Ministerio de Obras Públicas

Gobierno de Chile

SUBSECRETARIA OO. PP.
OFICINA DE PARTES
02 FEB 2023
TRAMITADO

DEJA SIN EFECTO PARCIALMENTE LA RESOLUCIÓN N° 983 DE FECHA 20 DE SEPTIEMBRE DE 2021 Y APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE OBRAS PÚBLICAS

Santiago, 02 FEB 2023

VISTOS:

El DFL Nº 1/19.653 de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la ley Nº 19.880, de 2003, que establece Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado; el DL N°1028 del Ministerio del Interior; el DFL MOP Nº 850, de 1997, del Ministerio de Obras Públicas, que fija el texto refundido, coordinado y sistematizado de la ley Nº 15.840, de 1964 y del DFL N° 206, de 1960; la Resolución Nº 6, de 2019, de la Contraloría General de la República; la Resolución Exenta SOP N° 983 de 2021; la Resolución Exenta SOP N° 246 de fecha 25 de noviembre de 2022; y el Ord. Nº704, de fecha 20 de diciembre de 2022, del Jefe de División de Administración y Secretaría General de la Subsecretaría de Obras Públicas.

CONSIDERANDO:

1.- Que, de conformidad a lo señalado en el artículo 24 del DFL N°1/19.653, de 2000 del Ministerio Secretaría General de la Presidencia, que fija en texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, en el artículo 14° del DFL N°7912, de 1927 del Ministerio del Interior, en el artículo 1° del DL N°1028 de 1975, del Ministerio del Interior, y en el artículo 6° del DFL N°850, de 1997del Ministerio de Obras Públicas, corresponde a este Subsecretario, entre otras las funciones y atribuciones , todo aquello relacionado con la administración y servicio interno de esta Subsecretaría de Estado.

2.- Que, el Ministerio de Obras Públicas y sus servicios dependientes, como integrante de la Administración del Estado, se encuentran en el deber de dar adecuado resguardo a los principios y normas en materia de Seguridad de la Información.

3.- Que, en concordancia con el proceso de continua modernización del MOP y el mejoramiento permanente de la gestión administrativa de esta Subsecretaría y con la finalidad de mejorar y profundizar todas aquellas medidas que garanticen una administración del Estado sustentada en la observancia de los principios de responsabilidad, eficiencia, eficacia, coordinación, impulsión de oficio del procedimiento, control, probidad, transparencia en la gestión pública, es necesario actualizar los roles y responsabilidades asociadas a la Seguridad de la Información a nivel Ministerial.

4.- En este contexto, con fecha 25 de noviembre de 2022 se dictó la Resolución Exenta SOP N° 246, que dejó sin efecto las Resoluciones SOP Exentas N° 1911, de 2011, N°1316, de 2014 y N°166 de 2021; y modificó las resoluciones SOP Exentas N°1271, de 2018 y N°983, de 2021 en el sentido que indica.

5.- Que, la mencionada resolución en el N° III de su parte resolutiva, instruyó al Comité de Seguridad de la Información de esta Subsecretaría, para que hasta el día 20 de diciembre de 2022, propusiese la adecuación de las Políticas Generales y Especificas de Seguridad de la Información, aprobadas mediante Resolución Exenta SOP N°983, de 2021, en el sentido de considerar en las mismas, la nueva estructura de roles y responsabilidades derivadas de las modificaciones que la citada resolución resolvió realizar a la Resolución Exenta SOP N°1271, de 2018.

6.- Que asimismo, la resolución en comento instruyó que las señaladas adecuaciones fuesen remitidas a esta autoridad para su aprobación mediante el correspondiente acto administrativo.

7.- En cumplimiento a lo anterior el Jefe de la División de Administración y Secretaría General de la Subsecretaría de Obras Públicas, en su calidad de presidente del Comité de Seguridad de la Información, mediante Oficio Ord. N°704 de fecha 20 de diciembre de 2022, propuso la adecuación de las políticas generales de Seguridad de la Información.

8.- Que, habiéndose dado cumplimiento a lo instruido por esta Subsecretaría, mediante Resolución Exenta SOP N° 246, de 25 de noviembre de 2022, las Políticas Generales de Seguridad de la Información, deben ser aprobadas por acto administrativo dictado por esta autoridad.

9.- Que sin perjuicio de lo anterior, las Políticas Específicas de Seguridad de la Información están siendo, a la fecha de este acto administrativo, sometidas a revisión y serán por consiguientemente aprobadas en su oportunidad. Por lo tanto, en lo relativo a las mismas se mantiene plenamente vigente lo dispuesto en la Resolución Exenta SOP N° 983, de fecha 20 de septiembre de 2021.

10.- En definitiva, teniendo en consideración de lo indicado en los numerales anteriores, es necesario, dar aprobación en este acto a la Política General de Seguridad de la Información.

