exigen actualizar la política institucional de seguridad de la información para adecuarla a los principios, obligaciones y exigencias vigentes.

5. Que, el Ministerio, mediante Resolución Exenta N° 983 de 2021, aprobó la Política General y Específica de Seguridad de la Información, y a través de la Resolución Exenta N° 32, de 2023, se dejó sin efecto parcialmente la Resolución Exenta N° 983 de 2021, en relación al numeral 2° de su parte resolutiva, referida a la Política General de Seguridad de la Información y manteniendo la vigencia de las Políticas Específicas aprobadas mediante la Resolución Exenta N° 983 de 2021.

6. Que, en este contexto, la Política General de Seguridad de la Información requiere ser actualizada a fin de incorporar las nuevas obligaciones regulatorias, los cambios tecnológicos y los lineamientos estratégicos definidos para el período 2023–2026.

7. Que la protección de datos personales, regulada por la Ley N° 19.628 y la Ley N° 21.719, constituye un deber esencial de los órganos de la Administración, razón por la cual se torna necesario reforzar mecanismos de gobernanza, privacidad desde el diseño, gestión del riesgo y seguridad digital.

8. Que, la misión estratégica institucional reconoce la necesidad de fortalecer capacidades en materias de inteligencia artificial, Ciberseguridad, ética algorítmica y gestión de riesgos emergentes, lo cual exige contar con un marco normativo interno actualizado, coherente y transversal.

9. Que, resulta indispensable consolidar un Sistema de Gestión de Seguridad de la Información (SGSI) que asegure confidencialidad, integridad y disponibilidad de la información institucional, bajo principios de mejora continua, gestión de riesgos, cumplimiento normativo y coordinación interinstitucional. De este modo, se debe actualizar la resolución exenta 32, de 2 de febrero de 2023, que contenían las Políticas Generales y Específicas de Seguridad de la Información para el Ministerio de Obras Públicas, mediante este nuevo acto administrativo.

10. Que, por otro lado, se mantendrá vigente parcialmente la Resolución Exenta N° 983, de 2021, en virtud de la necesidad de mantener políticas específicas, basadas en criterios técnicos en materia de Seguridad de la Información, que complementen los criterios generales establecidos mediante el presente acto administrativo.

11. Que, la Subsecretaría de Obras Públicas, ha revisado y aprobado el contenido actualizado de la Política General de Seguridad de la Información y Ciberseguridad, cumpliendo los requisitos técnicos y legales aplicables.

RESUELVO:

I. **APRUÉBESE** la Política General de sistema de Gestión de Seguridad de la Información y Ciberseguridad del Ministerio de Obras Públicas.

II. **DÉJESE SIN EFECTO** la Resolución Exenta N° 32, de 2023, que aprueba la Política General de Seguridad de la Información para el Ministerio de Obras Públicas.

III. **ESTABLECESE** que continúa vigente la Resolución Exenta N° 983, de 2021, solo en relación a las Políticas Específicas de Seguridad de la Información para el Ministerio de Obras Públicas, aprobadas en el numeral 2° de su parte resolutiva, en todo aquello que no contradiga el contenido de la presente resolución y normativa vigente asociada.

Ministerio de Obras Públicas

Gobierno de Chile

POLÍTICA GENERAL DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MINISTERIO DE OBRAS PÚBLICAS

2025

ÍNDICE

1. PRESENTACIÓN

El Ministerio de Obras Públicas es la secretaría de gobierno que está a cargo de planear, estudiar, proyectar, construir, ampliar, reparar, conservar y explotar la infraestructura pública de carácter fiscal, que esté bajo su tuición, a lo largo del país. Entre las obras que tiene a cargo se incluyen caminos, autopistas, puentes, túneles, aeropuertos y aeródromos, además de embalses de riego, defensas fluviales, colectores de agua lluvia y agua potable rural.

En el contexto de la ejecución de estas labores, y considerando que el uso de tecnologías es indispensable para ofrecer un buen servicio, es evidente que los riesgos de filtraciones de información y datos relevantes son cada vez más presentes. Por ello, se hace necesario desarrollar un Sistema General de Seguridad de la Información y Ciberseguridad (SGSI) que establezca lineamientos generales y defina roles clave para actuar tanto de manera reactiva como preventiva.

