



<b>MINISTERIO DE HACIENDA</b> <b>OFICINA DE PARTES</b>
<b>R E C I B I D O</b>

**DEJA SIN EFECTO RESOLUCIONES EXENTAS N° 2193, de 2016 Y N° 2366, DE 2019, Y APRUEBA POLITICA GENERAL Y ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE OBRAS PÚBLICAS CONFORME SE DETALLA.**

**983**

**SANTIAGO, 20 de septiembre de 2021**

<b>CONTRALORIA GENERAL</b>		
<b>TOMA DE RAZON</b>		
<b>R E C E P C I O N</b>		
DEPART. JURIDICO		
DEPT. T. R. Y REGISTRO		
DEPART. CONTABIL.		
SUB. DEP. C. CENTRAL		
SUB. DEP. E. CUENTAS		
SUB. DEPTO. C. P. Y BIENES NAC.		
DEPART. AUDITORIA		
DEPART. V. O. P. , U. y T.		
SUB. DEPTO. MUNICIP.		
<b>REFRENDACION</b>		
REF. POR \$	_____	
IMPUTAC.	_____	
ANOT. POR \$	_____	
IMPUTAC.	_____	
DEDUC. DTO.	_____	

**VISTO:**

Lo dispuesto en el Decreto con Fuerza de Ley N°1/19.653, de 2000, del Ministerio 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 N°19.880, sobre Bases de los Procedimientos Administrativos que rigen los actos de la Administración del Estado, Decreto Supremo N° 83, de 2005 del Ministerio Secretaría General de la Presidencia; 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 y DFL N°206, de 1960; y la Resolución N° 6, de 2019 de la Contraloría General de la República;

**CONSIDERANDO:**

- 1.- Que, el Ministerio de Obras Públicas y sus servicios dependientes, como integrante de la Administración Pública, se encuentra en el deber de dar adecuado resguardo a los principios y normas en materia de Seguridad de la Información.
- 2.- Que, mediante Resolución Exenta SOP N° 2366, de fecha 18 de diciembre de 2019, se aprobó la actualización de la Política General de Seguridad de la Información del MOP.
- 3.- Que mediante Resolución Exenta SOP N° 2193 de fecha 27 de octubre de 2016, se aprobaron las Políticas Específicas de Seguridad de la Información
- 4.- Que, mediante resolución exenta SOP N° 1271, de 2018, se determinó la nueva conformación del Comité de Seguridad de la Información, sus funciones y organización interna, acto administrativo que fue modificado por la Resolución Exenta ( E ) N° 167, de fecha 16 de febrero de 2021.

5.- Que, en la Resolución Exenta SOP 1271, de 2018, en su resuelvo 2° letra B) se determinaron las funciones del Comité de Seguridad de la Información, y en la letra g) se estableció expresamente que corresponde al Comité "hacer seguimiento respecto del cumplimiento de las Políticas Internas y las responsabilidades en materia de Seguridad de la Información, y proponer las modificaciones que se estimen pertinentes a las políticas internas y las responsabilidades en materia de seguridad de la información.

6.- Que, en cumplimiento de esta función, el Comité de Seguridad de la Información ha procedido a revisar en su sesión de fecha 9 de agosto del presente año, la propuesta de Política General de Seguridad de la Información para el Ministerio de Obras Públicas y las siguientes Políticas Específicas :

1. Política de Gestión de Activos de Información
2. Política de Control de Acceso
3. Política de Seguridad Física y Ambiental
4. Política de Escritorio y pantalla limpios
5. Política de Continuidad de Seguridad de la Información
6. Política de Seguridad de Gestión y Desarrollo de Personas
7. Política de Gestión de Incidentes de Seguridad de la Información
8. Política de Control de Gestión de las Operaciones y las Comunicaciones
9. Política de Cumplimiento Legal
10. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

7.- Que, así revisadas y aprobadas por el Comité de Seguridad de la Información del MOP, conforme a acuerdo adoptado en la sesión indicada en el considerando anterior, aquellas deben ser aprobadas por acto administrativo dictado por esta autoridad.