RESUELVO: 32

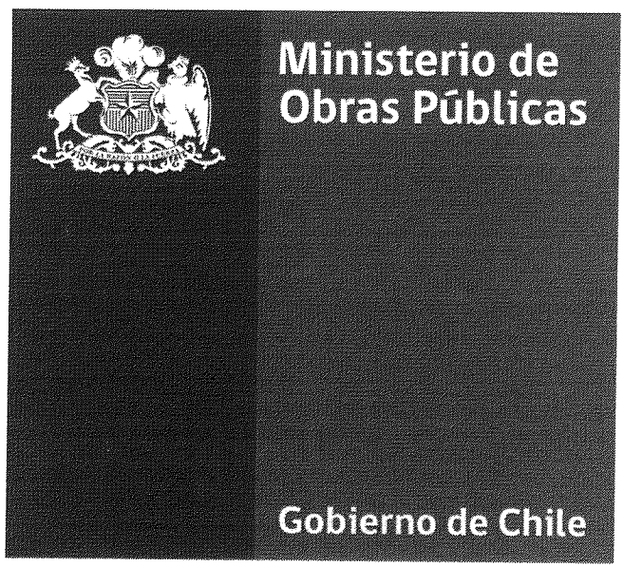
1. **DÉJESE SIN EFECTO PARCIALMENTE,** a contar de esta fecha la Resolución Exenta SOP N° 983, de fecha 20 de septiembre de 2021, en numeral 2° de su parte resolutiva lo referido a la aprobación de la POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

2. **ESTABLECE** que en todo lo no modificado continua vigente la resolución Exenta SOP N° 983, de fecha 20 de septiembre de 2021, en cuanto a las Políticas Específicas de Seguridad de la Información.

3. **APRÚEBESE,** a contar de esta fecha, las adecuaciones de las Políticas Generales de Seguridad de la Información, remitidas mediante Oficio Ordinario N° 704 de 2022, por el Jefe de la División de Administración y Secretaría General de la Subsecretaría de Obras Públicas, cuyo texto íntegro se transcribe a continuación:

MINISTERIO DE OBRAS PÚBLICAS

Subsecretaría de Obras Públicas



POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Contenido

CONTROL DE CAMBIO

Control de cambio, corresponde al registro de actualización de la política general de seguridad de la información.

Autor	*Versión*	*Adecuación*	*Aprobador*	*Fecha*
Carlos Soto Bascur	*1.0*	*Versión Inicial*		*07-12-22*

INTRODUCCION

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 (SGSI) fijando los estándares de seguridad de la información a aplicar, para proteger adecuadamente los activos de información y dar cumplimiento a lo establecido en la **Norma Chilena NCh-ISO/IEC 27001:2020**, que aborda los siguientes tópicos "Tecnología de la información, Técnicas de seguridad, Sistema de gestión de la seguridad de la información y sus requisitos de control **Norma ISO 27002.**

La implementación se llevará a cabo de manera continua, con la creación del sistema de gestión de la seguridad **SGSI**, que establece, implementa, mantiene y genera la mejora de manera continua del sistema.

La adopción del sistema de gestión de la seguridad de la información es una decisión estratégica para el MOP. El establecimiento e implementación de un sistema de gestión de la seguridad de la información está definido por las necesidades y objetivos de la organización, los requisitos de seguridad y los procesos organizacionales.

El sistema de gestión de la seguridad de la información conserva la **confidencialidad, integridad y disponibilidad de la información** al aplicar un proceso de gestión de riesgo.

OBJETIVO

La política General de Seguridad de la información, tiene como objetivo establecer las directrices institucionales referentes a la responsabilidad, resguardo y gestión de riesgos asociados a la información, además de la definición de reglas sobre el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento u otro tratamiento sobre el activo de la información que afecte al Ministerio de Obras Públicas, la que debe ser comunicada y documentada.

Desarrollar una metodología para la identificación, el análisis, la evaluación, las opciones para el tratamiento y la selección de controles para gestionar los riesgos de la seguridad de la información del **Ministerio de Obras públicas (MOP)**, que produzca resultados comparables y reproducibles.

ALCANCE

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)

El ámbito de aplicación de esta política comprende a todo el personal del Ministerio de Obras Públicas (MOP) y sus Servicios dependientes, cualquiera sea su calidad jurídica, vale decir, personal de planta, contrata, código del trabajo u honorarios a suma alzada. Además, quedan comprendidos, los proveedores externos del MOP y sus Servicios Dependientes, sean personas naturales o jurídicas y que presten servicios en forma permanente o esporádica.

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

La Política define la siguiente metodología; establecer, implementar, mantener y mejorar de manera continua el sistema de gestión de la seguridad de la información con la correspondiente evaluación y tratamiento de los riesgos de la seguridad de la información que se adapta a las necesidades del MOP.