2. ANTECEDENTES

Actualmente, el Ministerio de Obras Públicas cuenta con una Política General y Específicas de Seguridad de la Información, aprobada por el Comité de Seguridad de la Información, mediante Res. Ex. N°983, con fecha 20 de septiembre de 2021. Sin embargo, debido al tiempo transcurrido y al rápido avance de las tecnologías, así como al surgimiento de nueva normativa en la materia, como la Ley Marco de Ciberseguridad (Ley N°21.663) y la Norma NCH ISO 27001:2023, que en su numeral 5.2 letra b) establece que la Política de Seguridad de la Información debe incluir objetivos de seguridad que se actualicen periódicamente, surge la iniciativa de revisar y actualizar estas políticas.

3. MISIÓN

Dentro de los propósitos del Ministerio de Obras Públicas, establecidos en su Definición Estratégica 2023–2026, se encuentra el de: *"Proveer y gestionar eficiente y eficazmente obras y servicios de infraestructura, así como regular y favorecer la gobernanza de los recursos hídricos que garantice su preservación y disponibilidad; para propiciar con visión de futuro, un desarrollo sostenible, resiliente, inclusivo, participativo y con perspectiva de género, conectando el territorio, cuidando a las personas y mejorando su calidad de vida en armonía con la naturaleza."*

En línea con esta visión de futuro, el Ministerio reconoce la necesidad de fortalecer las capacidades institucionales en tecnologías emergentes, particularmente en inteligencia artificial (IA), ética algorítmica y su aplicación en la gestión de infraestructura pública. Por ello, se promoverá la incorporación progresiva de programas de capacitación dirigidos a funcionarios y funcionarias del MOP, orientados a:

- Comprender los fundamentos técnicos y operativos de la IA y su impacto en la toma de decisiones públicas.
- Aplicar principios de ética algorítmica, transparencia y no discriminación en el diseño, adquisición y uso de sistemas automatizados.
- Evaluar riesgos asociados al uso de IA en obras públicas, incluyendo sesgos, opacidad y afectación de derechos fundamentales.
- Fomentar el uso responsable de tecnologías inteligentes en planificación, mantenimiento predictivo, gestión de recursos hídricos, movilidad y sostenibilidad.

Estas acciones permitirán al MOP avanzar hacia una infraestructura pública más inteligente, segura, ética y centrada en las personas, alineada con los principios de la Ley Marco de Ciberseguridad, la Ley de Protección de Datos Personales y los estándares internacionales de gobernanza digital.

4. DECLARACIÓN MINISTERIAL

El Ministerio de Obras Públicas reconoce la importancia y el valor de la información con respecto al buen y efectivo funcionamiento de la organización. Esta no es sólo crítica para el éxito de la organización, sino clave para su supervivencia a largo plazo. Por esta razón, se establece la presente política que regula el manejo de la información, a través de la implementación de un **SGSI**. Éste preserva la confidencialidad, integridad y disponibilidad (**CID**) de la información mediante la aplicación de un proceso de gestión de riesgos y brinda confianza a las partes interesadas de que los riesgos se gestionan adecuadamente.

El **SGSI** estará completamente integrado en los procesos estratégicos y la estructura de gestión del MOP. Esto significa que la seguridad de la información será una parte fundamental en el diseño de todos los procesos, sistemas de información y controles. Además, la implementación del SGSI se ajustará y escalará según las necesidades internas y externas de la organización. En nuestro compromiso con un Sistema de Gestión de Seguridad de la Información (SGSI) sólido y alineado con las mejores prácticas, estándares internacionales de seguridad de la información, Ciberseguridad y la Ley de Protección de Datos Personales, reconocemos la importancia de anticiparnos a las normativas emergentes, como la Ley Marco de Ciberseguridad. De esta manera, aseguramos una transición ordenada, eficiente y proactiva desde el inicio.

