Ministerio de Obras Públicas

Gobierno de Chile

MINISTERIO DE HACIENDA
OFICINA DE PARTES

R E C I B I D O

CONTRALORIA GENERAL
TOMA DE RAZON

R E C E P C I O N

| | | |
|---|---|---|
| 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. | | |
| | | |

REFRENDACION

REF. POR $ _____

IMPUTAC. _____

ANOT. POR $ _____

IMPUTAC. _____

_____

DEDUC.DTO. _____

| | | |
|---|---|---|
| | | |

**DEJA SIN EFECTO RESOLUCIÓNES 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**

**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 Nº 850/97, que fija el texto refundido, coordinado y sistematizado de la Ley 15.840, de 1964 y DFL Nº206, de 1960; y la Resolución Nº 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 Mantención 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 Mantención 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**

**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.<br>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 |
|---|---|---|
| **SOP** | 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. |
| **DCyF** | Servicio de pagos a personal del Ministerio de Obras Públicas.<br><br>Servicio de pagos a Contratistas y Proveedores del Ministerio de Obras Públicas | 2. Gestión de Servicios Financieros (Pago de Remuneraciones al Personal)<br><br>3. Gestión de Servicios Financieros (Contratistas y Proveedores) |
| **DIRPLAN** | Gestión de Inversiones MOP | 4. Gestión de Inversiones MOP |

| | | |
|---|---|---|
| **FISCALIA** | 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. |
| **DGA** | 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. |
| **DGOP** | Fiscalización de la Gestión de la Contratación de Obras y Consultorías a nivel MOP. | 10. Contratación de Obras y Consultorías.<br>11. Fiscalización de Contratos.<br>12. Administración del Registro de Contratistas y Consultores MOP. |
| | Fiscalización de Obras de Infraestructura Pública. | 13. Prevención de Riesgos. |
| **DV** | 1) Infraestructura vial interurbana.<br>2) Infraestructura vial de integración externa.<br>3) Infraestructura vial urbana | 14. Diseño. |
| | 1) Infraestructura vial interurbana.<br>2) Infraestructura vial de integración externa.<br>3) Infraestructura vial urbana | 15. Expropiaciones y Gestión de predios. |
| | 1) Infraestructura vial interurbana.<br>2) Infraestructura vial de integración externa.<br>3) Infraestructura vial urbana.<br>4) Mantenimiento y explotación de infraestructura vial. | 16. Contrataciones. |
| **DOH** | 1) Servicios de Infraestructura Hidráulica de Riego.<br>2) Servicios de Infraestructura Hidráulica de Evacuación y Drenaje de Aguas Lluvias.<br>3) Servicios de Infraestructura Hidráulica de Control Aluvial y de Manejo de Cauces. | 17. Contratación (Seguimiento de Inversiones).<br>Diseño (Diseño y ejecución de proyectos).<br>Gestión de Inversión (Gestión de la contratación de obras y consultorías). |
| **DOP** | 1) Servicios de Infraestructura Portuaria pesquera artesanal.<br>2) Servicios de Infraestructura Portuaria de Conectividad.<br>3) Servicios de Infraestructura Portuaria de Ribera.<br>4) Servicios de Infraestructura de Mejoramiento de Borde Costero.<br>5) Conservación de Infraestructura Portuaria y Costera.<br>6) Servicios de Infraestructura. Portuaria para el Turismo y Deportes Náuticos | 18. Contratación.<br>19. Diseño. |
| **DAP** | 1) Servicios de Infraestructura Aeroportuaria en la Red Primaria.<br>2) Servicios de Infraestructura Aeroportuaria en la Red Secundaria. | 20. Gestión de la Contratación de Obras.<br>21. Diseño y Ejecución de Proyectos. |

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

- **Auditores(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 Nº 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 dela 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)

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.

# POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

## SUBSECRETARÍA DE OBRAS PÚBLICAS

**Comité de Seguridad de la Información**

## TABLA DE CONTENIDOS

**Control de Cambios**

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Septiembre 2012 | 1 | Creación del Documento | Carlos Guzmán | 26-09-2012 |
| Septiembre 2016 | 2 | Actualizada según observaciones de los Servicios MOP | Pedro Alcaide | 08-09-2016 |
| Agosto 2017 | 3 | Actualización de Formato de acuerdo a lo solicitado por la red de expertos 2017 | Pedro Alcaide | 07-08-2017 |
| Septiembre 2017 | 4 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Junio 2018 | 5 | Actualización, se modifica el alcance agregando controles involucrados.<br>Se modifica la difusión de la presente Política | Mauricio Leiva | 14-06-2018 |
| Julio 2018 | 6 | 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 | 7 | 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 | 8 | En reunión de coordinación con los | Pedro Alcaide | 21-11-2018 |

| | | | | |
|---|---|---|---|---|
| | | encargados de PMG SSI de cada Dirección se acuerda agregar los dominios de la norma NCh 27001 of 2013.- Minuta Número 6. | | |
| Noviembre 2018 | 9 | Encargados de PMG SSI de los Servicios MOP cambian estructura de documento a presentar a la Red de Expertos | Servicios MOP | 28-11-2018 |
| Diciembre 2018 | 10 | Revisión final Encargados de Seguridad de la Información de Servicios. | Servicios MOP | 06-12-2018 |
| Noviembre 2019 | 11 | Se actualiza de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 06-11-2019 |
| Abril 2021 | 12 | Actualización y adecuación a nueva estructura Comité de Seguridad, se ajusta formato de firmas | Pedro Alcaide | 14-04-2021 |
| Mayo 2021 | 13 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta | 18-05-2021 |
| Julio 2021 | 14 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta | 27-07-2021 |

## 1. INTRODUCCIÓN

El presente documento, se enmarca en la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP), las recomendaciones de seguridad indicadas en el Decreto Supremo DS Nº 83 de fecha 12 de enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), Ley de Transparencia 20.285 del 11 de agosto del 2008, DS N°577 del 11 octubre de 1978 y la normativa vigente NCh-ISO 27001:2013. Además se define el objetivo y alcance de la Política de Gestión de Activos de Información, para un adecuado resguardo de ellos, asociados a los procesos de negocio, a efecto de que permita asegurar la continuidad operacional del MOP y sus Servicios dependientes.

## 2. OBJETIVO GENERAL

Asegurar que los activos de información del MOP sean resguardados, inventariados y clasificados adecuadamente, según su nivel de criticidad en términos de disponibilidad, integridad y confidencialidad. Además para la administración de los activos de Información, el uso del equipamiento institucional, y servicios computacionales provistos a través de la plataforma tecnológica de apoyo al cumplimiento de la gestión, en consistencia con los principios rectores de la política general de seguridad de la información

.

## 3. ALCANCE

Los activos de información que dan soporte a los productos estratégicos del MOP, detallados en la Política General de Seguridad de la Información.

Esta Política actúa sobre el ámbito del **dominio A.8 “Administración de Activos”, los controles A.8.1.1 y A.8.1.2**, de la **norma Nch-ISO 27001:2013.**

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información**

- 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.

- Es miembro del Comité de Seguridad de la Información

**Comité de Seguridad de la Información**

- 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

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer, cumplir la política de seguridad de la información vigente.

## 5. DEFINICIONES

### Activos

Debe entenderse que los Activos de Información, son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución, cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten, tales como: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional, entre otros

### Responsabilidad sobre Activos

La información que se produce, procesa, transmite, almacena y los medios físicos utilizados por el ministerio y sus empleados, es de propiedad de la institución y su custodia y protección será de responsabilidad del dueño del proceso que se vincule con dicha información. Con relación a los datos contenidos en medios administrados por la Subdivisión de Tecnología de la Información y Telecomunicaciones (SDIT), esta

unidad estará a su cargo y resguardo. Sin embargo, los accesos y usabilidad de la información, en las Unidades usuarias, son de responsabilidad de los dueños de los procesos y trabajadores que la acceden, los que deberán quedar formalmente establecidos en documentos de control de proyectos.

Inventario de activos: Todos los activos TI deben estar claramente identificados, confeccionando y manteniendo un inventario actualizado.

La información y campos que debe contener este inventario son:

- Código (Id) del activo: en el caso de ser un activo inventariable, identificar el código asignado por el departamento de Administración.
- Nombre del activo: Nombre operativo o comercial del activo.
- Tipo de activo: clasificación del activo, los utilizados son: software, sistema, equipos, documento, infraestructura, formulario, base de datos, y otros.
- Ubicación: identificación del lugar físico que aloja al activo o lógico, en caso de ser un software, sistema y/o base de datos.
- Fecha de creación: Fecha con el cual el activo fue creado o recibido.
- Definición de propietario.

Uso aceptable de los activos: Todo Activo TI ya sea hardware o software que se autorice su acceso y uso, deberá ser utilizado solo en actividades atingentes al MOP.

Devolución de activos: Todos los empleados y usuarios de terceras partes deberá devolver todos los activos de la organización que estén en su posesión / responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.

.