GLOSARIO

Acrónimo	Definición
MOP	Ministerio de Obras Públicas
S.G.S.I	Sistema de gestión de Seguridad de la Información
SOP	Subsecretaria de Obras Publicas
DGOP	Dirección General de Obras Públicas
DGA	Dirección General de Aguas
DGC	Dirección General de Concesiones de Obras Públicas
DAP	Dirección de Aeropuertos
DARQ	Dirección de Arquitectura
DCYF	Dirección de Contabilidad y Finanzas
FIS	Fiscalía de Obras Públicas
DOH	Dirección de Obras Hidráulicas
DOP	Dirección de Obras Portuarias
DIRPLAN	Dirección de Planeamiento
DV	Dirección de Vialidad
I.S.O	Institución Internacional de Estándares
I.E.C	Comisión Electrotécnica Internacional
OAE	Órgano Administración del Estado
Seguridad de la Información	Protección de la información mediante políticas, normativas, estándares, controles, procedimientos, softwares, Hardware, que tiene como objetivo mantener la confidencialidad, integridad, disponibilidad de los activos.
Amenaza	Evento que tiene la propiedad potencial de dañar activos tales como información, procesos y sistemas y por lo tanto afectar las operaciones de la institución. Las amenazas pueden ser naturales, humanas, operacionales, sociales, tecnológicas y a las instalaciones (fuego, daños de agua), entre otras
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Control	Actividad, recurso, actuación o dispositivo que se usa para cumplir con una función en específico o política.
Disponibilidad	Propiedad de la información que tiene como atributo; accesible y utilizable por solicitud de una entidad autorizada.
Impacto	Supone la pérdida de cualquier principio de seguridad de cada activo de información (confidencialidad, integridad y disponibilidad).
Integridad	Propiedad de la información que apunta a mantener la exactitud, autenticidad y totalidad de la información.
Riesgo	Resultado de una amenaza que explota una vulnerabilidad. Se obtiene en función de los valores de amenaza y vulnerabilidad e Impacto.
Gestión del Riesgo	Aplicación de medidas para modificar el riesgo, mitigarlo, aceptar o bien traspasarlo, dependiendo de la Tolerancia o apetito al riesgo que la institución adopte.
Apetito al Riesgo	Cantidad y tipo de riesgo que una institución está dispuesta a aceptar o mantener.
Tolerancia al riesgo	Máxima cantidad de riesgo que una institución puede soportar considerando los controles.
Vulnerabilidad	Debilidad que puede ser explotada por amenazas para causar daños a los activos de la organización. Las vulnerabilidades no causan daño por si solas
Evento de Seguridad	Corresponde al no cumplimiento de los controles o políticas de seguridad.
Incidente de Seguridad	La ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la

	información y el no cumplimiento de la Política de Seguridad de la Información con un impacto en los activos de la Organización.
Activo de la Información	*Todo dato, elemento, componente, equipamiento o sistema relacionado con información o su tratamiento, que tenga valor para la Institución que los utiliza, genera, almacena, envía o intercambia, con otras organizaciones afines o con terceros, que debe ser protegido considerando por su confidencialidad, integridad, disponibilidad u otros factores de importancia.*
Ciberataque	*Una o más acciones desarrolladas en el ciberespacio, con el propósito deliberado de irrumpir, explotar, denegar, degradar o destruir la infraestructura tecnológica; un componente lógico o interacciones de este y que pueden tener distintos niveles según su duración, frecuencia y daño producido.*
Ciberespacio	*Es la geografía virtual o entorno digital, creado por computadoras y redes unidas para interoperar en una red. No solo involucra las redes y protocolos de comunicación, sino que constituye un espacio virtual que es soportado por las redes y computadores. En él, los operadores del equipo pueden interactuar de manera similar al mundo real.*
Ciberseguridad	*Conjunto de políticas, procesos, técnicas, acciones posibles, y buenas prácticas para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos informáticos, los componentes lógicos de la información, datos, servicios, y las interacciones que se verifican en el ciberespacio. Permitiendo la reducción de los efectos y del daño causado durante y después de su ocurrencia de las amenazas e incidentes.*
TIC	*Tecnologías de la Información y la Comunicación.*
Datacenter	*Es la instalación que proporciona acceso compartido a aplicaciones de datos mediante una infraestructura de red, computación y almacenamiento.*
Criptografía	*La criptografía, es la técnica para proteger documentos con el uso de cifras o códigos para ocultar o sobrescribir documentos digitales*
IC	*Infraestructuras Criticas o estratégicas*
CIBERSEG	*Controles de Ciberseguridad basados en la Norma ISO 27032.*
NIST	*Marco de referencia en ámbito de Ciberseguridad.*

POLITICA DE SEGURIDAD

Principio de la Política

La política debe mantener un lineamiento acorde a las directrices definida por el ministerio, siempre que se base en el marco constitucional y legislativo vigente.

El MOP, a través de sus servicios dependientes, se compromete a gestionar la seguridad de la información, como un proceso continuo en el tiempo, para mantener un único Sistema de Gestión de Seguridad de la Información Ministerial, basado en la Norma Chilena NCh-ISO/IEC 27001, que en cumplimiento de las recomendaciones de seguridad contenidas en el Decreto Supremo DS N°83 de fecha 12 de enero del 2005 del Ministerio Secretaría General de la Presidencia (MINSEGPRES), el DS N°93 de fecha 8 de julio del 2006 de MINSEGPRES, y lo establecido en la Política Nacional de Ciberseguridad PNCS 2017-2022, promulgada el 27 de abril del 2017 y el instructivo presidencial N°8 del 23 de octubre de 2018. En la ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, la Ley N°19.628 sobre Protección de la vida privada, la Ley N°21.459 sobre Normas de Delitos informáticos, la Ley N°17.336 de Propiedad Intelectual, la Ley N°21.180 de Transformación digital del Estado, la Ley N°20.285 de Transparencia en la función pública, el Decreto Supremo N°577 del 1978, del Ministerio de Bienes Nacionales, la Ley N°19.913, sobre de Lavado de Activos y todas las demás normas pertinentes aplicables.