5. MARCO NORMATIVO

5.1. Leyes

- Ley N° 21.663 que aprueba la Ley Marco de Ciberseguridad.
- DFL N° 1-21663 del Ministerio del Interior y Seguridad Pública, que fija planta de personal de directivos de la agencia nacional de Ciberseguridad y regula otras materias a que se refiere el artículo primero transitorio de la ley Nº 21.663.
- Ley N° 20285 sobre Acceso a la Información Pública.
- Ley N° 19628, sobre Protección de la Vida Privada.
- Ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.
- Ley N° 21.459, que Establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
- Ley N° 19799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

5.2. Decretos

- Decreto N° 293, de 2024, del Ministerio del Interior: Aprueba Reglamento para el funcionamiento de la Red de Conectividad Segura del Estado y las obligaciones especiales de los organismos de la administración del Estado.
- Decreto N° 285, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba Reglamento del Procedimiento de Calificación de los Operadores de Importancia Vital de la ley N° 21.663.
- Decreto N° 295, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba reglamento de reporte de incidentes de Ciberseguridad de la ley N° 21.633.
- Decreto N° 275, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba reglamento sobre funcionamiento del Comité Interministerial sobre Ciberseguridad.
- Decreto N° 276, de 2024, del Ministerio del Interior y Seguridad Pública: Aprueba reglamento que establece normas para el funcionamiento del Consejo Multisectorial sobre Ciberseguridad.
- Decreto N° 7, de 2023, del Ministerio Secretaría General de La Presidencia: Establece Norma Técnica de Seguridad de la Información y Ciberseguridad.
- Decreto N° 164, de 2023, del Ministerio Del Interior y Seguridad Pública: Aprueba la Política Nacional de Ciberseguridad 2023-2028.
- Decreto N° 83, de 2017, del Ministerio de Relaciones Exteriores: Convenio sobre ciberdelincuencia.
- Decreto N° 273, de 2022, del Ministerio Del Interior y Seguridad Pública: Establece obligación de reportar incidentes de Ciberseguridad.

- Decreto N° 1, de 2015, del Ministerio Secretaría General De La Presidencia: Aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado.
- Decreto N° 285, de 2024, del Ministerio Del Interior y Seguridad Pública: que aprueba reglamento del procedimiento de calificación de los Operadores de Importancia Vital de la ley N° 21.663.

5.3. Normas de estándares Internacionales

- NCH ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- ISO/IEC 27003
- ISO/CEI 27004
- ISO/IEC 27005

6. ALCANCE

El ámbito de aplicación de esta política comprende al conjunto de personas, naturales o jurídicas y sistemas que conforman el Ministerio de Obras Públicas (MOP), así como también los servicios dependientes y los proveedores externos del MOP, sean personas naturales o jurídicas y que presten servicios en forma permanente o temporal.

La política aplica sobre todos los productos estratégicos y activos de información propios o administrados por externos al MOP, de acuerdo al alcance de inventario de activos de información definidos por cada una de sus direcciones dependientes.

7. OBJETIVO GENERAL

Propender a cumplir la ley y garantizar la resiliencia en el rol de Operador de Importancia Vital (OIV). El objetivo de esta política es implementar un Sistema de Gestión de Seguridad de la Información (SGSI) de manera sistemática y documentada, bajo el liderazgo del Comité de Seguridad de la Información y Ciberseguridad. Este comité tiene la misión de guiar a toda la organización, reconociendo la importancia del papel de cada integrante en el fortalecimiento de la seguridad de la información y Ciberseguridad.

La gestión de este objetivo se realizará de manera transversal, alineándose con el objetivo estratégico ministerial 2024-2026. Esto asegurará que las bases del SGSI estén en consonancia con la visión y misión global del ministerio, permitiendo a cada servicio operar bajo principios comunes de seguridad de la información, innovación, eficiencia, eficacia y mejora continua. Esta alineación facilitará una implementación más rigurosa y homogénea. En particular, los servicios finales de infraestructura tecnológica, soporte tecnológico y las políticas de Ciberseguridad y transformación digital están directamente vinculados con este objetivo estratégico institucional, que busca una gestión eficiente y eficaz. Todo ello se fundamenta en la innovación y mejora continua, con el propósito de generar información oportuna y de calidad en los ámbitos relacionados con la infraestructura y los recursos hídricos.

8. OBJETIVOS ESPECÍFICOS

8.1. Objetivo Específico y Prioritario:

Garantizar la resiliencia operativa y el cabal cumplimiento de las obligaciones y requisitos mínimos establecidos por la Ley N° 21.663, Ley Marco de Ciberseguridad, en razón de la designación de la designación de la direcciones generales y subsecretaría del Ministerio como Operador de Importancia Vital (OIV).

A continuación se enumeran las acciones clave que se derivan de este objetivo específico:

8.1.1. Alineación Regulatoria:

Adoptar y aplicar oportunamente las normas técnicas, protocolos, y directrices que emita la **Agencia Nacional de Ciberseguridad (ANCI)** y el **CSIRT Nacional**.