## 6. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional.

# POLÍTICA DE CONTROL DE ACCESO

## SUBSECRETARIA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

**Control de Cambios**

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Agosto 2012 | 1 | Creación del Documento | Carlos Guzmán | 17-08-2012 |
| Mayo 2016 | 2 | Actualizada según observaciones de los Servicios MOP | Pedro Alcaide | 09-05-2016 |
| Agosto 2017 | 3 | Actualización de Formato de acuerdo a lo solicitado por la red de expertos 2017 | Pedro Alcaide | 07-08-2017 |
| Septiembre 2017 | 4 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Junio 2018 | 5 | Actualización, se modifica la Difusión de la presente Política | Mauricio Leiva | 14-06-2018 |
| Julio 2018 | 6 | Actualización, se modifica el alcance en forma y se agrega el Dominio según últimos lineamientos enviados por la red de expertos. | Mauricio Leiva | 17-07-2018 |
| Julio 2018 | 7 | 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 | 8 | En reunión de coordinación con los encargados de PMG SSI de cada Dirección se acuerda agregar los dominios de la norma NCh 27001 of 2013.- Minuta Número 6. | Pedro Alcaide | 21-11-2018 |
| Noviembre 2018 | 8.5 | Encargados de PMG SSI de los Servicios MOP cambian estructura de documento a presentar a la Red de Expertos | Servicios MOP | 28-11-2018 |
| Diciembre 2018 | 9 | Revisión final Encargados de Seguridad de la Información de los servicios. | Servicios MOP | 06-12-2018 |

| | | | | |
|---|---|---|---|---|
| Noviembre 2019 | 10 | Revisión Política, se modifica de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 06-11-2019 |
| Abril 2021 | 11 | Actualización y adecuación de estructura para la SOP. Revisión de cambios realizados para estructura de SOP | Pedro Alcaide | 14-04-2021 |
| Mayo 2021 | 12 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta | 18-05-2021 |
| Julio 2021 | 13 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta | 27-07-2021 |

## 1. INTRODUCCIÓN

El presente documento, se enmarca en la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP), las recomendaciones de seguridad indicadas en el Decreto Supremo DS Nº 83 de fecha 12 de enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), Ley de Transparencia 20.285 del 11 de agosto del 2008 y la normativa vigente NCh-ISO 27001:2013. Además, se define objetivo y alcance de la Política de Control de Acceso a los activos de información del MOP, tales como sistemas, aplicaciones y servicios de tecnologías de información (TI).

## 2. OBJETIVO

Controlar el acceso por medio de un Sistema de Restricciones y Excepciones a la información como base de todo sistema Informático, así como también aquellas áreas que contengan Activos de Información. Restringir el acceso en cualquiera de sus formas (Plataformas, Bases de datos, Dominio Activo, etc.), y a las instalaciones de procesamiento de información (Salas donde residen equipos servidores, plataformas y Bases de Datos). Con el objeto de resguardar su disponibilidad, confidencialidad e integridad

## 3. ALCANCE

Evitar el acceso sin autorización a las áreas en las que se encuentran los dispositivos de proceso y almacenamiento de información, tales como sistemas, aplicaciones, bases de datos y servicios de tecnología de información (TI), de acuerdo al alcance de procesos críticos definidos para cada Servicio, en la Política General de Seguridad del MOP.

Esta Política actúa sobre todos los controles contenidos en el dominio Control de Acceso A.09, controles A.09.01.01, A.09.1.2 y A.09.4.3 de la norma Nch-ISO 27001 de 2013.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del comité de Seguridad de la Información.

**Comité de Seguridad de la Información**

- Son los representantes de la Subsecretaria, destinados a dar Gobernabilidad a nivel estratégico al sistema de gestión de Seguridad de la Información.
- 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

**Subdivisión de Tecnologías de la Información y Telecomunicaciones**

- Definir e implementar estándares de seguridad para acceder a las plataformas tecnológicas (sistemas de información, servicios de red, correo institucional, etc) de propiedad Ministerial, velando por el cumplimiento de la normativa vigente.

**Propietarios o responsables de los sistemas de información**

- Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer, cumplir la política de seguridad de la información vigente.

## 5. DEFINICIONES

**Requisitos de negocio para el control de acceso**

Control de acceso a las redes y servicios asociados: Se deberá proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

Utilización de los Servicios de Red:

- El acceso a los servicios TI y/o recursos de red transversales, deberá ser solicitado al Jefe(a) de la Subdivisión de Tecnologías de la Información y

Telecomunicaciones, quien aprobará, o rechazará justificadamente dicha solicitud, si se compromete la seguridad de la información a nivel Institucional.
- Se deberán implementar controles y procedimientos para proteger el acceso servicios TI y/o recursos de red transversales.

A continuación, se establecen algunos controles que se deben implementar para controlar el acceso a las aplicaciones vía red:

- La ruta de acceso, a través de la red, a los sistemas de información debe ser única.
- Los equipos o sistemas que controlan y fuerzan el acceso a nivel de red (servidores DNS, Proxy, Gateway, Enrutadores, Cortafuegos u otras soluciones tecnológicas), deben contar con controles de seguridad.
- Restringir el acceso de la red, implementado segmentación de redes, redes privadas u otros procedimientos para separar en forma segura dominios de red, jerarquizados.

**Gestión de acceso de usuario**

Gestión de altas/bajas en el registro de usuarios: Deberá existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

Gestión de los derechos de acceso asignados a usuarios: Se deberá de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales deberá ser restringido y controlado.

En la creación de las cuentas de administración de la plataforma tecnológica, deben tenerse presentes las siguientes consideraciones, además de las ya enunciadas en esta política:

- Debe estar declarado formalmente, al Encargado de Seguridad de la Información de la SOP, la justificación, el alcance y objetivos de dichas cuentas.
- Estas cuentas y claves de acceso especiales deben ser resguardadas de forma que, en caso de requerirse, el Encargado de Seguridad de la Información deberá tener acceso a ellas.
- Cada contraseña de administración y operación de sistemas se renovará cada 60 días o cuando se presuma que se ha filtrado a personas no autorizadas.
- Los usuarios Administradores deben tener una cuenta especial con los privilegios de administración, esta cuenta debe ser distinta a la que utiliza para acceder a la red como usuario (dominio, correo, intranet, mesa de ayuda etc.)

Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación deberá ser controlada mediante un proceso de gestión controlado.

Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberán revisar con regularidad los derechos de acceso de los usuarios.

Retirada o adaptación de los derechos de acceso: Se deberán retirar los derechos de acceso para todos los empleados, contratistas, a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

Equipos desatendidos en áreas de usuarios: Se entiende como equipos desatendidos a aquellos que prestan un servicio tal como servidor de archivos, servidores de impresión o repositorio de documentos digitales que no residen en el Datacenter Institucional, tales como: aquellos situados al interior de una oficina en particular, o dispuestos en zonas de acceso público.

En la eventualidad de que se requiera implementar un equipo en la modalidad desatendido, deberá ser solicitada su autorización al Jefe(a) de la Subdivisión de Tecnologías de la Información y Telecomunicaciones

**Responsabilidad del usuario**

Uso de información confidencial para la autenticación: Se deberá exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.

Todos los usuarios de sistemas de información, independiente de su rol o perfil de acceso, deben tener un identificador único (ID de usuario), a través del cual se conectan y emplean los sistemas y/o aplicaciones a las que han sido autorizados.

Si se utilizará un método de autenticación físico tales como: autenticadores de hardware; tarjetas electrónicas; Token u otros, deberá implementarse un procedimiento de acuerdo a lo establecido en la Política de Recursos Humanos, que incluya al menos:

- Registrar la asignación de herramienta de autenticación.
- Recuperar el autenticador al momento de la desvinculación del personal al que se le otorgó.
- Caducar el acceso del autenticador, en caso de riesgos de seguridad.

Los sistemas y aplicaciones que requieren control de acceso deben contar con procedimientos para solicitar y otorgar el acceso requerido, que identifique aspectos tales como vigencia, privilegios.

**Control de acceso a sistemas y aplicaciones**

Restricción del acceso a la información: Se deberá restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

Servicios de interoperación electrónica con entidades externas

Las conexiones externas o acceso remoto a los sistemas de información o conexiones entre sistemas de información del MOP y otros organismos externos (públicos o privados) deberán ser autorizadas por el Encargado de Seguridad de la Información SOP. Además, deben ser respaldadas por un Convenio de interoperación o colaboración que establezca con claridad el alcance, objetivos y responsabilidades en la transmisión/recepción de datos y de su integridad, disponibilidad.

Desde el punto de vista técnico, esta comunicación deberá implementarse teniendo presente los siguientes aspectos:

- Privilegiar el uso e implementación de canales de comunicación privados (enlaces directos).
- De no ser posible lo anterior, se deben establecer mecanismos de interoperación vía internet, empleando procedimientos de autenticación encriptados.
- La exposición de servicios de interoperación vía internet debe emplear certificados de autenticación en ambos lados de la comunicación.
- Debe contar con procedimientos de control de errores en la comunicación (CRC u otros).
- Debe contar con registro (log) de la data transmitida/recibida que permitan determinar posibles errores.

Se debe además contemplar la firma de un documento de confidencialidad de la información y de los datos a los cuales se les da derecho de acceso.

Procedimientos seguros de inicio de sesión: Cuando sea requerido, se deberá controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on

Gestión de contraseñas de usuario: Los sistemas de gestión de contraseñas deberán ser interactivos y asegurar contraseñas de calidad.

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes aspectos:

- Implementar procedimientos para entregar contraseñas provisorias y que obliguen a los usuarios a cambiarlas cuando se otorgan por primera vez.
- Implementar procedimientos para recuperación segura de contraseñas, cuando estas son olvidadas por los usuarios.
- Almacenar las contraseñas implementando procedimientos que aseguren su resguardo y confidencialidad.

Uso de herramientas de administración de sistemas: El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberán estar restringidos y estrechamente controlados.

En la utilización de herramientas de apoyo para la administración de plataforma tecnológica, o de soporte final a usuarios debe tenerse presente los siguientes aspectos:

- Utilizar procedimientos de autenticación para utilitarios o herramientas para administrar la plataforma tecnológica o sistemas de información.
- Establecer autorizaciones para uso de utilitarios de sistema.

Control de acceso al código fuente de los programas: Se debe restringir el acceso al código fuente de las aplicaciones software.

## 6. PERIODICIDAD DE EVALUACION Y REVISIÓN

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 particulares de la MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora.

