POLÍTICA DE GESTIÓN DE LAS OPERACIONES Y LAS COMUNICACIONES

Versión 1.0

MINISTERIO DE OBRAS PÚBLICAS

ELABORADO POR:	REVISADO POR:	APROBADO:
Dirección General de Obras Públicas **FECHA: 9/09/2012**	Jefe Subdirección de Informática y Telecomunicaciones Oficial de Seguridad Información MOP **FECHA: 14/11/2012**	Comité de Seguridad de la Información **FECHA: 11/12/2012**

Índice

1. Introducción 5
2. Objetivo General 5
3. Objetivos Específicos 5
4. Alcance 5
5. Destinatarios 6
6. Política de Gestión de las Operaciones y las Comunicaciones 6
6.1. Responsabilidades 6
6.2. Procesos Operacionales 8
6.3 Gestión delncidentes 9
6.4. Separación (segregación) de Funciones 9
6.5. Separación de ambientes 9
6.6. Monitoreo de capacidad instalada 9
6.7. Criterios de aceptación de sistemas 10
6.8. Protección contra software malicioso 10
6.9. Procedimiento de respaldo y restauración de sistemas y servicios 10
6.10. Administración de la Red de Datos 11
6.11. Administración y seguridad de los medios removibles 12
6.12. Procedimientos administración de la información relativa a la plataforma TI 12
6.13. Intercambios de información o software con otras entidades 12
7. Encargados de provisión de Servicios de Operaciones y Telecomunicaciones en Direcciones dependientes del MOP 16
8. Difusión de la política de seguridad de recursos humanos 16
GLOSARIO DE TÉRMINOS 17

Control de Versión

REVISIÓN	Numeral del procedimiento	MODIFICACIÓN REALIZADA	Nombre y Firma de quien autoriza	FECHA DEL CAMBIO

1. Introducción

La presente política de gestión de las operaciones y las comunicaciones (la "**Política**"), se enmarca dentro de la Política General de Seguridad de la Información para el Ministerio de Obras Públicas ("**MOP**"), contenida en el ORD N° 3082 del 12 de diciembre del 2011, y de las recomendaciones de seguridad dadas en el Decreto Supremo MINSEGPRES N° 83 (**"DS 83**"), de 3 de junio del 2004.

En particular este documento, junto con la norma respectiva, define el objetivo y alcance de la Política de Gestión de la Operación y las Comunicaciones de la Plataforma Tecnológica del MOP.

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 de información y de los servicios de información que la componen, asegurando continuidad operacional y el adecuado resguardo de sus activos de información.

3. Objetivos Específicos

Los objetivos específicos de esta Política incluyen asegurar el correcto funcionamiento de la plataforma tecnológica del MOP y establecer las responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas (soporte, mantención, configuración), procedimientos para la respuesta a incidentes y separación de funciones y, finalmente, asegurar sus activos, en términos de preservar la confidencialidad, integridad y disponibilidad de éstos.

4. Alcance

El alcance de esta Política, se extiende a toda la plataforma tecnológica del MOP, independiente de quién sea el administrador de ésta. 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).

5. Destinatarios

Son destinatarios de esta Política, todos los funcionarios, independiente de su modalidad de contratación, así como el personal de empresas de servicios que sean responsables de la operación y administración de las telecomunicaciones y operación de la plataforma tecnológica del MOP.

6. Política de Gestión de la Operación y las Comunicaciones

6.1. Responsabilidades

Jefe Subdirección de Informática y Telecomunicaciones

La responsabilidad de la seguridad de las tecnologías de la información y comunicaciones del Ministerio de Obras Públicas, le corresponde al Jefe de la Subdirección de Informática y Telecomunicaciones. En particular, están dentro de su ámbito de responsabilidades las siguientes:

6.1.1. 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.

6.1.2. Velar y ser responsable, por la seguridad de los sistemas de información (seguridad informática) del MOP, en conjunto con la Unidad de Seguridad de la Información.

6.1.3. Informar por escrito y en forma oportuna, a todos los proveedores de servicios externos, respecto de cambios en los responsables de la Subdirección de Informática y Telecomunicaciones relacionados con la gestión y administración de los servicios contratados.

Jefe Unidad de Seguridad de la Información

En particular, están dentro de su ámbito de responsabilidades las siguientes:

6.1.4. Revisar y evaluar los contratos de servicio o interoperación con terceros, para asegurar la incorporación de cláusulas relativas a la seguridad de la información.

6.1.5. Evaluar el riesgo e impacto operativo que implican todos los cambios y/o mantenciones proyectadas, que involucren los sistemas y servicios de información y telecomunicaciones, administrados en forma directa o a través de terceros.

6.1.6. Revisar regularmente los registros relativos a los procedimientos operativos emanados de la ejecución de las tareas operativas de la Unidad de Operaciones y de la Unidad de Telecomunicaciones.

Jefe Unidad de Operaciones

Están dentro de su ámbito de responsabilidades las siguientes:

6.1.7. Implementar ambientes que sean independientes entre sí para el procesamiento de datos de: producción, pre producción (pruebas) y construcción.