8.1.2. Reporte Obligatorio:

Establecer e implementar un procedimiento interno que asegure el **reporte inmediato** al CSIRT Nacional de todo incidente de Ciberseguridad que pueda afectar de manera significativa la continuidad del servicio esencial provisto por el Ministerio.

8.1.3. Coordinación y Cooperación:

Mantener canales de comunicación activos y participar en los mecanismos de coordinación y cooperación establecidos por la autoridad (ANCI y CSIRT Nacional) para la gestión y respuesta a incidentes de Ciberseguridad.

8.1.4. Inversión Proporcional:

Asegurar que los recursos, tecnologías y medidas de seguridad implementadas sean **proporcionales** al riesgo inherente y al impacto potencial (vital) de la interrupción del servicio, en cumplimiento del principio de **Racionalidad** de la Ley.

Los sistemas, aplicaciones y tecnologías de la información deben diseñarse e implementarse considerando la seguridad y la privacidad desde el inicio.

8.2. Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI se alinea con otras políticas ministeriales, como la de protección de datos, de varias maneras. Una vez establecido un objetivo general para la Política de un SGSI, se hace necesario fijar los siguientes propósitos concretos:

8.2.1. Enfoque integrado

Propiciar una implementación coherente tanto del SGSI como de las políticas de protección de datos, ya que ambas persiguen el mismo objetivo fundamental: salvaguardar la información y garantizar su confidencialidad, integridad y disponibilidad. Esta coherencia permite un enfoque integral en la gestión de la seguridad de la información.

8.2.2. Políticas y Procedimientos Coordinados

Crear políticas y procedimientos que aborden de manera conjunta la seguridad de la información y la protección de datos, asegurando que ambos aspectos sean considerados y que existan directrices claras para el manejo y tratamiento de información sensible.

8.2.3. Proteger los activos de información clave del negocio

Garantizar la protección de la información crítica, tanto interna como externa, para asegurar la continuidad operativa del ministerio y minimizar los riesgos operativos, legales, reputacionales y financieros asociados.

8.2.4. Protección contra Amenazas Emergentes

Fortalecer la capacidad del Ministerio para detectar, prevenir y responder a amenazas emergentes, como el ransomware, mediante la implementación de tecnologías avanzadas de Ciberseguridad, incluyendo sistemas de detección y respuesta ante amenazas, inteligencia de amenazas, y simulaciones periódicas de ataques.

8.2.5. Fortalecer la confianza de la ciudadanía, socios estratégicos, contratistas y consultores

Implementar medidas de seguridad que respalden nuestro compromiso con la confidencialidad, integridad y disponibilidad de la información, generando un entorno de confianza inclusivo con todos los actores claves, incluidos la ciudadanía y el Estado.

8.2.6. Cumplimiento normativo

Alinear el SGSI con la política de protección de datos, asegurando el cumplimiento de leyes y regulaciones aplicables sobre la gestión de datos personales, incluyendo el Reglamento General de Protección de Datos (RGPD) y otras regulaciones locales. En concordancia con la Ley N.º 19.628 sobre Protección de la Vida Privada y las recomendaciones del Consejo para la Transparencia, el Ministerio de Obras Públicas se compromete a incorporar el principio de protección de datos personales desde el diseño y por defecto en todos sus procesos, sistemas y servicios que involucren tratamiento de datos. Esto implica adoptar medidas técnicas y organizativas que aseguren la confidencialidad, integridad y disponibilidad de los datos personales, así como garantizar el respeto a los derechos de los titulares, tales como el acceso, rectificación, cancelación y oposición. Asimismo, se promoverá la capacitación continua del personal en materia de protección de datos y se establecerán mecanismos de evaluación de impacto y gestión de riesgos específicos para el tratamiento de datos personales, con el fin de prevenir accesos no autorizados, filtraciones o usos indebidos de la información.

8.2.7. Optimizar la eficiencia operativa mediante la innovación segura

Adoptar tecnologías innovadoras y procesos automatizados que mejoren la eficiencia de nuestras operaciones mientras se asegura la seguridad en el ciberespacio, de acuerdo con lo establecido en el artículo 3°, punto 4 de la Ley N° 21.663.