El Comité de Seguridad de la Información SOP determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN

Se difundirá por medio de correo electrónico la presente Política, la que además se encontrará publicada en la Intranet Institucional.

# POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

## SUBSECRETARÍA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

**Control de Cambios**

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Octubre 2012 | 1.00 | Creación del Documento | Carlos Guzmán | 02-10-2012 |
| Septiembre 2016 | 2.00 | Actualizada según observaciones de los Servicios MOP | Pedro Alcaide | 08-09-2016 |
| Agosto 2017 | 3.00 | Actualización de Formato de acuerdo a lo solicitado por la red de expertos 2017 | Pedro Alcaide | 07-08-2017 |
| Septiembre 2017 | 4.00 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Junio 2018 | 5.00 | Actualización, se modifica la difusión de la presente Política. | Mauricio Leiva | 14-06-2018 |
| Julio 2018 | 6.00 | Actualización, se modifica el alcance en forma y se agrega el Dominio según últimos lineamientos enviados por la red de expertos. | Mauricio Leiva | 17-07-2018 |
| Julio 2018 | 6.09 | 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 | 7.00 | En reunión de coordinación con los encargados de PMG SSI de cada Dirección se acuerda agregar los dominios de la norma NCh 27001 of 2013.- Minuta Número 6. | Pedro Alcaide | 21-11-2018 |
| Noviembre 2018 | 7.01 | Encargados de PMG SSI de los Servicios MOP cambian estructura de documento a presentar a la Red de Expertos | Servicios MOP | 30-11-2018 |
| Diciembre 2018 | 7.02 | Revisión final Encargados de Seguridad de la Información de los servicios | Servicios MOP | 06-12-2018 |
| Noviembre 2019 | 8.0 | Se actualiza de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 06-11-2019 |

| | | | | |
|---|---|---|---|---|
| Abril 2021 | 9.0 | Actualización y adecuación a nueva estructura Comité de Seguridad, se ajusta formato de firmas | Christian Acosta Verdugo | 14-04-2021 |
| Mayo 2021 | 10.0 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta Verdugo | 18-05-2021 |
| Julio 2021 | 11.0 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta | 27-07-2021 |

## 1. INTRODUCCIÓN

El presente documento, se enmarca dentro de la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP), las recomendaciones de seguridad indicadas en el Decreto Supremo DS Nº 83 de fecha 12 de Enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), Ley de Transparencia 20.285 del 11 de Agosto del 2008 y la normativa vigente NCh-ISO 27001:2013. Además se define objetivo y alcance de la Política de Seguridad Física y Ambiental para un adecuado resguardo de los activos de información.

## 2. OBJETIVO

El objetivo es evitar el acceso físico no autorizado, los daños físicos e interferencias a los medios de almacenamiento físicos de información de la organización y las instalaciones de procesamiento de la información. El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

Establecer las directrices de seguridad física y ambiental para facilitar la implementación de controles de protección de las instalaciones de procesamiento de información de la organización, contra accesos físicos no autorizados.

## 3. ALCANCE

Están dentro del alcance de esta Política todas las instalaciones del MOP, incluyendo edificios, bodegas, lugares de acopio, instalaciones de faenas, infraestructura de proveedores externos y otros lugares donde se almacene, procese o mantenga activos de información, que dan soporte a los productos estratégicos, de acuerdo al alcance definido por cada Dirección dependiente del MOP.

Esta Política actúa sobre los controles contenidos en el dominio **“Seguridad Física y del Ambiente” A.11, el control A.11.1.1** de la Nch-ISO 27001.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del Comité de Seguridad de la Información

**Comité de Seguridad de la Información**

- 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

**Subdivisión de Tecnologías de la Información y Telecomunicaciones.**

- Definir e implementar estándares seguros para acceder a las plataformas tecnológicas (sistemas de información, servicios de red, correo institucional, etc) de propiedad Ministerial, velando por el cumplimiento de la normativa vigente.

**Departamento de Seguridad Física SOP**

- Definir e implementar estándares seguros para acceder a Instalaciones Ministeriales de uso común de los Servicios, velando por el cumplimiento de la normativa vigente.

**Propietarios o responsables de los sistemas de información**

- Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer, cumplir la Política de seguridad de la información vigente.

## 5. DEFINICIONES

**Áreas seguras**

Perímetro de seguridad física: Se deberá definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.

Controles de acceso físico: Las áreas seguras deberán estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado cuenta con permiso de acceso.

Seguridad de oficinas, salas e instalaciones: Se deberá diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.

Protección contra amenazas externas y del ambiente: Seguridad de la Información deberá diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

Trabajo en áreas seguras: Se deberán diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.

Áreas de entrega y carga: Se deberán controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.

**Equipamiento**

Ubicación y protección del equipamiento: Los equipos se deberán emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.

Elementos de soporte: Los equipos deberán estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.

Seguridad en el cableado: Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberán proteger contra la intercepción, interferencia o posibles daños.

Mantenimiento del equipamiento: Los equipos deberán mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

Retiro de activos: Los equipos, la información o el software no se deberán retirar del sitio sin previa autorización.

Seguridad del equipamiento y los activos fuera de las instalaciones: Se deberá aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.

Seguridad en la reutilización o descarte de equipos: Se deberán verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

Equipo de usuario desatendido: Los usuarios deberán asegurar de que los equipos no supervisados cuentan con la protección adecuada.

Política de escritorio y pantalla limpios: Se deberá adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

## 6. PERIODICIDAD DE EVALUACION Y REVISIÓN

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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años, al menos, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN DE LA POLÍTICA

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional.

# POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

## SUBSECETARÍA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

## Control de Cambios

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Agosto 2012 | 1.0 | Creación del Documento | Carlos Guzmán | 17-08-2012 |
| Mayo 2016 | 2.0 | Actualizada según observaciones de los Servicios MOP | Pedro Alcaide | 09-05-2016 |
| Agosto 2017 | 3.0 | Actualización de Formato de acuerdo a lo solicitado por la red de expertos 2017 | Pedro Alcaide | 07-08-2017 |
| Septiembre 2017 | 4.0 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Junio 2018 | 5.0 | Actualización, se modifica la Difusión de la presente Política | Mauricio Leiva | 14-06-2018 |
| Julio 2018 | 6.0 | 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 | 7.0 | 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 | 7.1 | En reunión de coordinación con los encargados de PMG SSI de cada Dirección se acuerda agregar los dominios de la norma NCh 27001 of 2013.- Minuta Número 6. | Pedro Alcaide | 21-11-2018 |
| Noviembre 2018 | 8.0 | Encargados de PMG SSI de los Servicios MOP cambian estructura de documento a presentar a la Red de Expertos | Servicios MOP | 28-11-2018 |
| Diciembre 2018 | 9.0 | Revisión final Encargados de Seguridad de la Información de Servicios | Servicios MOP | 06-12-2018 |
| Noviembre 2019 | 10 | Se actualiza de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 06-11-2019 |
| Abril 2021 | 11 | Actualización y adecuación a nueva estructura Comité de Seguridad, se ajusta formato de firmas | Christian Acosta Verdugo | 14-04-2021 |
| Mayo 2021 | 12 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta Verdugo | 18-05-2021 |
| Julio 2021 | 13 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta | 27-07-2021 |

## 1. INTRODUCCIÓN

El presente documento, se enmarca en la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP), las recomendaciones de seguridad indicadas en el Decreto Supremo DS Nº 83 de fecha 12 de enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), Ley de Transparencia 20.285 del 11 de agosto del 2008 y la normativa vigente NCh-ISO 27001:2013. Además se define objetivo y alcance de la Política de Escritorio y Pantalla Limpios.

## 2. OBJETIVO

Establecer el marco de referencia para la protección de la información contenida en aquellos activos tales como: escritorio o estación de trabajo, computador de escritorio, notebook y dispositivos removibles (pendrive, memorias Flash, CD, DVD, discos externos o removibles). Con el objetivo de reducir los accesos no autorizados, perdida o daño de la información contenida durante y después de la jornada laboral.

## 3. ALCANCE

Comprende la política de seguridad de la información obligatoria para todo el personal del MOP. Asimismo comprende los activos de información que dan soporte a los productos estratégicos del MOP, de acuerdo al alcance definido por cada dirección dependiente del MOP.

Esta Política actúa sobre los controles contenidos en el Subdominio **Equipamiento, control A.11.2.9** de la Nch-ISO 27001.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del Comité de Seguridad de la Información

**Comité de Seguridad de la Información**

- 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

**Subdivisión de Tecnologías de la Información y Telecomunicaciones**

- Definir e implementar estándares seguros para acceder a las plataformas tecnológicas (sistemas de información, servicios de red, correo institucional, etc.) de propiedad Ministerial, velando por el cumplimiento de la normativa vigente

**Departamento de Seguridad Física SOP**

- Definir e implementar estándares seguros para acceder a Instalaciones Ministeriales de uso común de los Servicios, velando por el cumplimiento de la normativa vigente.

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer, cumplir la política de seguridad de la información vigente.

## 5. DEFINICIONES

### Ubicación de Escritorios y Equipos.

Los lugares de trabajo del personal que presta servicios en la institución deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el trabajador.

Los equipos que queden ubicados cerca de zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas.

Los equipos de reproducción de información (por ejemplo: impresoras, fotocopiadoras), deben estar ubicados en lugares con acceso controlado y cualquier documentación confidencial o sensible se debe retirar inmediatamente del equipo.

### Escritorios Limpios

Toda vez que el personal se ausente de su lugar de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.

Si la estación de trabajo del personal está ubicada cerca de zonas de atención de público, al ausentarse de su lugar de trabajo, debe guardar también los documentos y medios que contengan información de uso interno.