El MOP en conjunto con 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 que garantice un alto nivel de continuidad operativa de los procesos críticos, así contribuyendo al cumplimiento de su misión y objetivos estratégicos.

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

El MOP reconoce como activos de información lo siguiente:

- Información.
- Servicios.
- Software.
- Infraestructura.
- Personas
- Procesos

Los activos mencionados, se declaran como "activos valiosos", que por definición deben ser protegidos con igual atención que el resto de los activos críticos de la institución. Todo activo de información debe ser protegido de manera adecuada en base a la clasificación de **confidencialidad, integridad y disponibilidad**, considerando especialmente lo relacionado con los productos estratégicos institucionales, procesos críticos, activos críticos y riesgos.

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

El MOP declara 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.

Todo funcionario o personal que preste servicios al MOP, tiene la obligación de notificar cualquier actividad o situación que afecte la seguridad de los activos de información.

Es responsabilidad del MOP que los terceros o externos, que presten servicios al ministerio, se adhieran a las políticas de seguridad de la información y estén considerados los controles para asegurar la entrega adecuada de accesos durante la vigencia de los respectivos contratos, como también la devolución de los activos del MOP facilitados para la ejecución de sus labores, al término de su contrato o servicio.

El Comité de Seguridad de la Información tiene la autoridad de definir políticas para la protección de la información y velar por la existencia de las medidas de seguridad destinadas a proteger la información del MOP.

Se deben establecer los controles de cumplimiento, para la implementación, mantención, monitoreo, auditoría, control y mejoramiento continuo del SGSI.

Los resultados del seguimiento y medición de un sistema de gestión de la seguridad de la información corresponden a la retroalimentación de información, para apoyar las decisiones relacionadas a la gobernanza, gestión, eficacia operacional y mejora continua del SGSI.

Seguridad del Activo de Información.

Se declara que todo activo de información que sea propio del MOP, deberá estar protegido bajo estricto resguardo que permita mantener la **confidencialidad, integridad y disponibilidad de la información**, permitiendo controlar los riesgos inherentes a los cuales por definición se pueden ver expuestos.

Normativa de Seguridad de la Información

La implementación se llevará a cabo de manera continua, a través del estándar ISO 27001:2020 con los controles basados en la normativa ISO 27002 de la seguridad de la información, la que deberá considerar prioritariamente la información de mayor valor o privilegiada o de uso estratégico.

Normativa de Ciberseguridad

La implementación se llevará a cabo de manera continua, a través de la adopción del estándar ISO 27032, para la correcta implantación de los controles y normativas en el ámbito de CIBERSEG.

Responsabilidad del personal MOP y de los proveedores externos

El personal del MOP, cualquiera sea su calidad jurídica, vale decir, personal de planta, contrata, código del trabajo u honorarios a suma alzada, así como también los proveedores externos a la institución, que posean acceso a la información, serán responsable de mantener el resguardo de los datos o información que traten, con lo que se definen los siguientes privilegios ligados al resguardo de la información.

Propietario(a): Responsable de la información en particular y valorización de la información de forma (Confidencial/ No Confidencial).
Administrador(a): Responsable de resguardar la información y administrar las definiciones de uso.
Usuario(a): realiza el tratamiento de la información, según el privilegio asignado.

Roles

Para cumplir con los objetivos de la política de seguridad de la información del MOP, se establece una estructura de gobernabilidad, en donde el Comité es designado para el cumplimiento del SGSI, dictamina el marco de trabajo de seguridad de la información y contempla la relación con entidades externas del MOP o empresas que entreguen servicio al Ministerio.

Definición de Roles:

Subsecretaria(o) de Obras Públicas

Responsable de aprobar la Política General de Gestión de Seguridad de la Información, con sus futuras modificaciones de mejora continua, con la asesoría del Comité de Seguridad de la Información del MOP.

Comité de Seguridad de la Información MOP

Son los representantes de las Jefaturas Superiores, destinados a dar gobernabilidad a nivel estratégico al sistema de gestión de seguridad de la Información del MOP, además son los responsables de las definiciones de las políticas como tareas en las funciones; aprobar, proponer mejoras, controlar el cumplimiento, seguimiento y monitoreo del **SGSI**, así como también son los responsables de informar al Subsecretario/a sobre el desempeño del sistema de gestión de la seguridad de la información y gestionar los recursos para el plan de desarrollo de la Seguridad de la Información.

Encargado(a) de Ciberseguridad Ministerial

Es el responsable de 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. Además, tiene como función, asesorar al Subsecretario/a y a los directivos del Ministerio de Obras Públicas (MOP) en materias de Ciberseguridad (CS). Deberá también, mantener comunicación y coordinación con el Ministerio del Interior, en materias de Ciberseguridad, y coordinarse 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/Coordinador/Asesor de Seguridad de la Información de las Direcciones MOP

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. Además, son los encargados de la recopilación de los datos necesarios para la alimentación de los indicadores de gestión implementados.

Subdivisión de Tecnologías de la Información y Telecomunicaciones (SDIT)

Es la responsable de las adquisiciones, desarrollo y mantenimiento de los sistemas de procesamiento de información, almacenamiento y transmisión de comunicaciones transversales del MOP.

