

3082

ORD.: N° _____/

ANT.: Decreto Supremo (Ministerio
Secretaría General de la
Presidencia) N°83, de fecha 3
de junio del 2004.
Política General de Seguridad
de la Información – MOP.

MAT.: Informa Política General de
Seguridad de la Información –
MOP.

SANTIAGO, 12 DIC. 2011

**DE : LORETO SILVA ROJAS
SUBSECRETARIA DE OBRAS PÚBLICAS**

A : SEGÚN DISTRIBUCIÓN

1. INTRODUCCIÓN

El presente documento de Política General de Seguridad de la Información, establece el marco de referencia a través del cual el Ministerio de Obras Públicas (MOP) y sus Servicios dependientes, implementarán el Sistema de Gestión de Seguridad de la Información Ministerial (SGSI), fijando así los estándares de seguridad de la información a aplicar para proteger adecuadamente sus activos de información. Ello según lo establecen el Decreto Supremo N°83 del 3 de Junio del 2004 (DS83), la norma NCh-ISO 27001 Of.2009 y la Ley 20.285 de Transparencia, y donde se han considerando los siguientes elementos centrales:

- La disponibilidad, integridad, confidencialidad, legalidad y confiabilidad de la información.
- La implementación, mantención, monitoreo y mejoramiento continuo de la aplicación de la presente política.
- Los procedimientos para asegurar la continuidad del negocio.
- La detección y la comunicación oportuna de vulnerabilidades y eventos de riesgos que afecten a los activos de información.
- El acceso amplio, pero controlado a los activos de información.
- La operación correcta y segura de las instalaciones de procesamiento de información.
- La seguridad física y del entorno donde se encuentran y operan los activos de información.


FRANCISCO JAVIER ESPINOZA SANHUEZA

Abogado

Almirante 59, piso 6, Santiago | Chile
Teléfono (56-2) 449 3931 | 449 3032
www.dgop.cl | www.mop.cl

[Handwritten mark]

- Los roles, responsabilidades y competencias de los funcionarios del MOP que tengan relación con activos de información.
- La identificación de los responsables de la seguridad de los activos de información.
- La relación con los proveedores y usuarios externos.

La protección de los activos de información y de la tecnología para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, es una responsabilidad de todos y cada uno de los Funcionarios del MOP, 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.

2. DECLARACIONES INSTITUCIONALES

Misión

Recuperar, fortalecer y avanzar en la provisión y gestión de obras y servicios de infraestructura para la conectividad, la protección del territorio y las personas, la edificación pública y el aprovechamiento óptimo de los recursos hídricos; asegurando la provisión y cuidado de los recursos hídricos y del medio ambiente, para contribuir en el desarrollo económico, social y cultural, promoviendo la equidad, calidad de vida e igualdad de oportunidades de las personas.

Objetivos Estratégicos

- Impulsar desarrollo económico del país a través de la infraestructura, con visión territorial integradora.
- Impulsar el desarrollo social y cultural a través de la infraestructura, mejorando la calidad de vida de las personas.
- Contribuir a la gestión sustentable del medioambiente, del recurso hídrico y de los ecosistemas.
- Alcanzar el nivel de eficiencia definido en el uso de los recursos.
- Desarrollar una gestión ministerial eficiente, eficaz, con transparencia, excelencia técnica, innovación y cercana a la ciudadanía.
- Proveer y mantener obras y servicios de infraestructura y de regulación hídrica, de calidad, con oportunidad y sustentabilidad.

Productos Estratégicos

- Planes de inversión elaborados con un enfoque territorial, participativo y de responsabilidad medioambiental.
- Servicios de Infraestructura Pública de Transporte vial, aeroportuario y de conectividad portuaria marítima, fluvial y lacustre.

- Servicios de Infraestructura Pública de Recursos Hídricos
- Servicios de Infraestructura de Edificación y Espacios Públicos para mejorar la calidad de vida.
- Gestión de Recursos Hídricos.

Valores

- Sentido de misión y amor por Chile
- Transparencia en nuestra gestión
- Excelencia en nuestro quehacer
- Sintonía para trabajar en equipo

Estrategia de Implantación del SGSI para el MOP

Para apoyar el cumplimiento de los objetivos estratégicos declarados por el MOP, se requiere incorporar políticas, normas y procedimientos para la seguridad de la información, y la sujeción a estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información. Por ello es necesario que se cumplan las normativas que se dicten y estén vigentes a través de la implantación de un Sistema de Seguridad de la Información único, orientado al resguardo de los activos de información. Las directrices y alcances contenidos en este documento 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 que el MOP requiera.

Política de Seguridad de la Información MOP

"El MOP y sus Servicios dependientes se comprometen a gestionar la seguridad de la información como un proceso continuo en el tiempo, manteniendo un sistema único de seguridad de la información ministerial, basado en la norma NCh – ISO 27001, y en cumplimiento con lo establecido en el D.S N° 83, de 2004, tendiente a homogeneizar los criterios de seguridad.