Al finalizar la jornada de trabajo, el personal debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además desconectarse de los computadores centrales o sistemas de información, servidores y estaciones de trabajo de oficina cuando la sesión haya finalizado (por ejemplo, no apagar sólo el monitor de la terminal o estación de trabajo).

La información clasificada o sensible, cuando se imprima se debería retirar inmediatamente de las impresoras.

Todo documento que este siendo trabajado por parte del personal, debe ser respaldado en los repositorios documentales o directorios de red destinados para su área o función.

### Pantalla Limpia

Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo al protector de pantalla definido por el Departamento de Soporte Informático de la Subdivisión de Tecnologías de la Información y Telecomunicaciones, de forma que se active ante un tiempo sin uso.

La pantalla de autenticación a la red de la institución debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.

Toda vez que el personal se ausente de su lugar de trabajo debe bloquear su estación de trabajo de forma de proteger el acceso a las aplicaciones y servicios de la institución.

## 6. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años al menos, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional

# POLITICA DE CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

## SUBSECRETARÍA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

## Control de Cambios

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Julio 2018 | 1.0 | Creación del Documento | SDIT-DCyF | 25-07-2018 |
| Julio 2018 | 1.1 | En reunión de coordinación con los encargados de PMG SSI de cada Dirección se acuerda agregar los dominios de la norma NCh 27001 of 2013.- Minuta Número 6. | Pedro Alcaide | 21-11-2018 |
| Noviembre 2018 | 2.0 | Encargados de PMG SSI de los Servicios MOP cambian estructura de documento a presentar a la Red de Expertos | Servicios MOP | 28-11-2018 |
| Diciembre 2018 | 3.0 | Revisión final Encargados de Seguridad de la Información de los Servicios. | Servicios MOP | 06-12-2018 |
| Noviembre 2019 | 4.0 | Revisión Política, se modifica de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 06-11-2019 |
| Abril 2021 | 5.0 | Actualización y adecuación a nueva estructura Comité de Seguridad, se ajusta formato de firmas | Christian Acosta Verdugo | 14-04-2021 |
| Mayo 2021 | 6.0 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta | 18-05-2021 |
| Julio 2021 | 7.0 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta | 27-07-2021 |

## 1. INTRODUCCIÓN

La presente Política de la Continuidad de la Seguridad de la Información se enmarca en la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP).

## 2. OBJETIVOS

El objetivo general de la presente Política, es mantener la seguridad de la información integrada en los sistemas de gestión de continuidad de los productos estratégicos y procesos definidos por el MOP y sus Servicios dependientes, definidos en la Política General de la Seguridad de la Información.

El objetivo de este documento es brindar una guía que permita, al personal designado por la Subdivisión de Tecnologías de la Información y Telecomunicaciones (SDIT) y en coordinación con las altas autoridades de la Subsecretaría de Obras Públicas (SOP) gestionar de mejor forma el desempeño diario de las tareas que involucran los activos de información de acuerdo con la normativa vigente, respecto de contingencias catastróficas o emergencias que impidan la operación normal de las plataformas tecnológicas que soportan los servicios y productos de la empresa.

El foco estará centrado en aquellas actividades críticas para el negocio según definición expresa de la alta dirección en la Política General de Seguridad de la Información.

## 3. ALCANCE

El alcance de esta Política, se extiende a todos los Servicios MOP, en específico a los activos de información involucrados que dan soporte a los productos estratégicos y procesos definidos en la Política General de Seguridad de la Información.

Esta Política actúa sobre todos los controles contenidos en el dominio, **“Aspectos de seguridad de la información en la Gestión de la continuidad del negocio**” ***A.17, en particular el control A.17.01.01*** *de la norma* Nch-ISO 27001 de 2013.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del Comité de Seguridad de la Información

**Comité de Seguridad de la Información**

- 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

**Subdivisión Tecnologías de la Información y Telecomunicaciones.**

- Definir e implementar estándares seguros para acceder a las plataformas tecnológicas (sistemas de información, servicios de red, correo institucional, etc) de propiedad Ministerial, velando por el cumplimiento de la normativa vigente.
- Definir planes de continuidad para los servicios dispuestos por la Subdivisión y en particular de la continuidad del Sistema de Gestión de la Seguridad de la Información.

### Funcionarios y Personal Externo

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer, cumplir la política de seguridad de la información vigente.

## 5. DEFINICIONES

**Continuidad de la Seguridad de la Información**

**Planificación de la continuidad de la seguridad de la información**: La organización debe determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

**Implantación de la continuidad de la seguridad de la información**: La organización debe establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.

**Verificación, revisión y evaluación de la continuidad de la seguridad de la información**: La organización debe verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 6. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años al menos, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional.

# POLÍTICA DE SEGURIDAD DE GESTION Y DESARROLLO DE PERSONAS

## SUBSECRETARIA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

**Tabla de Contenidos**

## Control de Cambios

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Agosto 2012 | 1 | Creación del Documento | Carlos Guzmán | 17-08-2012 |
| Diciembre 2015 | 2 | Actualizada según observaciones de los Servicios MOP | Pedro Alcaide | 28-12-2015 |
| Septiembre 2016 | 3 | Actualización según revisión y observaciones de los servicios MOP | Pedro Alcaide | 08-09-2016 |
| Septiembre 2017 | 4 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Noviembre 2019 | 5 | Actualización del nombre de acuerdo a lineamientos del Servicio Civil y se agregan nuevos requisitos de control del dominio A7.<br>se modifica de acuerdo a la nueva estructura | Servicios MOP | 06-11-2019 |
| Febrero 2021 | 6 | Actualización y adecuación de estructura para la SOP | Christian Acosta Verdugo | 16-02-2021 |
| Mayo 2021 | 7 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta Verdugo | 18-05-2021 |
| Julio 2021 | 8 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta | 27-07-2021 |

## 1. Introducción

La presente política, se enmarca en la Política General de Seguridad de la Información para el Ministerio de Obras Públicas (MOP), aprobada por el Comité de Seguridad de la Información, vigente a la fecha.

En particular este documento, define y establece el objetivo y alcance de la POLÍTICA DE SEGURIDAD DE GESTION Y DESARROLLO DE PERSONAS.

## 2. Objetivo general

Asegurar que el personal de la SOP y proveedores externos, conozcan, entiendan y asuman los derechos, las responsabilidades y obligaciones que les corresponden por el uso y/o acceso a los activos de información de la organización, procurándose la idoneidad para los roles para los cuales son considerados.

## 3. Objetivo específico

Establecer el marco de referencia para la implementación de normas y procedimientos referidos a los derechos, responsabilidades y obligaciones aplicables a todas las personas que laboran o ejecutan tareas en la SOP en relación con los activos de información a los cuales tienen acceso con ocasión de su quehacer en la SOP.

## 4. Alcance

Comprende la política de Seguridad de la Información obligatoria para todo el personal del SOP, desde su ingreso hasta su desvinculación y considera los productos estratégicos, de acuerdo al alcance definido por la SOP.

Esta Política actúa sobre los controles contenidos en el **dominio Seguridad ligada a los Recursos Humanos, Dominio A.7, los controlesA.07.2.1 y el control A.07.2.2** de la Norma NCh-ISO 27001

## 5. Roles y Responsabilidades

**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.

**Jefatura de Gestión y Desarrollo de Personas SOP**

- Esta debe velar por la implementación, aplicación y cumplimiento de la presente política, además visar las normas y procedimientos que emanen de ella.

**Encargado de Seguridad de la Información**

- 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.
- Es miembro del Comité 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

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer y cumplir la política de seguridad de la información vigente.

## 6. Materia especifica que aborda la Política de Seguridad de Gestión y Desarrollo de Personas

En las siguientes secciones se define específicamente la Política relativa a seguridad de la Gestión y Desarrollo de Personas en materia de Seguridad de la Información complementando las Políticas propias del Proceso de Gestión y Desarrollo de personas vigentes en la SOP, que comprende desde el ingreso hasta la desvinculación del personal.

### 6.1. Selección de personal (Investigación de antecedentes)

Durante el proceso de selección de personal se debe tener presente lo siguiente:

Los perfiles de cargo deberán considerar en la descripción de las responsabilidades, las relacionadas con el manejo y resguardo de los activos de información a los cuales se tendrá acceso, especialmente cuando se trate de manipular información sensible o altamente confidencial.

Si el cargo está relacionado con la gestión de información sensible o altamente confidencial, el proceso de selección deberá medir la posesión de las competencias relacionadas en los postulantes.

### 6.2. Contratación e Inducción (términos y condiciones de contratación)

Las responsabilidades de seguridad deberán incluirse expresamente en los decretos o resoluciones de nombramiento o en las contrataciones respectivas.

En el caso de alumnos en práctica, o personal contratado a honorarios, sus resoluciones convenios deben incluir una cláusula en que el Asesor o Experto se comprometa aceptar y cumplir las políticas y normas de seguridad de la información

vigentes, y a hacer un uso adecuado de los activos de información que conozca en virtud del desarrollo de sus labores, obligándose a guardar confidencialidad en los casos que corresponda.

En el caso de terceros o proveedores externos que presten servicios en la SOP, en los contratos se debe incluir una cláusula en que dichas personas se comprometan a aceptar y cumplir las política y normas de seguridad de la información y hacer un uso adecuado de los activos información que conozca en virtud del desarrollo de sus labores y a guardar confidencialidad en los casos que corresponda.

En el proceso de inducción institucional se debe incluir un acápite referido a la normativa vigente (Políticas, Procedimientos e Informes) de Seguridad de la Información, destacando la responsabilidad que el personal tiene respecto al uso de activos de información.