### **RESUELVO SOP (EXENTO) (E)**

N° \_\_\_\_\_/

**1° DÉJASE SIN EFECTO**, a contar de esta fecha la Resolución Exenta SOP N°2366, de fecha 18 de diciembre de 2019, que aprobó la actualización de la Política General de Seguridad de la Información del Ministerio de Obras Públicas; y la Resolución Exenta SOP N°2193, de fecha 27 de octubre de 2016, que aprobó Políticas Específicas de Seguridad de la Información.

**2° APRÚEBASE**, a contar de esta fecha, la Política General de Seguridad de la Información; y las siguientes Políticas Específicas, todas para Ministerio de Obras Públicas

1. Política de Gestión de Activos de Información
2. Política de Control de Acceso
3. Política de Seguridad Física y Ambiental
4. Política de Escritorio y Pantalla Limpios
5. Política de Continuidad de Seguridad de la Información
6. Política de Seguridad de Gestión y Desarrollo de Personas

7. Política de Gestión de Incidentes de Seguridad de la Información
8. Política de Control de Gestión de las Operaciones y las Comunicaciones
9. Política de Cumplimiento Legal
10. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Cuyos textos íntegros son los que se transcriben a continuación



# **POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

**MINISTERIO DE OBRAS PÚBLICAS**

## TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	5
2. OBJETIVO GENERAL.....	5
3. ALCANCE DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN .....	5
4. ROLES Y RESPONSABILIDADES .....	7
5. LINEAMIENTOS DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN ..	8
6. SANCIONES .....	10
7. REVISIÓN DE LA POLÍTICA.....	10
8. DIFUSIÓN DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN .....	11

## Control de Cambios

Revisión	Versión del Documento	Modificación Realizada	Autor	Fecha del Cambio
Diciembre 2011	1	Creación del Documento	Carlos Guzmán	12-12-2011
Septiembre 2015	2	Actualizada según observaciones de los Servicios MOP	Paul Cook	29-09-2015
Diciembre 2015	3	Actualizada según observaciones de los Servicios MOP	Pedro Alcaide	10-12-2015
Julio 2017	4	Actualización según consideraciones entregadas por la red de Expertos	Mauricio Leiva	12-05-2017
Septiembre 2017	5	Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP	Mauricio Leiva	06-09-2017
Junio 2018	6	Actualización, se modifica título del alcance eliminando las palabras "DE GESTION" además se modifica la Difusión y el Alcance	Mauricio Leiva	14-06-2018
Julio 2018	7	Actualización, se modifica el alcance en forma y se agrega el Dominio según últimos lineamientos enviados por la red de expertos.	Mauricio Leiva	19-07-2018
Julio 2018	8	Actualización, se reemplaza la firma del Oficial de Seguridad de la Información MOP, por el Encargado Transversal de Seguridad de la Información MOP.	Mauricio Leiva	20-07-2018
Julio 2018	9	En reunión de coordinación de con los encargados de PMG de cada servicio se acuerda agregar los dominios de la norma NCh 27001 of 2013- Minuta N° 6.	Pedro Alcaide	20-07-2018
Septiembre 2018	10	Comité de Seguridad de la Información aprueba Política General de Seguridad de la Información en Minuta 1 de Septiembre de 2018. En conjunto la gobernanza u forma de operar del mismo comité.	Pedro Alcaide	27-09-2018
Noviembre 2019	11	Se modifica de acuerdo a la nueva estructura MOP. Se modifica el alcance para la Dirección General de Aguas.	Servicios MOP	05-11-2019
Abril 2021	12	Revisión periódica de 2 años.	Subsecretaría	14-04-2021
Mayo 2021	13	Se agrega rol de Ciberseguridad y sus respectivas funciones	Christian Acosta Verdugo	18-05-2021
Julio 2021	14	Se agregan recomendaciones de la Unidad de Ciberseguridad	Christian Acosta Verdugo	27-07-2021

Agosto 2021	15	Se desagrega proceso estratégico de DCyF, de acuerdo al Formulario A1	Christian Acosta Verdugo	09-08-2021
----------------	----	---	--------------------------------	------------

## 1. INTRODUCCIÓN

La presente Política de Seguridad de la Información establece el marco de referencia a través de la cual el Ministerio de Obras Públicas (MOP) y sus Servicios dependientes, implementarán el Sistema de Seguridad de la Información Ministerial (SSI), fijando así los estándares de seguridad de la información a aplicar para proteger adecuadamente sus activos de información, según lo establecido en la Norma NCh 27001 vigente.