Se declara la absoluta relevancia de la seguridad de la información para su quehacer diario, protegiendo los activos de la información y su infraestructura de soporte para garantizar un alto nivel de continuidad operativa de los procesos de negocio del MOP y de sus Servicios dependientes contribuyendo al cumplimiento de su misión y de sus objetivos estratégicos."

3. OBJETIVOS DE LA GESTION DE LA SEGURIDAD DE LA INFORMACION

- Proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad de los

procesos de negocio del Ministerio de Obras Públicas.

- Identificar y clasificar los activos de información de la Institución para la operación y continuidad del negocio, considerando la Matriz de Riesgo.
- Detectar, eliminar o mitigar las vulnerabilidades y los riesgos que amenacen los activos de información que afecten la operación y continuidad del negocio.
- Establecer políticas, normas, procedimientos o instructivos para la manipulación, uso y resguardo adecuado de los activos de información.
- Difundir la Política de Seguridad de la Información y capacitar a todos los funcionarios del MOP sobre los alcances y buenas prácticas que se establezcan en relación al resguardo de los activos de información y las tecnologías para su procesamiento.
- Establecer los mecanismos de auditoría y control de los activos de información y tecnologías de procesamiento.

4. ALCANCE DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

La Política General de Seguridad de la Información Ministerial es única y será aplicada por todos sus Servicios dependientes. Los Servicios dependientes del MOP incluidos en el alcance de esta política son:

- Subsecretaría de Obras Públicas
- Dirección General de Obras Públicas
- Dirección General de Aguas
- Dirección de Aeropuertos
- Dirección de Arquitectura
- Dirección de Contabilidad y Finanzas
- Fiscalía
- Dirección de Obras Hidráulicas
- Dirección de Obras Portuarias
- Dirección de Planeamiento
- Dirección de Vialidad
- Coordinación de Concesiones de Obras Públicas

Esta política general aplica y es extensible a todo el personal de los Servicios dependientes del MOP y debe ser conocida y cumplida por todos sus funcionarios, ya sea Planta, Contrata u Honorarios a nivel nacional y por el personal externo que presten servicios permanentes o temporalmente.

Se establece que la difusión de la Política de Seguridad de la

Información es responsabilidad de los Directores de cada Servicio dependiente del Ministerio de Obras Públicas. Los mecanismos de difusión a emplear, a lo menos deben considerar la publicación en los espacios de Intranet de cada Servicio y el envío semestral de correos electrónicos a los funcionarios con el contenido de las políticas vigentes.

Esta política general aplica sobre toda la información propia o administrada por el MOP y sus Servicios dependientes, considerando toda forma de soporte, almacenamiento, transporte y/o transmisión, sea en formato físico, electrónico, virtual o cualquier otro tipo de formato.

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 2 años, al menos, esta política será sometida a revisión.

5. COMPONENTES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MOP

La política general de seguridad de la información del MOP estará complementada por políticas específicas acordes con los dominios de seguridad que establece el DS 83 y la Norma NCH 27.001.

Estas políticas específicas se generarán como consecuencia de las revisiones realizadas a los procesos operacionales en uso, como resultado de análisis de riesgo, como respuesta ante incidentes que afecten la seguridad o por la revisión periódica de las políticas vigentes. En todo caso, cualquiera sea el origen de la necesidad de implantar una nueva política ésta debe ser planteada al Comité de Seguridad de la Información del MOP, quien finalmente aprueba o rechaza la política.

Políticas Específicas por Dominio

- **Política de la organización de la seguridad de información**

Establecer un marco referencial a nivel directivo para la implementación del sistema de la seguridad de la información para el MOP.

- **Política de gestión de los activos**

Implementar y mantener una apropiada protección de los activos de información institucionales. Todos los activos deben ser inventariados, catalogados y contar con un responsable identificado.

- **Política de seguridad de los recursos humanos**

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. También debe considerar la capacitación regular de éstos.

- **Política de seguridad física y del ambiente**

Prevenir el acceso no autorizado, daño, interferencia, eventos, o causas de índole ambiental que afecten negativamente los activos de información.

- **Política de gestión de las comunicaciones y 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.

- **Política de control de acceso**

Asegurar que el acceso del usuario es 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.

- **Política de adquisición, desarrollo y mantenimiento 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.

- **Política de 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.

- **Política de gestión de la continuidad del negocio**

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.

- **Política de cumplimiento de las normativas legales y técnicas y de las oportunidades de mejoras resultantes de las auditorías.**

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. ROLES Y RESPONSABILIDADES

Para cumplir los objetivos de la Política de Seguridad de la Información del MOP se establecen los siguientes roles y responsabilidades:

Subsecretaria (o) de Obras Públicas

Responsable de aprobar la política y sus futuras modificaciones con la asesoría del Comité de Seguridad de la Información del MOP.