### 6.3. Durante el ejercicio del cargo o función (Responsabilidades de Gestión)

Todo el personal que se desempeña en el MOP, alumnos en práctica y las personas externas que presten servicios permanentes o temporales, deben respetar y adherir a la Política General de Seguridad de la Información del MOP y a las Políticas específicas que la complementan.

Para este efecto se deben tener presente los siguientes lineamientos:

Todo el personal debe ser informado periódicamente por el Encargado de Seguridad de la Información del Servicio, y recibir capacitación cuando corresponda, sobre las políticas, normas y procedimientos de seguridad de la información aplicables en la MOP. Se debe promover la importancia que reviste el resguardo de la información, de manera que estén preparados para apoyar y cumplir la política de seguridad de la organización durante su trabajo normal.

La evaluación del desempeño deberá reflejar el cumplimiento o incumplimiento de las responsabilidades establecidas en el perfil del cargo y en los casos de cargos relacionados con la gestión de información sensible o altamente confidencial, ello deberá formar parte de los compromisos de desempeño de la persona que sirve el cargo, específicamente en el factor 2 Comportamiento Individual, en el sub factor 2.2 Compromiso letra c) maneja adecuadamente información en función de su cargo, transmitiéndola por los canales adecuados, como también la que le requiera reserva.

En relación al tránsito por las dependencias del MOP, así como al acceso a activos de información, tales como documentos, sistemas, bases de datos, aplicaciones u otros, dispuestos por la institución para su desempeño, el personal debe respetar las normas que dicte esta Política y marco normativo vigente en el MOP.

Además, durante el ejercicio de sus funciones, todo el personal del MOP deberá mostrar un comportamiento acorde con las siguientes definiciones:

- No vulnerar los atributos de confidencialidad, integridad y disponibilidad a los que están sujetos los activos de información sobre los cuales tiene tuición o acceso.
- En caso de tener conocimiento de algún incidente o evento que afecte o pueda afectar los principios de confidencialidad, integridad o disponibilidad de los activos de información del MOP, debe comunicarlo inmediatamente a través de los canales establecidos para ello, de acuerdo con la política, normas y procedimientos que se establezcan para estos propósitos.

- Respecto del uso de activos de información, tales como correo electrónico, acceso a internet, impresoras e insumos asociados, debe adherir y respetar las políticas y normas establecidas para ello, las cuales serán dadas a conocer al momento de la inducción después de su contratación.
- En relación al registro o almacenamiento de la información o datos de tipo electrónico, relevantes para las labores o funciones dentro de la SOP, deben ser ingresados, mantenidos o almacenados en los sistemas de información o repositorios o aplicaciones de la red de datos institucional.

### 6.4. Capacitación

Todo el personal que se desempeña en el MOP y las personas externas que presten servicios permanentes o temporales, deberá recibir entrenamiento apropiado del conocimiento y actualizaciones regulares de la normativa vigente en el MOP, referido a la Seguridad de la Información.

### 6.5. Cese o cambio de Funciones y Procesos Disciplinarios

Al momento de la desvinculación o cambio de funciones del personal, en particular en lo relativo a la recuperación de los activos de información asignados, se deberán tener presentes y aplicarse las siguientes consideraciones:

a) El Personal que se desvincule del MOP, debe hacer entrega de todos los activos de información de la organización que estén en su posesión. Este proceso debe ser formal, de acuerdo a las normas y procedimientos que se dicten para este efecto.

b) La Unidad de Gestión y Desarrollo de Personas de la SOP, o que corresponda dentro de la Orgánica del Servicio, debe gestionar la revocación de cuentas y claves de acceso a los sistemas, aplicaciones, dispositivos de autentificación física, u otros servicios, que estén asignados al personal que se desvincula.

Los contratos celebrados con terceros deben contemplar las consideraciones mencionadas en la letra a) y b) del punto 6.5.

En cuanto a Procesos Disciplinarios estos se desarrollarán de acuerdo a la normativa aplicable al MOP, ante evidencias de vulneración en los atributos de Integridad, Disponibilidad y Confidencialidad de los activos de Información.

## 7. Revisión y actualización 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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política

## 8. Difusión de la Política de Seguridad de Gestión y Desarrollo de Personas

Se informará por medio de correo electrónico la revisión y/o actualización de la presente política, la que deberá encontrarse publicada en la Intranet Institucional.

# POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

## SUBSECRETARÍA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

**Control de Cambios**

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Septiembre 2012 | 1.0 | Creación del Documento | Carlos Guzmán | 26-09-2012 |
| Septiembre 2016 | 2.0 | Actualizada según observaciones de los Servicios MOP | Pedro Alcaide | 08-09-2016 |
| Agosto 2017 | 3.0 | Actualización de Formato de acuerdo a lo solicitado por la red de expertos 2017 | Pedro Alcaide | 07-08-2017 |
| Septiembre 2017 | 3.5 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Junio 2018 | 4.0 | Actualización, se modifica la Difusión de la presente Política | Mauricio Leiva | 14-06-2018 |
| Julio 2018 | 5.0 | 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 |
| Noviembre 2018 | 6.0 | Encargados de PMG SSI de los Servicios MOP cambian estructura de documento a presentar a la Red de Expertos | Servicios MOP | 30-11-2018 |
| Diciembre 2018 | 7.0 | Revisión final Encargados de Seguridad de la Información de los Servicios. | Servicios MOP | 06-12-2018 |
| Noviembre 2019 | 8.0 | Se actualiza de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 06-11-2019 |
| Abril 2021 | 9.0 | Actualización y adecuación a nueva estructura Comité de Seguridad, se ajusta formato de firmas | Christian Acosta Verdugo | 14-04-2021 |
| Mayo 2021 | 10.0 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta Verdugo | 18-05-2021 |
| Julio 2021 | 11.0 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta | 27-07-2021 |

## 1. INTRODUCCIÓN

El presente documento, se enmarca dentro de la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP), las recomendaciones de seguridad indicadas en el Decreto Supremo DS Nº 83 de fecha 12 de Enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), Ley de Transparencia 20.285 del 11 de Agosto del 2008 y la normativa vigente NCh-ISO 27001:2013. Además se define objetivo y alcance de la Política de Gestión de Incidentes de Seguridad de la Información, y de cómo se deben prever, reportar, registrar, y gestionar las acciones destinadas a mitigar, corregir y/o eliminar su impacto.

## 2. OBJETIVO

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

## 3. ALCANCE

Todo evento o incidente que afecte negativamente los activos de información que dan soporte a los productos estratégicos del MOP, de acuerdo al alcance definido por cada dirección dependiente del Ministerio.

Esta Política actúa sobre los controles contenidos en el Dominio **Incidente de Seguridad de la Información, A.16 los controles A.16.1.1, A.16.1.2 y A.16.1.5** de la norma NCh-ISO 27001.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del Comité de Seguridad de la Información

**Comité de Seguridad de la Información**

- 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

**Subdivisión de Tecnologías de la Información y Telecomunicaciones.**

- Definir e implementar estándares seguros para resguardar las plataformas tecnológicas (sistemas de información, servicios de red, correo institucional, etc) de propiedad Ministerial, velando por el cumplimiento de la normativa vigente.

**Departamento de Seguridad Física SOP**

- Definir e implementar estándares seguros para resguardar las Instalaciones Ministeriales de uso común de los Servicios, velando por el cumplimiento de la normativa vigente.
- Gestionar y coordinar el contacto con autoridades competentes.

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer, cumplir la política de seguridad de la información vigente.

## 5. DEFINICIONES

**Gestión de incidentes de Seguridad de la Información y Mejoras**

- Responsabilidades y procedimientos: Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- Informe de Eventos de Seguridad de la Información: Los eventos de seguridad de la información se deben informar mediante un ticket de Mesa de Ayuda, por los distintos Administradores de las plataformas de Seguridad de la Información.

- Informe de las debilidades de seguridad de la información: Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización

- Evaluación y decisión de los eventos de seguridad de la información: Se deben evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.

- Respuestas ante incidentes de seguridad de la información: Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.

- Aprendizaje de los incidentes de seguridad de la información: Se debe utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro. Esta base de conocimiento será auditada por Seguridad de la Información.

- Recolección de evidencias: La organización debe definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

## 6. PERIODICIDAD DE EVALUACION Y REVISIÓN

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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional.

# POLÍTICA DE CONTROL DE GESTION DE LAS OPERACIONES Y LAS COMUNICACIONES

## SUBSECRETARÍA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

**Control de Cambios**

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Diciembre 2015 | 1 | Creación del Documento | Pedro Alcaide | 28-12-2015 |
| Septiembre 2016 | 2 | Actualizada según observaciones de los Servicios MOP | Pedro Alcaide | 08-09-2016 |
| Agosto 2017 | 3 | Actualización de Formato de acuerdo a lo solicitado por la red de expertos 2017 | Pedro Alcaide | 07-08-2017 |
| Septiembre 2017 | 4 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Julio 2018 | 5 | Actualización, se modifica el alcance en forma y se agrega el Dominio según últimos lineamientos enviados por la red de expertos. | Mauricio Leiva | 17/07/2018 |
| Julio 2018 | 6 | 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 |
| Noviembre 2019 | 7 | Servicios Cloud Computing al interior del MOP | Christian Acosta | 18/11/2019 |
| Noviembre 2019 | 8 | Se actualiza de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 19/11/2019 |
| Abril 2021 | 9 | Revisión por actualización periódica y cambio estructura en SOP | Pedro Alcaide | 14/04/2021 |
| Mayo 2021 | 10 | *Se agrega rol de Ciberseguridad y sus respectivas funciones* | Christian Acosta Verdugo | 18-05-2021 |
| Julio 2021 | 11 | *Se agregan recomendaciones de la Unidad de Ciberseguridad* | Christian Acosta | 27-07-2121 |

## 1. INTRODUCCIÓN

El presente documento, se enmarca en la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP), las recomendaciones de seguridad indicadas en el Decreto Supremo DS Nº 83 de fecha 12 de enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), Ley de Transparencia 20.285 del 11 de agosto del 2008, DS N°577 del 11 octubre de 1978 y la normativa vigente NCh-ISO 27001:2013. Además se define objetivo y alcance de la Política de Gestión de Activos de Información, para un adecuado resguardo de ellos, asociados a los procesos de negocio a efecto de que permita asegurar la continuidad operacional del MOP y sus Servicios dependientes.