## 2. OBJETIVO GENERAL

Establecer los lineamientos estratégicos institucionales que definen la postura del MOP para implementar el marco de referencia del Sistema de Seguridad de la Información (SSI) Ministerial.

El SSI tiene como finalidad proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información, considerando elementos de procesamiento y toda forma de soporte, almacenamiento, transporte y/o transmisión, sea en formato físico, electrónico, virtual u otro.

## 3. ALCANCE DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Política General de Seguridad de la Información Ministerial es única y será aplicada en todas las Direcciones dependientes del Ministerio de Obras Públicas (MOP). Estas son:

- Subsecretaría de Obras Públicas (SOP)
- Dirección General de Obras Públicas (DGOP)
- Dirección General de Aguas (DGA)
- Dirección General de Concesiones de Obras Públicas (DGC)
- Dirección de Aeropuertos (DAP)
- Dirección de Arquitectura (DARQ)
- Dirección de Contabilidad y Finanzas (DCyF)
- Fiscalía de Obras Públicas (FIS)
- Dirección de Obras Hidráulicas (DOH)
- Dirección de Obras Portuarias (DOP)
- Dirección de Planeamiento (DIRPLAN)
- Dirección de Vialidad (DV)

Esta política es extensible a todo el personal de los servicios dependientes del MOP, sin importar su modalidad de contratación ya sea planta, contrata, código del trabajo u honorario a nivel central y a personas naturales o jurídicas que presten servicios en forma permanente o temporalmente en el MOP.

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

Se identifican los Productos Estratégicos de cada Dirección del MOP en la siguiente tabla:

Servicio	Productos Estratégicos	Procesos
<b>SOP</b>	Sistema Integral de Infraestructura Computacional, Informática y Telecomunicaciones del MOP	1. Aseguramiento de continuidad operacional (Adm. de operaciones TI y Redes). Asociado al producto estratégico de Informática y Telecomunicaciones.
<b>DCyF</b>	Servicio de pagos a personal del Ministerio de Obras Públicas. Servicio de pagos a Contratistas y Proveedores del Ministerio de Obras Públicas	2. Gestión de Servicios Financieros (Pago de Remuneraciones al Personal) 3. Gestión de Servicios Financieros (Contratistas y Proveedores)
<b>DIRPLAN</b>	Gestión de Inversiones MOP	4. Gestión de Inversiones MOP