Jefes (as) de Servicio

Son responsables de la aplicación de las políticas de seguridad de la información al interior de cada Servicios, así como del cumplimiento de dicha política por parte de sus funcionarios.

Comité de Seguridad de la Información MOP

El Comité de Seguridad de la Información del MOP, es un cuerpo integrado por representantes de los Servicios Transversales del Ministerio, destinado a asegurar la implantación del Sistema de Gestión del Sistema de Seguridad de la Información en el MOP. Se constituyó a través de la Resolución Exenta N° 1665 del 31 de Mayo del 2011 de la Subsecretaría de Obras Públicas.

Las funciones más relevantes son proponer, impulsar, promover y revisar periódicamente las políticas de seguridad de la información del MOP.

Oficial de Seguridad de la Información MOP

Corresponde al cargo/persona del Ministerio que cumple la función de supervisar el cumplimiento de la presente política y de asesorar en materia de seguridad de la información a las autoridades Ministeriales y a los integrantes del Comité de Seguridad de la Información y de coordinar y asesorar a los encargados de seguridad de la información de los Servicios MOP. Sus funciones principales corresponden a liderar el establecimiento, implementación y mantenimiento de un sistema de gestión de seguridad de los activos de información y tecnologías de procesamiento.

9.

Encargado (a) de Seguridad de la Información de los Servicios

Corresponde al cargo/persona de cada Servicio dependiente del Ministerio, que cumple la función de supervisar y coordinar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los Jefes de Servicio.

Subdirección de Informática y Telecomunicaciones (SDIT)

Responsable de las adquisiciones, desarrollo y mantenimiento de los sistemas de registro, procesamiento e información, procesamiento telecomunicaciones e informática transversales del Ministerio de Obras en cumplimiento de la Resolución N°120 de 23-01-2003.

Unidad de Auditoría Ministerial/Auditoría Interna Servicios MOP

Responsable de practicar auditorías sobre el cumplimiento de las especificaciones, medidas de seguridad de la información establecidas por esta política, las normas, procedimientos y prácticas que de ella surjan, debiendo informar al Ministro, al Comité de Seguridad de la Información o al Jefe de Servicio según corresponda.

Usuarios (as)

Son las personas que usan los activos 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 y además tienen la obligación de reportar incidentes de seguridad.

7. GLOSARIO DE TÉRMINOS

Activo de Información

Sistemas de información, aplicaciones o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información considerada relevante para los procesos de negocio del Ministerio de Obras Públicas o sus Servicios dependientes.

Administración de Riesgos

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo

aceptable, de los riesgos de seguridad que podrían afectar a los activos información.

Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

Evento de seguridad de la información.

Ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de la seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser pertinente a la seguridad.

Incidente de Seguridad

Un incidente de seguridad es uno o varios eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

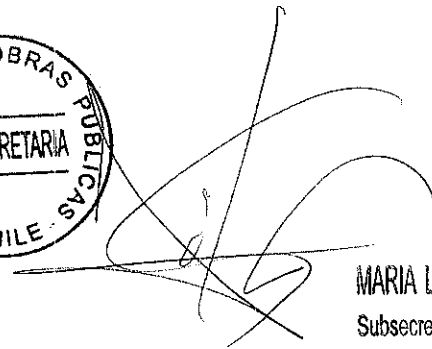
Seguridad de los Activos de Información

Es proteger, resguardar y asegurar la disponibilidad, privacidad, confidencialidad e integridad de los activos de información y tecnologías para su procesamiento a efecto de garantizar la continuidad operacional de la institución.

Sin otro particular, saluda atentamente a Ustedes.



Gino Curotto Godoy
Jefe División
Subdirección General de Obras Públicas
Dirección General de Obras Públicas



MARIA LORETO SILVA ROJAS
Subsecretaria de Obras Públicas

GCG/CGG/ DISTRIBUCIÓN:

- Sra. Luz Granier - Jefa de Gabinete Sr. Ministro de OO.PP.
- Sr. José Manuel Mondaca - Jefe de Gabinete SS.OO.PP.
- Sra. Jimena López - Jefa de Gabinete DGOP.
- Sr. Marcelo Robles - Fiscal MOP.
- Sr. Matias Desmadryl - Director General de Aguas.
- Sr. Fernando Prat - Director General de Obras Públicas.
- Sr. Alejandro Sepúlveda - Director Nacional de Arquitectura.
- Sra. María Isabel Castillo - Directora Nacional de Aeropuerto.
- Sra. Vivien Villagran - Directora Nacional de Planeamiento.
- Sr. Mario Fernández /Director Nacional de Vialidad.
- Sra. Mariana Concha - Directora Nacional de Obras Hidráulicas.
- Sr. Ricardo Tejada - Directora Nacional de Obras Portuarias.
- Sra. Patricia Contreras - Director Nacional de Contabilidad y Finanzas.
- Sr. Emilio Pellegrini - Coordinador de Concesiones de Obras Públicas.

Proceso N° 53382291