Jefes Unidades de Tecnologías de la Información de las Direcciones.

Son responsables de las adquisiciones, desarrollo y mantenimiento de los sistemas de procesamiento de información, de almacenamiento y transmisión propias del servicio al que pertenece.

Auditores(as).

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

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 y activos de la organización.

Seguridad ligada a las personas

Las principales medidas de control asociadas a las personas son:

El Jefe de Servicio debe asegurar que los funcionarios a contrata, código del trabajo, personal a honorarios y proveedores externos, conozcan la política y normas de seguridad de la información, asumiendo sus responsabilidades.

Reducir el riesgo del factor humano, asociado a errores con la pérdida de datos, robos o usos indebidos de la información.

Definir acuerdos de confidencialidad de tratamiento de la información.

Definir controles de selección rigurosa del personal, acorde a la inclusión de la seguridad dentro de las responsabilidades contractuales.

Concientización del personal en cuanto a política de seguridad de la información y las medidas que deben contemplar para evitar los riesgos.

Será responsabilidad de cada Dirección el procurar la capacitación de sus funcionarios; personal de planta, contrata, código del trabajo u honorarios a suma alzada y proveedores externos, incluidos los cargos superiores y los Encargados(as), Coordinadores(as), Asesores(as) de la seguridad de la información y ciberseguridad de acuerdo a sus roles y responsabilidades asignadas, de ser necesario para cumplir lo descrito en la normativa vigente.

Cada Dirección deberá desarrollar y mantener un plan de capacitación anual en ciberseguridad y seguridad de la información, que brinde conocimientos sobre la materia a sus funcionarios y asesores. Este plan debe ser aprobado por Ciberseguridad Ministerial y las respectivas áreas de capacitación de las Direcciones.

Definir y conocer los medios de difusión de los incidentes una vez ocurran, de modo que todos los integrantes de la cadena de responsabilidad sepan qué hacer y a quién deben informar en todo momento.

Identificación del personal crítico.

El personal que debe cubrir las tareas críticas del MOP, cuya importancia es vital para la institución. Los procesos críticos son más importantes que los procesos de apoyo.

Las contrataciones del personal del MOP, y los acuerdos contractuales con proveedores externos deben incluir la Política General de Seguridad de la Información.

Seguridad física y ambiental

Prevenir el acceso no autorizado, daño, interferencia, eventos o causas de índole ambiental que afecten negativamente los activos de información. En rigor la aplicación de la política de pantalla y escritorio Limpios, con la que se reduce el riesgo del acceso a personal no autorizado, además la pérdida o daño de la información durante y/o fuera del horario de trabajo.

Establecer áreas seguras que tienen como objetivo evitar los accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información.

Establecer Perímetro de seguridad física como Control, es decir, definir un perímetro de seguridad para proteger las áreas que contienen información sensible o crítica y las instalaciones de procesamiento de información (Datacenter).

Controles de acceso físico, estableciendo las áreas seguras que deben estar protegidos por controles apropiados que aseguren que solo se permite el acceso a personal autorizado.

Protección contra amenazas externas y del ambiente, diseñando y aplicando la protección física contra daños por desastre natural, ataque malicioso o accidentes.

Trabajo en áreas seguras, para lo cual se deben diseñar y aplicar procedimientos para cumplir.

Áreas de entrega y carga, es decir, se deben controlar los puntos de acceso tales como áreas de acceso a las dependencias, donde las personas no autorizadas puedan acceder a las instalaciones de la institución y aislarlas de las instalaciones de procesamiento de la información o áreas críticas operacionales.

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 transportan a redes públicas, a través de distintos medios. Para ello se debe considerar lo siguiente:

- Correcta administración de las redes, cualquiera sea su naturaleza, manteniendo siempre una separación entre entornos.

- Adecuada monitorización de eventos y/o anomalías, de manera tal que permita identificar, si corresponde o no a un incidente de Seguridad de la Información y mejorar la toma de decisiones.

- Los accesos a las redes internas deben ser monitoreados y solo se debe permitir el acceso a personal autorizado, ya sean funcionarios o asesores, que presten soporte o mantención a las plataformas cuya autorización formal con anticipación.

- Se debe utilizar servicios de red privada virtual (VPN) para conexiones desde otras redes hacia las redes internas donde se encuentran las plataformas del MOP. Este servicio debe contar con una segunda validación de autentificación.

- Se debe administrar y monitorear continuamente el uso operacional de puertos, protocolos y servicios tanto en dispositivos de red como en servidores y plataformas para minimizar los riesgos de seguridad.

- La administración de la red deberá ser complementada con un sistema de cortafuegos actualizado. La configuración del cortafuego y otros dispositivos, no debe ser la configuración de fábrica de los dispositivos, sino que se debe adaptar a los requerimientos específicos del MOP.

Seguridad en la operación

Seguridad en las Operaciones, tiene como objetivo asegurar la continuidad operativa de los sistemas, que permita asegurar los medios de procesamiento, almacenamiento y transmisión de los activos de información, a través de la creación de procedimientos y definición de responsabilidades operacionales.

Se debe definir procedimientos de operación y responsabilidades que aseguren el correcto acceso al Datacenter.

Procedimientos de operación documentados. Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.