<b>FISCALIA</b>	Actos Administrativos necesarios para adquirir o regularizar bienes y terrenos necesarios para la construcción y emplazamiento de obras de infraestructura pública.	5. Gestión de Terrenos.
	Asesoría Jurídica	6. Asesoría Jurídica.
<b>DGA</b>	Expedientes resueltos de Derechos de aprovechamiento de aguas	7. Resolución de Solicitudes de Derechos de Aprovechamiento de Aguas
	Sistema Nacional de Información del Agua	8. Obtención de Datos.
	Sistema Nacional de Información del Agua	9. Análisis y procesamiento de datos.
<b>DGOP</b>	Fiscalización de la Gestión de la Contratación de Obras y Consultorías a nivel MOP.	10. Contratación de Obras y Consultorías. 11. Fiscalización de Contratos. 12. Administración del Registro de Contratistas y Consultores MOP.
	Fiscalización de Obras de Infraestructura Pública.	13. Prevención de Riesgos.
<b>DV</b>	1) Infraestructura vial interurbana. 2) Infraestructura vial de integración externa. 3) Infraestructura vial urbana	14. Diseño.
	1) Infraestructura vial interurbana. 2) Infraestructura vial de integración externa. 3) Infraestructura vial urbana	15. Expropiaciones y Gestión de predios.
	1) Infraestructura vial interurbana. 2) Infraestructura vial de integración externa. 3) Infraestructura vial urbana. 4) Mantenimiento y explotación de infraestructura vial.	16. Contrataciones.
<b>DOH</b>	1) Servicios de Infraestructura Hidráulica de Riego. 2) Servicios de Infraestructura Hidráulica de Evacuación y Drenaje de Aguas Lluvias. 3) Servicios de Infraestructura Hidráulica de Control Aluvial y de Manejo de Cauces.	17. Contratación (Seguimiento de Inversiones). Diseño (Diseño y ejecución de proyectos). Gestión de Inversión (Gestión de la contratación de obras y consultorías).
<b>DOP</b>	1) Servicios de Infraestructura Portuaria pesquera artesanal. 2) Servicios de Infraestructura Portuaria de Conectividad. 3) Servicios de Infraestructura Portuaria de Ribera. 4) Servicios de Infraestructura de Mejoramiento de Borde Costero. 5) Conservación de Infraestructura Portuaria y Costera. 6) Servicios de Infraestructura Portuaria para el Turismo y Deportes Náuticos	18. Contratación. 19. Diseño.
<b>DAP</b>	1) Servicios de Infraestructura Aeroportuaria en la Red Primaria. 2) Servicios de Infraestructura Aeroportuaria en la Red Secundaria.	20. Gestión de la Contratación de Obras. 21. Diseño y Ejecución de Proyectos.

	3) Servicios de Infraestructura Aeroportuaria en la Red de Pequeños Aeródromos.	22. Conservación y Explotación de Infraestructura.
<b>DARQ</b>	1) Servicios de Edificación Pública. 2) Servicios de Edificación Pública Patrimonial.	23. Contratación de Obras y Consultorías. 24. Diseño de Ingeniería y/o Arquitectura de Proyectos. 25. Ejecución de Obras.
<b>DGC</b>	1) Servicios de Infraestructura Concesionada de Vialidad Interurbana. 2) Servicios de Infraestructura Concesionada de Vialidad Urbana 3) Servicios de Infraestructura Concesionada Aeroportuaria 4) Servicios de Infraestructura Concesionada Urbana, Productiva y de Edificación Pública	26. Desarrollo y Licitación de Proyectos 27. Construcción de Obras Públicas Concesionadas. 28. Operaciones de Obras Públicas

#### 4. ROLES Y RESPONSABILIDADES

Para cumplir los objetivos de la Política de Seguridad de la Información del MOP se establece una Estructura de Gobernabilidad para su gestión, definiendo sus roles y responsabilidades.

- **Subsecretaria(o) de Obras Públicas**  
Responsable de aprobar la Política General de Gestión de Seguridad de la Información y sus futuras modificaciones con la asesoría del Comité de Seguridad de la Información del MOP.
- **Comité de Seguridad de la Información MOP**
  - Son los representantes de la Jefatura Superior del Servicio, destinados a dar Gobernabilidad a nivel estratégico al sistema de gestión de Seguridad de la Información del MOP.
  - Aprueba las Políticas de Seguridad de la Información
  - Realizar el seguimiento y monitoreo del Sistema de Seguridad de la Información
- **Encargada de Ciberseguridad Ministerial**
  - Advertir las amenazas actuales y potenciales en el ámbito del ciberespacio para la seguridad de las redes, plataformas, programas e infraestructuras informáticas del Ministerio de Obras Públicas, proponiendo las acciones que les parezcan necesarias para mitigar o superar dichos riesgos
  - Asesorar al Jefe de Servicio y a los directivos del Ministerio de Obras Públicas (MOP) en materias de Ciberseguridad (CS)
  - Coordinar con la Subdivisión de Tecnologías de la Información y Telecomunicaciones del Ministerio de Obras Públicas a fin de mantener una correcta comunicación sobre incidentes, actualización de sistemas y herramientas entre otros
- **Encargado(a) de Seguridad de la Información de los Servicios**
  - Corresponde al cargo que cumple la función de supervisar y coordinar el cumplimiento de las Políticas de Seguridad de la Información
  - Asesorar en materia de Seguridad de la Información a las Jefaturas Superiores del Servicio
  - Participar en la Creación y/o Actualización de las Políticas de Seguridad de la Información.
  - El Encargado de Seguridad de la Información de la Subsecretaría es miembro del comité de Seguridad de la Información.
- **Jefatura Superior de Servicio**  
Son responsables de la aplicación de las Políticas de Seguridad de la Información al interior del Servicio, así como del cumplimiento de las mismas por parte de sus funcionarios y/o Personal Externo.
- **Subdivisión de Tecnologías de la Información y Telecomunicaciones (SDIT)**  
Responsable de las adquisiciones, desarrollo y mantenimiento de los sistemas de procesamiento de información, de almacenamiento y transmisión transversales del MOP.