## 2. OBJETIVO GENERAL

El objetivo general de la Política es definir las medidas y controles para eliminar, prevenir y/o mitigar los riesgos y potenciales amenazas relativas a la administración y operación de los sistemas y servicios de información que la componen, asegurando continuidad operacional y el adecuado resguardo de sus activos de información.

## 3. ALCANCE

El alcance de esta Política, se extiende a toda la plataforma tecnológica que da soporte a los productos estratégicos del MOP, independiente de quién sea el administrador de ésta. De acuerdo al alcance definido por cada Servicio dependiente del MOP. A su vez, dicha plataforma se compone de todas las instalaciones y tecnologías relativas al procesamiento y transmisión de voz, datos y video, sistemas de apoyo (respaldo de energía, climatización, y control de incendios) y los sistemas y servicios de información, los cuales se otorgan en forma directa por los respectivos administradores, o a través de terceros (servicios contratados a empresas y/o proveedores externos).

Esta política actúa sobre los controles: A.6.1.1, A.6.1.2, A.12.2.1, A.12.3.1, A.12.4.1 A. 12.4.4 del dominio **A.6 Organización de la seguridad de la información** y **A.12 Seguridad de las Operaciones** respectivamente de la Nch-ISO 27001:2013.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del comité de Seguridad de la Información.

**Jefe Departamento de Operaciones**

- Implementar ambientes que sean independientes entre sí para el procesamiento de datos de producción, pre-producción (pruebas) y construcción.
- Elaborar procedimientos para:
    - asegurar el registro de las actividades realizadas por el personal operativo, para su revisión y fiscalización periódica.
    - comunicar y clasificar eventuales fallas o errores durante la ejecución de tareas operativas.
    - Administrar la información y documentación relativa a la arquitectura, configuración y operación de la plataforma tecnológica del MOP.
- Asegurar la continuidad operacional de los servicios de procesamientos de datos alojados en el Datacenter Ministerial.
- Gestionar de manera preventiva los riesgos institucionales asociados a la implementación de tecnologías de la información.
- Evaluar regularmente la capacidad instalada a efecto de prevenir discontinuidad operacional.

**Jefe Departamento de Telecomunicaciones**

- En particular, están dentro de su ámbito de responsabilidades las siguientes:
- Gestionar de manera preventiva los riesgos institucionales asociados a la implementación de tecnologías de telecomunicaciones.
- Elaborar procedimientos para:
    - asegurar el registro de las actividades realizadas por el personal operativo, para su revisión y fiscalización periódica.
    - comunicar y clasificar eventuales fallas o errores durante la ejecución de tareas operativas.
- Definir e implementar procedimientos para la administración de información y documentación relativa a la arquitectura, configuración y operación de la plataforma tecnológica del MOP.
- Asegurar la continuidad operacional de los servicios de telecomunicaciones alojados en el Datacenter Ministerial, evaluando regularmente la capacidad instalada, a efecto de prevenir la discontinuidad operacional.

**Jefe Departamento de Servicios de Aplicaciones Informáticas**

- En particular, están dentro de su ámbito de responsabilidades la siguiente:
- Definir e implementar controles para evitar la instalación de software, o actualizaciones de software, no autorizados, o que impliquen riesgo para la plataforma tecnológica del MOP.

**Comité de Seguridad de la Información**

- 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

**Subdivisión de Tecnologías de la Información y Telecomunicaciones**

- La responsabilidad de la seguridad de las tecnologías de la información y comunicaciones del MOP, le corresponde al Jefe(a) de la Subdivisión de Tecnologías de la Información y Telecomunicaciones (SDIT). En particular, están dentro de su ámbito de responsabilidades las siguientes:
- Definir y asesorar las políticas, estándares en tecnologías, seguridad de la información (integridad y confidencialidad) y su soporte tecnológico, velando por el cumplimiento de la normativa legal.
- Velar y ser responsable, por la seguridad de los sistemas de información (seguridad informática) del MOP, en conjunto con el Encargado de Seguridad de la Información.
- Informar por escrito y en forma oportuna, a todos los proveedores de servicios externos, respecto de cambios en los responsables de la Subdivisión de Tecnologías de la Información y Telecomunicaciones relacionados con la gestión y administración de los servicios contratados.

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer, cumplir la política de seguridad de la información vigente.

**Encargados de provisión de Servicios de Operaciones y Telecomunicaciones en Direcciones dependientes del MOP.**

- Aquellas Direcciones que cuenten con departamentos o áreas de provisión de servicios de Operaciones y Telecomunicaciones tienen la obligación de cumplir con lo dictaminado en la presente Política.

## 5. Procesos Operacionales

- Se debe contar con procedimientos debidamente documentados para:
  - los procesos en que se sustentan los productos y servicios emanados desde los departamentos de Operaciones, Telecomunicaciones y Servicios Informáticos, que describan las actividades y tareas que deben ejecutarse para la obtención de éstos.
  - los controles de cambios en las configuraciones.

- efectuar monitoreo de servicios categorizados de alta criticidad, debido al impacto en la continuidad operacional del MOP, así como aquellos a los que tenga acceso la ciudadanía.
- la administración y gestión de los servicios proporcionados por proveedores externos al MOP.

- El Departamento de Auditoría Ministerial, tendrá la responsabilidad de efectuar revisiones periódicas respecto del cumplimiento de esta Política, emitiendo un informe de hallazgos con recomendaciones y plazos para subsanar las no conformidades, según su nivel de criticidad.

### 5.1 Separación (segregación) de Funciones

- Las funciones de operación o ejecución de tareas relacionadas con los servicios de operaciones y telecomunicaciones, deben, ser ejecutadas por distintas personas con el objeto de reducir el riesgo de que se produzcan eventuales modificaciones no autorizadas, como asimismo, de un eventual mal uso de la información que podría realizarse por parte de los funcionarios responsables de su ejecución. De no ser posible se debe dejar documentado y colocar en funcionamiento mecanismos de control especiales para mitigar los posibles errores o faltas.

### 5.2 Sincronización de relojes

- Se deben sincronizar los relojes de todos los sistemas de procesamiento de información críticos del MOP con una fuente de tiempo de referencia única.

### 5.3 Separación de ambientes

- Los ambientes de producción, pre-producción (pruebas) y construcción, deben estar separados en forma física y a través de segmentaciones lógicas, y definidas y documentadas las reglas para la transferencia de software entre éstos.

### 5.4 Monitoreo de capacidad instalada

- Se debe contar con procedimientos adecuados para evaluar periódicamente la capacidad instalada a efectos de prevenir la pérdida de rendimiento en capacidad de procesamiento, memoria, almacenamiento y transmisión.
- El resultado del monitoreo deberá ser informado en forma oportuna a los responsables respectivos de manera de poder gestionar las acciones o medidas para prevenir una discontinuidad operacional.

### 5.5 Criterios de aceptación de sistemas

- El Jefe(a) de la Subdivisión de Tecnologías de la Información y Telecomunicaciones, en conjunto con los Jefes de los departamentos de "Operaciones", "Sistemas y Proyectos Informáticos" y el Encargado de Seguridad de la Información, deberán establecer los criterios de aceptación de nuevos sistemas de información y/o las actualizaciones (o nuevas versiones) de los sistemas existentes.

### 5.6 Protección contra software malicioso

- El Jefe del Departamento de Operaciones debe implementar los controles de prevención y detección de software no autorizado, o que genere riesgos para la plataforma tecnológica del MOP (software malicioso).

- Encargado de Seguridad de la Información SOP y/o Ciberseguridad deben definir las plataformas tecnológicas y reglas de operación, para la protección contra software malicioso y ataques cibernéticos

### 5.7 Procedimiento de respaldo y restauración de sistemas y servicios

- El Jefe del Departamento de Operaciones y el Encargado de Seguridad de la Información SOP, deberán determinar los requerimientos, alcances y objetivos del proceso de respaldo de los sistemas de información, software, bases de datos y servicios, en función de su nivel de criticidad e impacto en la continuidad operacional. En su análisis, deberán tenerse presente los requerimientos establecidos por los dueños de los procesos de negocio, en la etapa de diseño de los sistemas de información.

### 5.8 Administración de la Red de Datos

- El Jefe del Departamento de Operaciones y de Telecomunicaciones conjuntamente con el Encargado de Seguridad de la Información SOP, deberán definir los controles necesarios para garantizar la seguridad de los datos y los servicios conectados en las redes del MOP.
- Los Departamentos de Operaciones y de Telecomunicaciones, son los responsables de implementar los controles requeridos en el punto anterior.
- El Encargado de Seguridad de la Información SOP, debe velar por la implementación y cumplimiento de estos controles.

### 5.9 Administración y seguridad de los medios removibles

- El Jefe(a) de la Subdivisión de Tecnologías de la Información y Telecomunicaciones, o quien este designe, en conjunto con el Encargado de Seguridad de Información, deberán implementar procedimientos para la eliminación de medios informáticos removibles empleados en los procesos de respaldo u otros como cintas, discos internos, discos externos, CD/DVD, u otros. Los procedimientos de eliminación deberán contar con registros de todos los medios removibles eliminados.