Gestión de cambios: Se deben controlar los cambios en los sistemas de la institución tales como; procesos de negocio, instalaciones de procesamiento de información y los sistemas.

Gestión de la capacidad: Se debe supervisar y ajustar el uso de los recursos, y realizar proyecciones de los requisitos futuros de capacidad para asegurar el desempeño requerido de las aplicaciones.

Separación de los ambientes de desarrollo, prueba y operacionales: Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.

Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.

Se deben cumplir los controles contra código malicioso con la adopción de controles de detección, prevención y recuperación, junto con los procedimientos adecuados para concientizar a los usuarios.

Se debe proteger la información definida como activos críticos, contra de la pérdida de datos.

Se deben hacer copias de respaldo, pruebas de recuperación de la información y/o softwares.

Se deben realizar pruebas de recuperación de imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada y planes de recuperación ante desastres.

Seguridad en el acceso de la información

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 de información.

Restringir el acceso a la información y a las instalaciones de procesamiento de información.

Definición de la política de control de acceso, para aquello se debe establecer, documentar y revisar la política de control de acceso que cumpla con los requisitos del negocio y de seguridad de la información.

Accesos a las redes y a los servicios de la red, los usuarios solo deben tener acceso directo a la red y a los accesos que específicamente son autorizados.

Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.

Las redes se deben gestionar y controlar, para proteger la información en los sistemas y aplicaciones.

Segmentación de las redes: se deben crear grupos de servicios de información con usuarios y sistemas, según criticidad.

Se debe mantener la seguridad de la información transferida dentro del MOP y con entidades externas.

Definir las políticas, procedimientos y controles de transferencia que deben estar protegidos.

Acuerdos sobre transferencia de información: Los acuerdos deben abarcar la transferencia segura de la información del negocio entre el MOP y terceros.

Mensajería electrónica: La información involucrada en la mensajería electrónica debe ser protegida de forma apropiada.

Acuerdos de confidencialidad o no divulgación: se debe identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización.

Seguridad en la adquisición, desarrollo y mantención de sistemas

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 externo.

- Control de acceso al sistema y aplicaciones tiene como objetivo evitar el acceso sin autorización a los sistemas.

- Restricción de acceso a la información: se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.

- Procedimientos de inicio de sesión seguro: Se debe definir el acceso a los sistemas y aplicaciones debe forma controlada con un control de inicio de sesión seguro.

- Control de gestión de contraseñas: deben ser interactivos y asegurar la complejidad de contraseñas.

- Se debe restringir y controlar estrictamente el uso de programas utilitarios capaces de anular los controles del sistema y de la aplicación.

- Control de acceso al código fuente de los programas: Se debe restringir el acceso al código fuente de los programas y asegurar mantener la última versión disponible.

- Todo desarrollo debe garantizar la confidencialidad de la información en la adquisición, desarrollo y mantenimiento del sistema.

- Requisitos de seguridad de los sistemas de información: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto incluye los sistemas que proporcionan servicios en las redes públicas.

- Los requisitos relacionados a la seguridad de la información, deben ser incluidos en los proyectos de modernización o mejoras para los sistemas de información existentes.

- Aseguramiento de servicios de aplicación en redes públicas. La información relacionada a servicios de aplicación que se trasmiten por redes públicas debe ser protegido de actividades fraudulentas, disputas contractuales, su divulgación y modificación no autorizada.

- Protección de las transacciones de servicios de aplicación. La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada.

- Seguridad en procesos de desarrollo y soporte: se debe asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información Seguro.

- Definición de Política de desarrollo seguro: Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a todos los desarrollos realizados en el MOP.

- Todo procedimiento de control de cambios del sistema debe ser controlado mediante el uso de control de cambio formal y documentación.

- Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación. Es decir, cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.

- Restricciones en los cambios a los paquetes de software: Se debe controlar la realización de modificaciones a los paquetes de software, bajo la limitación de cambios necesarios para la operación, los que deben ser controlados de manera estricta.

- Principios de ingeniería de sistema seguro: Se debe establecer, documentar, mantener y aplicar los principios de ingeniería de sistemas seguros para todos los esfuerzos de implementación del sistema de información.

- Desarrollo tercerizado: La institución debe supervisar y monitorear la actividad del desarrollo del sistema contratado externamente, validando el cumplimiento de todas las normativas definidas para el cumplimiento de la seguridad de la información.

- Prueba de seguridad del sistema, durante el desarrollo se deben realizar pruebas de funcionalidad de la seguridad, para cumplir se debe contar con ambiente de pruebas, para garantizar el cumplimiento de las políticas de seguridad de la información.

- Prueba de aprobación del sistema: Se debe establecer el plan de pruebas, que conlleva a la aceptación de los sistemas, que cumplan con las políticas de seguridad de la información.

Seguridad en Criptografía de la Información.

La criptografía corresponde a la capacidad de resguardar los datos reales como técnica para proteger documentos. En este sentido, se establece como requisito, disponer de los siguientes controles criptográficos:

- Asegurar el uso adecuado y eficaz de la criptografía para proteger la **confidencialidad, autenticidad o integridad de la información.**

- Se debe desarrollar e implementar la política sobre el uso de controles criptográficos para la protección de la información.

- Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante todo su ciclo de vida

Gestión de activos de la información

La gestión de activos de la información define que es de obligación implementar un sistema SGSI, que permite mantener una apropiada protección de los activos de información.

Todos los activos deben ser inventariados, clasificados y contar con un dueño identificado.

La información u otros activos asociados a la información, deben ser identificados e inventariados.

Todo el personal del MOP debe resguardar los activos pertenecientes a la institución que contengan información del MOP.

La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para prevenir la divulgación o modificación sin autorización por el responsable.

Se deben desarrollar e implementar los procedimientos, para el manejo de activos, de acuerdo al esquema de clasificación adoptado por la institución.

Se debe prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de acceso a los datos., tales como; discos extraíbles, discos compartidos, discos físicos u otros medios.

Se deben implementar los procedimientos para la gestión de los medios extraíbles, de acuerdo al esquema de clasificación adoptado por la organización.

Gestión de Equipamientos

En la Gestión de equipamientos, se debe prevenir pérdidas, daños, o hurtos de los activos, que atenten con las actividades de la institución, además conocer la ubicación del equipamiento.

El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales.

Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por elementos de operación

Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información.

El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.

Todo equipo al ingresar a la red del MOP, debe estar securitizado de acuerdo a las normas, políticas y procedimientos vigentes de Seguridad de la Información y ciberseguridad del MOP.

Está prohibido extraer información o softwares de la institución sin previa autorización, o redirigir información a cuentas personales.

Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de las instalaciones en el MOP.

En la reasignación de equipamiento, todos los elementos de almacenamiento, deben ser revisados para asegurar que todos los datos sensibles se hayan borrado antes de su descarte o reutilización.

Los usuarios son los responsables de que los equipos desatendidos, sin accesos a red MOP, se les otorgue protección apropiada y actualizada.

Gestión de incidentes de seguridad

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.

Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información e incluir una comunicación sobre eventos de seguridad y debilidades.

Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.

Informe de eventos de seguridad de la información: se debe informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados.

Informe de las debilidades de seguridad de la información: se debe requerir que el personal y contratistas del MOP que utilicen los sistemas de información de la institución, adviertan e informen cualquier debilidad en la seguridad de la información de los sistemas o anomalías.

Evaluación y decisión sobre los eventos de seguridad de la información. Los eventos de seguridad de la información se deben evaluar y decidir si cumplen o no como incidente.

Respuesta ante incidentes de seguridad de la información. Los incidentes de seguridad de la información deben ser atendidos de acuerdo con los protocolos establecidos.

Aprendizaje de los incidentes de seguridad de la información, se debe utilizar el conocimiento adquirido a resolver el incidente de seguridad de la información, para reducir la probabilidad e impacto de incidentes futuros.

Recolección de evidencia. La institución debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda ser útil de evidencia.

Gestión de continuidad de la Seguridad de la Información

Contar con planes de contingencia, para contrarrestar las interrupciones en los procesos críticos asociados a fallas significativas o desastres que afecten a los activos de información

Continuidad de la seguridad de la información: se debe Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del MOP.

Planificación de la continuidad de la seguridad de la información. El MOP debe determinar los requisitos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas durante (una crisis o desastre)

Implementación de la continuidad de la seguridad de la información. El MOP debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

El MOP debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas.

Establecer redundancia en la disponibilidad de las instalaciones de procesamiento de la información (Datacenter).

Disponibilidad de las instalaciones de procesamiento de la información. Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad.

Gestión del Proveedor Externo.

Seguridad de la información en las relaciones los proveedores externos: Se debe asegurar la protección de los activos del MOP, al que tienen acceso los proveedores externos.

Se debe acordar con los proveedores los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso a los activos del MOP.

Abordar la seguridad dentro de los acuerdos con el proveedor: se deben establecer todos los requisitos de seguridad de la información pertinente, definidos y acordados con cada proveedor que pueda **acceder, procesar, almacenar, comunicar**, proporcionar componentes de infraestructura de TIC para la información de la organización.

Los acuerdos con los proveedores deben incluir en todos los procesos de adquisición de compras públicas, los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información, las comunicaciones y la cadena de suministro del producto.

Gestión de Acceso

Asegurar el acceso de usuarios autorizados evitando el acceso sin autorización a los sistemas y servicios

Asegurar el registro de alta y baja de usuarios, se debe implementar control de alta y baja de usuario para restringir el acceso a la información de la institución.

Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios.

Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.

Se debe controlar la asignación de información de privilegio confidencial mediante un proceso de gestión formal.

Los propietarios de activos críticos, deben revisar los derechos de acceso de los usuarios de forma periódica.

Se deben retirar los derechos de acceso a la información para todo el personal del MOP y usuarios externos, también a las instalaciones de procesamiento de información y dependencias del MOP, una vez que termine la relación laboral, contrato o acuerdo.

Gestión de cumplimiento normativo

El incumplimiento de la Política de Seguridad de la Información, será sancionado en conformidad a las disposiciones administrativas internas. Lo anterior, sin perjuicio de la responsabilidad civil o penal que corresponda u otras normativas pertinentes.