- **Audidores(as).**

Responsables de practicar auditorías sobre el funcionamiento del SSI, en el cumplimiento de las especificaciones, las medidas de seguridad de la información establecidas por esta política, las normas, los procedimientos y prácticas que de ella surjan, debiendo informar ya sea al Ministro(a), Subsecretario(a), o al Comité de Seguridad de la Información o al Jefes(as) de Servicio según corresponda.

Personal independiente del área bajo revisión, con las habilidades y experiencias adecuadas.

- **Usuarios(as) Internos**

Son las personas que usan los activos de información y los sistemas para su procesamiento. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente. Tienen la obligación de reportar todo incidente de seguridad del que tengan conocimiento.

- **Usuarios(as) Externos**

Son personas o empresas a las que se deben condicionar para el manejo adecuado de la información de la organización.

## 5. LINEAMIENTOS DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El MOP a través de sus servicios dependientes se comprometen a gestionar la seguridad de la información como un proceso continuo en el tiempo, manteniendo un único Sistema de Gestión de Seguridad de la Información Ministerial, basado en la Norma Chilena NCh-ISO 27001 vigente y en cumplimiento de las recomendaciones de seguridad contenidas en el Decreto Supremo DS N° 83 de fecha 12 de Enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), el DS N° 93 de fecha 8 de julio del 2006 de MINSEGPRES, y lo establecido en la Política Nacional de Ciberseguridad PNCS 2017-2022, promulgada el 27 de Abril del 2017 y el instructivo presidencial N° 8 del 23 de Octubre de 2018.

El MOP y sus Servicios dependientes declaran la absoluta relevancia de la seguridad de la información para su quehacer diario, comprometiéndose a la protección de los activos de información y su infraestructura de soporte para garantizar un alto nivel de continuidad operativa de los procesos de negocio, contribuyendo así al cumplimiento de su misión y de sus objetivos estratégicos.

Esta Política está alineada con la misión, los valores, los objetivos y productos estratégicos de los servicios del MOP y se encuentra al mismo nivel que dichas declaraciones estratégicas.

El MOP reconoce como activos de información, la documentación, tecnología, infraestructura y personas necesarias para su procesamiento. Los declara activos valiosos que deben ser protegidos con igual atención que el resto de los activos críticos de la institución. Asimismo, se reconoce la Seguridad de la Información como un atributo necesario en los servicios ofrecidos por MOP.

Todo activo de información debe ser protegido de una manera adecuada a sus requerimientos de confidencialidad, integridad y disponibilidad, considerando especialmente los relacionados con los productos estratégicos institucionales y procesos críticos, gestionando sus vulnerabilidades y riesgos asociados.

La información confidencial del MOP no debe quedar disponible a personas o entidades externas, salvo en las situaciones y formas expresamente establecidas en las normas vigentes y con controles que garanticen la protección de la información.

MOP declara su decisión de cumplir con la normativa y legislación vigente en temas de Seguridad de la Información.