8.2.8. Concienciación y capacitación

Desarrollar iniciativas de concienciación y capacitación continua del personal en prácticas de Ciberseguridad, asegurando que todos los funcionarios/as comprendan sus responsabilidades en la gestión segura de los datos personales y la importancia de implementar prácticas de seguridad efectivas. Fomentar una mentalidad de seguridad en todos los niveles de la organización es fundamental.

8.2.9. Asegurar la capacidad de respuesta ante incidentes de Ciberseguridad

Implementar mecanismos para detectar, gestionar y resolver de manera efectiva cualquier incidente de seguridad, garantizando la continuidad de las operaciones con el menor impacto posible. Esto incluye procesos para la gestión de brechas de información y la notificación de incidentes, en cumplimiento con las regulaciones de protección de datos vigentes.

8.2.10. Evaluación de riesgos conjunta

Integrar procesos de evaluación de riesgos relacionados con la protección de datos, identificando vulnerabilidades y amenazas que puedan afectar la seguridad de la información. Esta evaluación permitirá priorizar medidas de mitigación que aborden tanto la seguridad de la información como la protección de datos, facilitando la alineación con diversas políticas ministeriales.

La alineación del SGSI con la política de protección de datos no sólo asegura un cumplimiento normativo y una gestión de riesgos eficaz, sino que también promueve una cultura organizacional cohesiva en la protección y gestión de la información, fortaleciendo la confianza pública y la reputación ministerial.

8.2.11. MEJORA CONTINUA

La implementación del SGSI deberá propiciar un ciclo de mejora continua que incluya la revisión y actualización de políticas relacionadas con la protección de datos, asegurando que se adapten a los cambios normativos, tecnológicos y operativos. Las políticas son revisadas al menos una vez al año o cada vez que sea necesario, para alinearse con las mejores prácticas, estándares internacionales y cambios en la normativa legal vigente.

9. IMPLEMENTACIÓN DEL SGSI

Para implementar un SGSI se deben llevar a cabo una serie de pasos que deben incluir:

- Una identificación y clasificación de los activos de información de la organización según sus requisitos para la seguridad de la información que van asociados al activo o al tipo de información que manejan.
- Realizar una evaluación de riesgos para la seguridad de la información identificados para cada activo de información.
- Implementar un plan de tratamiento de riesgos de forma ponderada teniendo en cuenta los resultados de la evaluación de riesgos.
- Implementar los controles seleccionados para minimizar los riesgos inaceptables
- Medir los resultados de la implantación de los controles.
- Evaluar la efectividad de los controles implementados asociados a los activos de información.
- Proponer planes de mejora para nuevos activos o riesgos identificados así como para los controles que lo necesiten

Este proceso debe sistematizarse y mantenerse a lo largo del tiempo con el objetivo de mejorar de forma continua la seguridad de la información en el MOP.

10. ROLES Y RESPONSABILIDADES

10.1. Subsecretario/a de Obras Públicas

Al Sr/a. Subsecretario/a de Obras Públicas le corresponde garantizar la idoneidad, adecuación y eficacia continua de gestión y el apoyo a la seguridad de la información de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales establecidos por la normativa vigente.

10.2. Comité de Seguridad de la Información y Ciberseguridad

El Comité de Seguridad de la Información no sólo será responsable de coordinar e impulsar la implementación de los procesos estratégicos vinculados a un Sistema de Gestión de Seguridad de la Información (SGSI) y alineado con las políticas establecidas, sino que sus integrantes, al pertenecer a un comité transversal, también promoverán la seguridad de la información a nivel ministerial y en sus respectivos Servicios. Está integrado por un Presidente del Comité y un Secretario Ejecutivo, además de un representante de cada Dirección y servicio que integra el MOP a nivel central. Cada miembro asumirá la responsabilidad de fomentar la implementación del SGSI.

10.3. Oficial de Cumplimiento de Ciberseguridad (OCC)

El Oficial de Cumplimiento de Ciberseguridad (OCC) establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de administración de seguridad de la información. Las responsabilidades primordiales del Oficial de Cumplimiento de Ciberseguridad (OCC), en su rol de liderazgo del Sistema de Gestión de Seguridad de la Información (SGSI) y del cumplimiento normativo como Operador de Importancia Vital (OIV), **se resumen en las siguientes funciones esenciales**:

- **Gobernanza y Coordinación del SGSI:** Establecer, implementar, mantener y **supervisar la mejora continua** del SGSI en su totalidad, asegurando que los procesos internos se alineen con los estándares internacionales y los objetivos estratégicos del Ministerio.