Auditorías

El MOP, debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información del sistema de gestión de la seguridad de la información que detalla lo siguiente:

Se debe cumplir con la planificación, establecer, implementar y mantener uno o varios programas de auditoría, que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Los programas de auditoria deben considerar la importancia de los procesos involucrados y los resultados de las auditorías anteriores.

Se debe definir los criterios de auditoría y el alcance.

Seleccionar los auditores y llevar a cabo las auditorías que aseguren la objetividad e imparcialidad del proceso de auditoría,

Asegurar que los resultados de las auditorías, se informen a la Dirección pertinente.

Conservar la información documentada, como evidencia de los programas de auditoría y los resultados de la auditoría.

Se debe asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos del MOP.

Revisión independiente de la seguridad de la información como enfoque de la institución para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información). Se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos.

Cumplimiento con las políticas y normas de seguridad de control. El comité de seguridad de la información, debe revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.

Verificación del cumplimiento técnico como control. Se debe verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la institución.

Evaluación

El comité de Seguridad de la Información, tiene como objetivo otorgar seguimiento, medición, análisis, evaluación de la institución en ámbitos de seguridad de la información, con mecanismos de evaluación del desempeño y la eficacia del sistema de gestión de la seguridad de la información con las siguientes definiciones:

- Seguimiento, medición, análisis y evaluación.
- Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles.

- Auditoría interna.
- Planificar y realizar una auditoría interna del SGSI.
- Revisión por la respectiva Dirección.
- La administración realiza una revisión periódica del SGSI.

Mejora Continua

El comité de seguridad de la información, debe establecer un plan de mejoras de manera continua en base a la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información, con los siguientes criterios:

- No conformidad y acciones correctivas.
- Identificar y corregir ante no conformidades en cambios de la política, para evitar su recurrencia documentando todas las acciones.
- Mejora continua de los dominios del SGSI.
- Mejora continua en los Controles del SGSI.
- Mejora continua en la auditoria del SGSI.
- Mejora continua de la Gestión del SGSI.

Metodología de Control Gestión de la Seguridad

Definición de estándar como objetivo de control, referencia ISO/IEC 27002:2022 mención objetivos de control y controles

Metodología de Gestión de Riesgos

La ISO 27005, establece lineamientos para a gestión de riesgos relacionados con la seguridad de la información, establece cuatro pasos fundamentales para la implementación de la misma:

- Establecer el contexto.
- Identificación de los riesgos relacionados con seguridad de la información.
- Análisis.
- Evaluación.

Al respecto también es importante tener en cuenta en el caso de los riesgos de seguridad de la información, se debe establecer un inventario y clasificación de activos de la información que se integran posteriormente a la gestión de los riesgos. Los criterios para clasificación del riesgo son los siguientes criterios: **Inicial, Repetible, Definido, Gestionado, Optimizado.**

CUMPLIMIENTO

Definición de cumplimiento con los requisitos legales y contractuales.

Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.

Identificación de la legislación vigente y los requisitos contractuales.

Todos los requisitos legales, estatutarios, regulatorios y contractuales pertinentes y el enfoque del MOP para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.

Derechos de propiedad intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados.

Se debe proteger la información contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legales, regulatorios, contractuales aplicables al MOP.

Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y demás regulaciones pertinentes.

DIFUSION DE POLITICA

La política general de seguridad de la información es susceptible de mejorar continuamente, por lo tanto, es factible de someter a modificaciones, actualizaciones, cambios periódicos, que permitan mantenerla actualizada y vigente.

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.gob.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, en consecuencia, sancionada.

Las personas que trabajen bajo el control del MOP, deben tomar conciencia de:

a) La política de seguridad de la información;

b) Su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de una mejora del desempeño de la seguridad de la información;

c) Las implicaciones del incumplimiento de los requisitos del sistema de gestión de la seguridad de la información.

CONTROL VERSIONES

Control de versiones es la información documentada requerida por el sistema de gestión de la seguridad de la información y por esta debe ser controlada para asegurarse de que esté disponible y sea idónea para su uso, donde y cuando se necesite, está protegida adecuadamente contra pérdida de confidencialidad, uso inapropiado o pérdida de integridad.

Revisor	*Versión*	*Modificación*	*Fecha de Revisión*	*Firma*
Rodrigo Venegas Ruiz	***1.0***	***Versión Inicial***	***31/01/2023***	
Natalia Kent Geell	***1.0***	***Versión Inicial***	***31/01/2023***	
Elia Puentes Garrido	***1.0***	***Versión Inicial***	***31/01/2023***	
Luis Guerrero Jorquera	***1.0***	***Versión Inicial***	***31/01/2023***	
Manuel Echeverría Valencia	***1.0***	***Versión Inicial***	***31/01/2023***	
Pablo Cornejo Campos	***1.0***	***Versión Inicial***	***31/01/2023***	
Carlos Soto Bascur	***1.0***	***Versión Inicial***	***31/01/2023***	

4. **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 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, y a los Encargados de Titular y Suplente de Seguridad de la Información, de esta Subsecretaría, e infórmese a través del Intranet institucional.

SUBSECRETARIO DE OBRAS PÚBLICAS

VALERIA BRUHN CRUZ
Subsecretaria de Obras Públicas
Subrogante

V°B° SDP JEFA GABINETE

V°B° SDP JEFE(A) JURIDICO GABINETE

N° Proceso: 16717152