### 5.10 Procedimientos administración de la información relativa a la plataforma TI

- Todos los activos de información administrados por la Subdivisión de Tecnologías de la Información y Telecomunicaciones, debe estar registrados en el inventario de activos, según lo establece la Política de Gestión de Activos.
- La documentación relativa a configuración, instalación, procesos de sistemas y servicios de información, bases de datos, conectividad de redes, servicios de respaldo de energía, entre otros, debe resguardarse a efecto de prevenir el acceso no autorizado. El acceso a esta documentación debe estar restringido sólo al personal autorizado.
- El acceso a esta información por parte de terceros no autorizados podrán ser permitidos por el Jefe(a) de la Subdivisión de Tecnologías de la Información y Telecomunicaciones, previa coordinación con el Encargado de Seguridad de la Información.

### 5.11 Intercambios de información o software con otras entidades

En los casos en que se requiera establecer intercambio de información o software entre el MOP y otras organizaciones (públicas o privadas), se deberá elaborar y formalizar convenios de intercambio que aborden los siguientes aspectos:

- Identificación de las autoridades responsables de este convenio (de intercambio, interoperación o colaboración).
- Inclusión de cláusulas de confidencialidad, propiedad de la información, derechos de autor, vigencia, condiciones de uso y disposición de la información (o software) involucrada.
- Controles de seguridad a aplicar, para asegurar la integridad y Confidencialidad de la información a intercambiar, si corresponde.
- Términos y condiciones de la licencia conforme a la cual se suministra el software, si corresponde.

Lo anterior, siempre y cuando la información forme parte del inventario de activos de información.

Los procedimientos de transporte de medios informáticos entre diferentes puntos (Envíos postales y mensajería) deberán contemplar:

- Servicios o medios de transporte o mensajería confiables.
- Se deberán incluir en los contratos de servicio cláusulas de confidencialidad, propiedad de la información, derechos de autor, vigencia, tipo de embalaje (cuando corresponda) a utilizar, y disposición de la información involucrada.

- En caso de requerirse la implementación de procesos de interoperación electrónica de datos entre el MOP y otras organizaciones (públicas o privadas), el Encargado de Seguridad de la Información deberá proponer, elaborar y velar para que se

establezcan convenios de interoperación que aborden los siguientes aspectos:

- Identificación de las autoridades responsables de este Convenio de interoperación.
- Inclusión de cláusulas de confidencialidad, propiedad de la información, derechos de autor, vigencia, retención, uso y disposición de la información involucrada.
- Identificación del o los protocolos de transmisión y recepción a emplear (formato de mensajes, notificación de fallas, chequeo de integridad, retransmisiones, término de transmisión, errores, o excepciones).
- Controles de seguridad a aplicar, para asegurar la integridad y confidencialidad de la información. Toda comunicación vía internet o enlace dedicado debe cumplir los tres puntos

  1) Autenticación
  2) Autorización
  3) Encriptación

- Cuando corresponda, se deberán definir acuerdos de niveles de servicio (SLA) y de soporte, que ambas partes se comprometan a proveer, para asegurar la normal operación del proceso de interoperación electrónica.
- Información sobre la propiedad de la información suministrada y las condiciones de su uso.

Se deberán implementar controles para reducir los riesgos en el servicio de correo electrónico institucional.
Debido a restricciones impuestas por el DS N° 83, de 12 de Enero del 2005, se evaluara el uso o contratación de servicios de repositorios electrónicos de datos (o documentos) que operen en internet, de acuerdo a la sensibilidad de los datos a tratar, incluyendo si se trata de datos personales, datos reservados o datos referentes a la seguridad nacional, que podrían tener exigencias específicas que deben ser analizadas caso a caso, pudiendo ser necesario descartar algunos modelos de servicio o implementación en la nube, lo cual es competencia del Comité de Seguridad de la Información MOP. Lo anterior, respetando las sugerencias de la Guía de Buenas Prácticas para el uso de Servicios Cloud Computing al interior de la Administración del Estado (Versión 2, Santiago, 19 de Febrero de 2018, de la División de Gobierno Digital, que se encuentra en publicada en la web, https://cdn.digital.gob.cl/Guia+Cloud+v2.pdf, actualizaciones de esta, cuando se efectúen, o en su reemplazo, por otras directrices que emanen de organismos competentes del Estado).

## 6. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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 particulares del MOP y potenciales consecuencias de incidentes. Sin

perjuicio de lo anterior, se establece que cada dos años, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional.

# POLÍTICA DE CUMPLIMIENTO LEGAL

## SUBSECRETARÍA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

**Control de Cambios**

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Agosto 2017 | 1 | Creación de Política con formatos y títulos acorde a instrucciones emanadas de la red de expertos PMG/MEI - SSI 2017 | Pedro Alcaide | 07-08-2017 |
| Septiembre 2017 | 2 | Actualización, se modifica el alcance agregando los controles involucrados. Se consideran las observaciones de los servicios MOP | Mauricio Leiva | 06-09-2017 |
| Noviembre 2019 | 3 | Se actualiza de acuerdo a la nueva estructura MOP y se ajusta formato de firmas. | Servicios MOP | 06-11-2019 |
| Abril 2021 | 4 | Revisión por actualización periódica y cambio estructura en SOP | Pedro Alcaide | 14-04-2021 |
| Mayo 2021 | 5 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta Verdugo | 18-05-2021 |
| Julio 2021 | 6 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta Verdugo | 27-07-2021 |

## 1. INTRODUCCIÓN

El presente documento, se enmarca en la Política General de Seguridad de la Información vigente para el Ministerio de Obras Públicas (MOP), las recomendaciones de seguridad indicadas en el Decreto Supremo DS Nº 83 de fecha 12 de enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), Ley de Transparencia 20.285 del 11 de agosto del 2008, DS N°577 del 11 octubre de 1978 y la normativa vigente NCh-ISO 27001:2013.

## 2. OBJETIVO GENERAL

Evitar incumplimientos a las obligaciones legales, estatutarias, normativas o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad.

Garantizar que la seguridad de la información se implementa y se opera de acuerdo a las políticas y procedimientos vigentes en el MOP y dando cumplimiento a la norma ISO 27001.

## 3. ALCANCE

Comprende la política de seguridad de la información obligatoria para todo el personal del MOP. Asimismo comprende los activos de información que dan soporte a los productos estratégicos del MOP, de acuerdo al alcance definido por cada dirección dependiente del MOP.

Esta Política actúa sobre los controles contenidos en el Subdominio **Política Cumplimiento de los Requisitos Legales y Contractuales, controles A.18.1.1, A.18.02.1** de la Nch-ISO 27001.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del comité de Seguridad de la Información.

**Comité de Seguridad de la Información**

- 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

**Subdivisión de Tecnologías de la Información y Telecomunicaciones**

- Mantener y custodiar pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.
- Controlar y revisar periódicamente los equipos para verificar que sólo se instale software y productos licenciados

## 5. Materia especifica que aborda esta política de cumplimiento legal

### 5.1. Identificación de los requisitos de legislación y contractuales correspondientes.

La normativa vigente relacionada con el Sistema de Seguridad de la Información debe ser identificada y debidamente difundida dentro de la institución, incluyendo lo siguiente:

- Marco Normativo Aplicable al MOP
- Modernización del Estado
- Gobierno Electrónico
- Transparencia y Acceso a la Información Pública
- Procedimiento Administrativo

### 5.2. Derechos de propiedad intelectual

En el correcto cumplimiento de la Ley de Propiedad Intelectual y Derechos de Autor, el MOP provee los recursos necesarios para el uso de software licenciados, los cuales deben ser adquiridos por proveedores autorizados y confiables, dejando

estrictamente prohibido el uso de software no licenciado. El uso ilegal de software es considerado falta grave, por lo que serán aplicadas las medidas disciplinarias correspondientes a quien se sorprenda incurriendo en esa falta.

No se debe duplicar, convertir a otro formato ni extraer grabaciones comerciales (película, audio) a no ser que lo permita la ley de derecho de autor; no copiar libros, artículos, informes u otros documentos en su totalidad o en parte, que no sean los permitidos por la ley de derecho de autor.

### 5.3. Protección de registros

Los activos de información de los procesos de provisión del MOP se deben proteger contra pérdidas, destrucción, falsificación, acceso no autorizado y publicación no autorizada de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales, considerando para estos casos, la Política Gestión de Activos de Información y los respectivos Procedimientos de Uso y Respaldo.

### 5.4. Privacidad y protección de información personal identificable

• La responsabilidad de manejar información personal identificable y de garantizar el conocimiento de los principios de privacidad se debe abordar de acuerdo con la legislación y las normativas pertinentes. Se deberían implementar las medidas técnicas y organizacionales adecuadas para proteger la información personal identificable.

• La protección de datos personales se encuentra regulada en diversos instrumentos jurídicos, clasificables en normas generales y sectoriales. La Ley 19628: "Sobre protección de la vida privada y Protección de Datos de Carácter Personal" y la Ley 20285: "Ley de Transparencia y Acceso a la Información Pública" establecen los procedimientos para el ejercicio del derecho, amparo y la protección de los datos personales.

• El MOP se compromete a asegurar la privacidad y la protección de la información personal identificable de acuerdo a la legislación y las normativas vigentes y a informar a sus funcionarios sobre cuál es el proceder de la Institución en lo que respecta a la obtención, almacenamiento, uso, protección y divulgación de información de carácter personal.

### 5.5. Obtención

• La información personal se puede obtener de diversas formas, por ejemplo de manera directa a través del mismo funcionario, proveedor o colaborador; así como otras fuentes permitidas por la ley.