- **Cumplimiento Legal y Enlace (Ley N° 21.663):** Actuar como **enlace oficial y punto de contacto** con la **Agencia Nacional de Ciberseguridad (ANCI)** y el **CSIRT Nacional**, garantizando el cumplimiento de las directrices y la ejecución del **reporte obligatorio** de incidentes de Ciberseguridad de efecto significativo.

- **Gestión de Riesgos y Resiliencia: Coordinar el proceso integral de gestión de riesgos**, identificando, evaluando y tratando las amenazas a los activos de información, con especial foco en aquellos que comprometan la continuidad y la resiliencia del servicio esencial provisto por el Ministerio como OIV.

- **Comunicación y Autoridad:** Dirigir la comunicación interna y externa relativa al SGSI y a las amenazas, poseyendo la **autoridad funcional** para impulsar las acciones y recursos necesarios para la protección del capital informativo de la Organización.

10.4. Encargados/as de Ciberseguridad de los Servicios MOP

Son los/as responsables de la seguridad informática de su servicio, el cual no podrá ser o depender del responsable de tecnología de la información del Ministerio. Cada Servicio se encarga de su designación, mediante resolución firmada por el Jefe de Servicio o Director Nacional, según corresponda.

10.5. Encargado/a de Ciberseguridad Ministerial

El/la Encargado/a de Ciberseguridad Ministerial diseñará, implementará y elaborará una puesta en conjunto de medidas que permitan proteger la seguridad de la información, la seguridad y libertad de los usuarios del ciberespacio, con la finalidad de promover un ciberespacio libre, abierto, democrático y seguro.

10.6. Subdivisión de Informática y Telecomunicaciones (SDIT)

Es función de la Subdivisión de Informática y Telecomunicaciones (SDIT), planificar, desarrollar, administrar y proveer servicios informáticos y de comunicaciones al Ministerio de Obras Públicas. (Res. Ex N° 2081 / 2019).

10.7. Encargados Administrativos de los Servicios

Cada unidad o departamento de RRHH, de las Direcciones del MOP deben participar en la protección de datos e infraestructura tecnológica. Además, es esencial que informen y cumplan con las normas de seguridad, asegurando que el personal conozca los procedimientos de gestión de información. Fomentar una cultura de seguridad es fundamental para minimizar riesgos.

En resumen, el compromiso compartido con la seguridad de la información es vital para proteger los activos. Cada unidad debe alinearse con las políticas establecidas, fortaleciendo así la postura de Ciberseguridad ante amenazas en el entorno digital.

10.8. Personal MOP

Se debe exigir que todo el personal aplique la seguridad de la información de acuerdo con la política general de seguridad de la información establecida, las políticas y los procedimientos específicos de cada tema de la organización.

11. PRINCIPIOS RECTORES

La Ley N°21.663 establece en su artículo 3°, lo que se conoce como **Principios Rectores**. Para alcanzar los objetivos de esta ley se deberán observar los ocho principios que allí se enumeran. Lo anterior se refiere a la necesidad de seguir, cumplir y respetar los principios establecidos en la legislación. Es decir, se debe tener en cuenta estos principios en su funcionamiento y en la implementación de medidas relacionadas con la Ciberseguridad.

A continuación se listan los principios específicos:

11.1. PE- SGSI-001 Política de Incidentes de Seguridad de Información

Principio de Control de Daños. Busca lograr la identificación, respuesta y gestión de incidentes de seguridad para evitar su escalada y propagación, garantizando una respuesta coordinada ante ciberataques.

11.2. PE-SGSI-002 Política Cumplimiento Normativo

Principio de Cooperación con la Autoridad: Tiene como objeto dar cumplimiento a las normativas aplicables y los requerimientos de cooperación con las autoridades en caso de incidentes de Ciberseguridad.

11.3. PE-SGSI-003 Política Roles y Responsabilidades

Principio de Coordinación: A través del establecimiento de políticas es posible garantizar la "Coordinación", mediante la definición clara de roles y las responsabilidades de cada equipo, garantizando la colaboración entre distintas áreas del Ministerio.