Es responsabilidad de todo el personal del MOP, proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información, frente a amenazas internas o externas, deliberadas o accidentales, con el propósito de mantener la continuidad de la provisión de los servicios y productos estratégicos de infraestructura pública destinados al

servicio de la ciudadanía, teniendo la obligación de notificar cualquier actividad o situación que afecte la seguridad de los activos de información.

Es responsabilidad del MOP que los terceros que presten servicios al ministerio, adhieran a las políticas de seguridad de la información y estén considerados en los controles del SSI.

Se debe establecer una estructura de gobernabilidad mediante un comité de seguridad a nivel estratégico, encargados de seguridad, roles de auditoría a nivel táctico y roles a nivel operacional. El Comité Seguridad de la Información tiene la autoridad de definir políticas para la protección de la información y la responsabilidad de velar por la existencia de las medidas de seguridad destinadas a proteger y preservar los activos de información del MOP.

El MOP y sus servicios dependientes, reconocen que es fundamental: el apoyo con recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SSI; el conocimiento, para todo el personal y terceros que trabajen bajo el control de nuestra institución tomen conciencia de: la política general de seguridad de la información; las implicaciones del incumplimiento de los requisitos del SSI, y su contribución a la eficacia del mismo, incluidos los beneficios de una mejora del desempeño de seguridad de la información.

El MOP reconoce que la sensibilización, capacitación y entrenamiento para todo el personal en las materias de Seguridad de la Información, es una tarea prioritaria y permanente, para entender y mantener un adecuado resguardo de los activos de información.

El MOP reconoce la importancia de la segregación de funciones, esto es, separar en áreas distintas las responsabilidades de autorización y registro de transacciones, con el objetivo de evitar la manipulación no autorizada de los activos de información.

Para la implementación, mantención, monitoreo, auditoría, control y mejoramiento continuo en la aplicación y cumplimiento de estos lineamientos institucionales se deben establecer los mecanismos necesarios.

Lo declarado anteriormente, está tratado en cada uno de los dominios de la NCh 27001 vigente:

- a) Políticas de Seguridad de la Información  
Definición de las políticas para la seguridad de la información, lineamientos que deberían ser entregados y publicados para el conocimiento de todos los funcionarios.
- b) Organización de la Seguridad de la Información  
Establecer un marco referencial a nivel directivo para la implementación del sistema de la información para el Ministerio de Obras Públicas.
- c) Seguridad de Gestión y Desarrollo de Personas  
El jefe de Servicio debe asegurar que los funcionarios, personal a honorarios y proveedores externos, conozcan la política y normas, entiendan sus responsabilidades y sean idóneos en los roles para los cuales son considerados, sin dejar de lado la capacitación regular de estos.
- d) Gestión de Activos  
Implementar y mantener una apropiada protección de los activos de información. Todos los activos deben ser inventariados, clasificados y contar con un responsable identificado.
- e) Control de Acceso  
Asegurar que el acceso del usuario sea debidamente autorizado y evitar el acceso no autorizado a los sistemas de información. Se deben establecer procedimientos formales para controlar la asignación y retiro de los derechos de acceso a los sistemas y servicios de información.
- f) Criptografía  
Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticación y/o la integridad de la información.