#### 5.5.1. Almacenamiento

• La información personal debe ser almacenada de manera de proteger su confidencialidad, integridad y disponibilidad, utilizando los mecanismos y herramientas adecuadas según sea el formato en el que se encuentra.

### 5.5.2. Uso

El MOP utiliza la información personal para dar cumplimiento a obligaciones contraídas por convenios, para permitir, adaptar y/o modificar servicios o programas administrados y para el envío de información que pudiera resultar de interés para funcionarios, proveedores y/o colaboradores.

### 5.5.3. Divulgación

El MOP no vende, comparte o divulga los datos personales o información de los funcionarios, proveedores y/o colaboradores, excepto en los casos en que una ley, reglamentación o autoridad judicial así lo requiera o cuando los derechos o propiedad del MOP se vean amenazados.

### 5.5.4. Protección

El MOP utiliza tecnología para proteger la información personal que se proporciona, mediante políticas de control de acceso y uso de software seguros. El manejo del uso y archivo de expedientes electrónicos y físicos se realiza a través de personal autorizado y capacitado que desarrolla sus funciones dentro del MOP y tiene pleno conocimiento de la presente política.

## 5.6. Revisión independiente de la seguridad en la información

Para asegurar la idoneidad, adecuación y efectividad continua del enfoque del MOP para administrar la seguridad de la información, se deben realizar periódicamente revisiones independientes.

Dicha revisión la deben realizar personas independientes del área bajo revisión, es decir, la función de auditoría interna, una Dirección independiente o una organización externa que se especialice en éstas revisiones. Las personas que realizan éstas revisiones deben contar con las habilidades y experiencia adecuadas.

Los resultados de esta revisión se deben registrar e informar a la dirección que inició esta revisión, manteniendo y protegiendo los registros que se generen durante el proceso de auditoría.

Si la revisión identifica o detecta que no se cumplen los objetivos y requisitos adecuados o que no cumplen con la indicación de seguridad de la información establecida en las políticas de seguridad de la información, se deben tomar las medidas correctivas correspondientes.

## 6. Revisión y actualización 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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN de la Política y Cumplimiento Legal

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional.

# POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENCIÓN DE SISTEMAS DE INFORMACIÓN

## SUBSECRETARÍA DE OBRAS PÚBLICAS

**Comité Seguridad de la Información**

## TABLA DE CONTENIDOS

**Control de Versión**

| Revisión | Versión del Documento | Modificación Realizada | Autor | Fecha del Cambio |
|---|---|---|---|---|
| Junio 2018 | 1 | Creación del Documento | Pedro Alcaide | 04-06-2018 |
| Junio 2018 | 2 | Actualización, se realizan cambios en gestión actual de las áreas involucradas en el paso a producción de un nuevo servicio informático o aplicación.<br>Se modifica alcance para agregar control normativo.<br>Se modifica mecanismo de difusión. | Pedro Alcaide | 05-06-2018 |
| Junio 2018 | 3 | Actualización, se modifica la difusión de la presente Política. | Mauricio Leiva | 14-06-2018 |
| Julio 2018 | 4 | 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 | 5 | 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 |
| Noviembre 2018 | 6 | Encargados de PMG SSI de los Servicios MOP cambian estructura de documento a presentar a la Red de Expertos | Servicios MOP | 28-11-2018 |
| Mayo 2019 | 7 | Encargados de PMG SSI de los Servicios MOP incorporan requisitos para el desarrollo seguro | Servicios MOP | 03-06-2019 |
| Julio 2019 | 8 | Actualización para coherencia con Procedimientos | Natalia Kent; Milena Lagos; Christian Acosta; Rodrigo Muñoz | 07-08-2019 |
| Noviembre 2019 | 9 | Actualiza Introducción - alcance – Roles y responsabilidades, se modifica de acuerdo a la nueva estructura MOP y se ajusta formato de firmas | Servicios MOP | 06-11-2019 |

| | | | | |
|---|---|---|---|---|
| Abril 2021 | 10 | Revisión por actualización periódica y cambio estructura en SOP | Pedro Alcaide | 14-04-2021 |
| Mayo 2021 | 11 | Se agrega rol de Ciberseguridad y sus respectivas funciones | Christian Acosta Verdugo | 18-05-2021 |
| Julio 2021 | 12 | Se agregan recomendaciones de la Unidad de Ciberseguridad | Christian Acosta Verdugo | 27-07-2021 |

## 1. INTRODUCCIÓN

La presente política, se enmarca en la Política General de Seguridad de la Información para el Ministerio de Obras Públicas (MOP), aprobada por el comité de Seguridad de la Información, vigente a la fecha.

En particular este documento, define y establece el objetivo y alcance de la Política de Desarrollo, Mantención y Adquisición de Sistemas de Información del MOP.

## 2. OBJETIVO

Definir el marco normativo de seguridad a aplicar en el proceso de desarrollo, mantención, y adquisición de sistemas de información en el MOP. Especificar los requisitos de seguridad en la implantación de los sistemas de información en fase de desarrollo (o adquisición) o de mantención (correctiva o evolutiva). Establecer los métodos de protección de la información crítica o sensible, aplicable a los sistemas de Información.

## 3. ALCANCE

Están dentro del alcance de esta política, todas las implementaciones (desarrollo y mantención) o adquisiciones de sistemas de información del Ministerio de Obras Públicas.

Esta Política actúa sobre los controles contenidos en el dominio **Adquisición, Desarrollo y Mantenimiento del Sistema, Dominio A.14, controles A.14.1.2, A.14.2.1, A.14.2.9** de la Nch-ISO 27001.

## 4. ROLES Y RESPONSABILIDADES

**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.

**Encargado de Seguridad de la Información del Servicio**

- 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.
- Es miembro del comité de Seguridad de la Información.

**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

**Subdivisión de Tecnologías de la Información y Telecomunicaciones.**

- Definir e implementar estándares seguros para desarrollo, mantención y adquisición de las plataformas tecnológicas (sistemas de información, servicios de red, correo institucional, etc) de propiedad Ministerial, velando por el cumplimiento de la normativa vigente.

**Funcionarios y Personal Externo**

- Es el personal, sin importar su calidad jurídica, y externos que presten servicios permanentes o temporalmente, que tengan acceso a los activos de información y/o los sistemas para su procesamiento, los que deben conocer y cumplir la política de seguridad de la información vigente.

**Unidades de Informática de los Servicios:**

- Implementa los estándares definidos por la Subdivisión de Tecnologías de la Información y Telecomunicaciones para desarrollo, mantención y adquisición de sistemas de información propios.

## 5. DEFINICIONES

**Requisitos de seguridad de los sistemas de información**

Se debe establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización. Considerando los siguientes aspectos:

- Cada aplicación debe ser liderada por un responsable del negocio quién define los impactos, requisitos funcionales y es responsable de los datos que contiene y quienes están autorizados para modificarlos o consultarlos.

- Categorizar la aplicación informática y donde se almacenan los datos según la clasificación de seguridad de los datos que contiene.

- Seguridad al acceso para los entornos de desarrollo, Pruebas y Producción. Entorno de desarrollo seguro: La organización deberá establecer y proteger adecuadamente

los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del software.

- Roles y Perfiles de la aplicación informática.

- Implementar metodología de desarrollo para cada proyecto.

- Implementar control de versiones para toda aplicación, tanto desarrollo interno a la organización como externalizado. Estos accesos a los códigos fuentes de las aplicaciones está restringido a personal autorizado.

- Fortalecer el conocimiento de los desarrolladores para evitar, detectar y solucionar vulnerabilidades en el ciclo de vida del software y sus controles de acceso.

- Si se externaliza el desarrollo, la organización debería obtener la garantía de que la parte externa cumple con la presente Política de Seguridad de la Información, como también las normas internas que se deban respetar.

- El Ministerio de Obras Publicas deberá velar por el cumplimiento de los lineamientos emitidos por el Estado de Chile, relativos a la seguridad del desarrollo de sistemas informáticos.

- Procedimientos de control de cambios del sistema: En el ciclo de vida de desarrollo se debe hacer uso de procedimientos formales de control de cambios.

- Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación: Las aplicaciones se deben revisar y probar para garantizar que no se generen impactos adversos en la operación o en la seguridad de la organización.

- Desarrollo externalizado: La organización deberá supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado y la propiedad de los programas fuentes deben ser del MOP.

- Pruebas de seguridad de tecnologías de la información y datos publicados hacia internet: Se debe realizar pruebas de vulnerabilidad en aspectos de seguridad durante las etapas del desarrollo y auditorias periódicas en la operación.

- Pruebas de aprobación del sistema: Se debe establecer planes de prueba y criterios relacionados para la aceptación de sistemas de información, como también evidencias de aprobación de las pruebas y su ejecución debe ser realizada por expertos del negocio.

- En el caso de compra de Servicios de software en la nube, el Jefe del Servicio respectivo debe evaluar los aspectos de seguridad de la información relativos a continuidad del negocio, confidencialidad e integridad de los datos que contiene y el cumplimiento de la normativa vigente.

## 6. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

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 particulares del MOP y potenciales consecuencias de incidentes. Sin perjuicio de lo anterior, se establece que cada dos años, esta Política debe ser sometida a revisión para evaluar necesidades de actualización y mejora.

El Comité de Seguridad de la Información determinará la necesidad de acciones puntuales de evaluación de cumplimiento de los lineamientos de esta política.

## 7. DIFUSIÓN

Se difundirá por medio de correo electrónico la presente Política, que además se encontrará publicada en la Intranet Institucional.

**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 PUBLICAS DIRE
Subsecretaría de Obras Públicas
2021-09-20 11:34

**SUBSECRETARIO DE OBRAS PÚBLICAS**

CAV NKG CBK EPG RCA