11.4. PE-SGSI-004 Política de Protección contra el Malware

Principio de Seguridad en el Ciberespacio: Implementar controles para proteger los sistemas informáticos contra ciberataques, con especial atención a los grupos vulnerables o los sistemas críticos.

11.5. PE-SGSI-005 Política de de Resiliencia Operacional y Continuidad del Negocio

Principio de Respuesta Responsable: Mediante la elaboración de una política de continuidad del negocio, se asegurará que las medidas de respuesta ante ciberataques sean defensivas y no ofensivas, manteniendo el enfoque en la recuperación.

11.6. PE-SGSI-006 Política Criptográfica

Principio de Seguridad Informática: A través del uso de cifrado para proteger la información en tránsito y en reposo. "

11.7. PE-SGSI-OO7 Política de Gestión de Riesgos y Activos de Seguridad de la Información

Principio de racionalidad: Se debe garantizar que las medidas de seguridad sean proporcionales al nivel de riesgo y al eventual impacto social y económico. La evaluación de riesgos debe utilizar un método que considere el **impacto catastrófico** de la interrupción del servicio esencial y que se adaptará a los **estándares técnicos específicos** que la ANCI emita para los OIV.

11.8. PE-SGSI-008 Política de Seguridad y Privacidad de los Datos Personales

Principio de seguridad y privacidad por defecto y desde el diseño: Es fundamental asegurar que los sistemas estén diseñados para proteger la seguridad y privacidad de los datos personales desde su concepción.

11.9. PE-SGSI-010 Política de Gestión de Inteligencia Artificial

La implementación de sistemas de Inteligencia Artificial en el Ministerio se guiará bajo un enfoque de **uso ético, responsable y centrado en las personas**, asegurando que el desarrollo y adopción de la IA sea compatible con el respeto a los derechos humanos, la probidad administrativa y la seguridad operacional.

11.10. PE-SGSI-011 Política Específica de Cultura Organizacional y Concientización

Esta Política tendrá como propósito central desarrollar una Cultura de Seguridad Digital Transversal en todo el MOP, entendiendo que la Ciberseguridad es una responsabilidad compartida, inherente a cada rol y proceso, y no una función exclusiva de Soporte TI. La implementación rigurosa de esta política garantizará que la defensa de los activos digitales del MOP sea robusta y sostenible, basada en la conciencia, el conocimiento y la acción de todo su capital humano.

12. GLOSARIO DE TÉRMINOS Y DEFINICIONES

La norma ISO/IEC 27000:2018 define los siguientes términos y definiciones como lenguaje común para todos los estándares ISO sobre la seguridad de la información.

Término	**Definición**
Amenaza	Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.
Confidencialidad	Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.
Control	Medida que modifica un riesgo.
Disponibilidad	Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada.
Integridad	Propiedad de la exactitud y la integridad. La integridad de la información se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambio
Riesgo	Efecto de la incertidumbre sobre los objetivos Un efecto es una desviación de lo esperado - positivo o negativo. En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información se pueden expresar como efecto de la incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas aprovechen las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.
Sistema de Gestión de Seguridad de la Información (SGSI)	Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos.
Mejora Continua	Actividad recurrente para mejorar el rendimiento.

IV. **COMUNÍQUESE** la presente Resolución a los jefes de Gabinete de la Sra. Ministra y del Sr. Subsecretario de Obras Públicas, a la Fiscal Nacional MOP, al Director General de Aguas, al Director General de Concesiones de Obras Públicas, al Director General de Obras Públicas y a los demás Jefes de Servicios y Direcciones del Ministerio; a la División de Administración y Secretaría General, División de Desarrollo y Gestión de Personas, Subdivisión de Gestión de Personas, Subdivisión de Abastecimiento, Subdivisión de Planificación y Gestión Financiera, Subdivisión de Bienes y Servicios, Subdivisión de Tecnologías de la Información, a la Unidad Jurídica, todas de la Subsecretaría de Obras Públicas; a la Unidad de Monitoreo y Control de Gestión Ministerial y Unidad de Auditoría Ministerial. Esta comunicación, la efectuará Oficina de Partes mediante correo electrónico a las respectivas jefaturas y Secretarías de las Unidades.

ANÓTESE,

Subsecretario de Obras Públicas

Danilo Núñez Izquierdo
Subsecretario de Obras Públicas

GML/DAL/DQV

V°B°
Jefe
División
Administración
Secretaría
General
SOPs

N° de proceso: **19687519**.