- g) Seguridad Física y Ambiental  
Prevenir el acceso no autorizado, daño, interferencia, eventos o causas de índole ambiental que afecten negativamente los activos de información.  
Junto a una política de Pantalla y Escritorio Limpios, la que ayuda a reducir el riesgo del acceso a personal no autorizado, la pérdida o daño de la información durante y fuera del horario de trabajo.
- h) Seguridad de las Operaciones  
Asegurar la operación correcta y segura de los medios de procesamiento, almacenamiento y transmisión de los activos de información, a través de la creación de procedimientos y definición de responsabilidades operacionales.
- i) Seguridad en las Comunicaciones  
Garantizar la seguridad de la información en las redes y la protección de los servicios conectados del acceso no autorizado, considerando las responsabilidades y procedimientos para la administración de los equipos en redes, resguardando la confidencialidad e integridad de los datos que se pasan a redes públicas a través de redes inalámbricas.
- j) Adquisición, Desarrollo y Mantención de Sistemas de Información  
Garantizar que la seguridad sea una parte integral de los sistemas de información y se incluya en la etapa de formulación del software, tanto para los sistemas que se desarrollen internamente, como para los que se encargue su elaboración a un proveedor calificado.
- k) Relaciones con los Proveedores  
Acordar los requisitos de seguridad de la información con los proveedores, para mitigar los riesgos asociados al acceso de estos a los activos de la organización, los que se deberían documentar debidamente.
- l) Gestión de Incidentes de Seguridad de la Información  
Asegurar que las vulnerabilidades y eventos que afecten negativamente la seguridad de la información asociados a sistemas, activos de información o procesos de negocio sean comunicados, registrados y gestionados de manera de permitir la adopción de acciones correctivas a tiempo.
- m) Gestión de la Continuidad de Seguridad de la Información.  
Contar con planes de contingencia para contrarrestar las interrupciones en los procesos críticos del negocio de los efectos de fallas significativas o desastres que afecten a los activos de información.
- n) Cumplimiento Legal  
Evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual legal y de cualquier requisito de seguridad a los cuales puede estar sujeto el diseño, operación, uso y gestión de los procesos de negocio y/o activos de información que los apoyan.

## **6. SANCIONES**

El no cumplimiento de la Política de Seguridad y Específicas, será sancionado en conformidad a las disposiciones administrativas internas. Lo anterior, sin perjuicio de la responsabilidad civil o penal que corresponda.

## **7. REVISIÓN DE LA POLÍTICA**

Las directrices y alcances contenidos en esta política son susceptibles de mejorar continuamente, por lo tanto son factibles de someter a modificaciones, actualizaciones y cambios periódicos

tendientes a mantenerla vigente y aplicable de acuerdo con las condiciones en que el MOP se encuentre. Sin perjuicio de lo anterior, se establece que cada dos años, esta política debe ser sometida a revisión y actualización por parte del Comité de Seguridad de la Información.

## **8. DIFUSIÓN DE LA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**


Se informará por medio de correo electrónico la revisión y/o actualización de la presente política, y se publicará en la web institucional del Ministerio de Obras Públicas para su difusión. ([www.mop.cl](http://www.mop.cl))

Las disposiciones relacionadas con las normas y políticas referidas a la Seguridad de la Información serán debidamente controladas en su cumplimiento por los estamentos definidos por el MOP. Cualquier acción que signifique desconocer lo señalado en los puntos anteriores o que afecte la Seguridad de la Información, será considerada como falta grave, y en consecuencia, sancionada como tal.

**2.- ESTABLÉCESE**, que las presentes Políticas serán aplicable a la Subsecretaria de Obras Públicas, a todos las Direcciones Generales, y demás servicios dependientes del Ministerio de Obras Públicas.

**3° COMUNÍQUESE**, la presente Resolución, a los jefes de Gabinete del Sr. Ministro y Subsecretario de Obras Públicas, a la Sra. Fiscal MOP, al Director General Generales de Aguas, al Director General de Concesiones de Obras Públicas; al Director General de Obras Públicas y a los demás Jefes de Servicios del Ministerio; a la División de Administración y Secretaría General de las Subsecretaría de Obras Públicas y Secretarías Regionales Ministeriales de Obras Públicas; a Auditoría Ministerial; a la Unidad de Monitoreo y Control de Gestión Ministerial, a la Unidad Jurídica y Unidad de Ciberseguridad, todas de esta Subsecretaría, e infórmese a través de la Intranet institucional.

**ANÓTESE,**

**Cristóbal Leturia I**  
Subsecretario de Obras Públicas  
MINISTERIO DE OBRAS PÚBLICAS DIRE  
Subsecretaría de Obras Públicas  
2021-09-20 11:34

**SUBSECRETARIO DE OBRAS PÚBLICAS**