6.1.8. Elaborar procedimientos para asegurar el registro de las actividades realizadas por el personal operativo, para su revisión y fiscalización periódica.

6.1.9. Elaborar normas y procedimientos para comunicar y clasificar eventuales fallas o errores durante la ejecución de tareas operativas.

6.1.10. Definir e implementar procedimientos para la administración de información y documentación relativa a la arquitectura, configuración y operación de la plataforma tecnológica del MOP.

6.1.11. Asegurar la continuidad operacional de los servicios de procesamientos de datos alojados en el Datacenter Ministerial.

6.1.12. Gestionar de manera preventiva los riesgos institucionales asociados a la implementación de tecnologías de la información.

6.1.13. Evaluar regularmente la capacidad instalada a efecto de prevenir discontinuidad operacional.

6.1.14. Velar por el cumplimiento de la normativa legal respecto de la seguridad de la información (integridad y confidencialidad) y su soporte tecnológico.

Jefe Unidad de Telecomunicaciones

En particular, están dentro de su ámbito de responsabilidades las siguientes:

6.1.15. Elaborar procedimientos para asegurar el registro de las actividades realizadas por el personal operativo, para su revisión y fiscalización periódica.

6.1.16. Gestionar de manera preventiva los riesgos institucionales asociados a la implementación de tecnologías de telecomunicaciones.

6.1.17. Elaborar procedimientos para comunicar y clasificar eventuales fallas o errores durante la ejecución de tareas operativas.

6.1.18. Definir e implementar procedimientos para la administración de información y documentación relativa a la arquitectura, configuración y operación de la plataforma tecnológica del MOP.

6.1.19. Asegurar la continuidad operacional de los servicios de telecomunicaciones alojados en el Datacenter Ministerial.

6.1.20. Evaluar regularmente la capacidad instalada, a efecto de prevenir la discontinuidad operacional.

6.1.21. Velar por el cumplimiento de la normativa legal respecto de la seguridad de la información (integridad y confidencialidad) y su soporte tecnológico.

Jefe Unidad de Servicios de Usuarios

En particular, están dentro de su ámbito de responsabilidades la siguiente:

6.1.22. 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.

6.2. Procesos Operacionales

6.2.1. Se debe contar con procedimientos debidamente documentados para los procesos en que se sustentan los productos y servicios emanados desde las unidades de Operaciones, Telecomunicaciones y Soporte de Usuarios, que describan las actividades y tareas que deben ejecutarse para la obtención de éstos.

6.2.2. Se debe contar con procedimientos debidamente documentados, para los controles de cambios en las configuraciones.

6.2.3. Se debe contar con procedimientos debidamente documentados, para 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.

6.2.4. Se debe contar con procedimientos debidamente documentados, para la administración y gestión de los servicios proporcionados por proveedores externos al MOP.

6.2.5. 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.

6.3. Gestión de Incidentes

6.3.1. En caso de detectar uno o más incidentes que afecten la seguridad de la plataforma tecnológica del MOP, cada uno de los responsables operativos de la misma, deberán reportarlo según lo establece la Política de Gestión de Incidentes. En caso de que el o los incidente estén dentro del ámbito de la operación y las telecomunicaciones, se debe proceder a su atención.

6.3.2. Se debe contar con procedimientos, debidamente documentados, para el registro de fallas.

6.4. Separación (segregación) de Funciones

6.4.1. Las funciones de operación o ejecución de tareas relacionadas con los servicios de operaciones y telecomunicaciones, deberán, en la medida de lo posible, ser ejecutadas por diversas 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.

6.5. Separación de ambientes

6.5.1. Los ambientes de producción, pre producción (pruebas) y construcción, deben estar separados, preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software entre éstos.

6.6. Monitoreo de capacidad instalada

6.6.1. 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.

6.6.2. 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.

6.7. Criterios de aceptación de sistemas

6.7.1. El Jefe de la Subdirección de Informática y Telecomunicaciones, en conjunto con los Jefes de las Unidades de "Operaciones", "Desarrollo y "Mantención de Sistemas de Información" y 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.

6.8. Protección contra software malicioso

6.8.1. El Jefe de la Unidad de Seguridad de la Información y de la Unidad de Operaciones, deberán definir e implementar los controles de prevención y detección de software no autorizado, o que revista riesgo para la plataforma tecnológica del MOP (software malicioso).

6.9. Procedimiento de respaldo y restauración de sistemas y servicios

6.9.1. El jefe de la Unidad de Seguridad de la Información y de la Unidad de Operaciones, 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.

6.9.2. En caso de detectarse problemas, errores y/o fallas en estos procesos de respaldo, señalados en el numeral anterior, se deberá revisar el proceso por quien corresponda, así también las posibles causas que originaron el problema, y deberán implementarse las medidas necesarias para corregir o evitar su reiteración. En caso de que dichas medidas no sean factibles de ser ejecutadas, se deberá llevar a cabo acciones alternativas para cumplir con el objetivo de contar con respaldos confiables de los sistemas, servicios y datos.

6.9.3. Se deberán elaborar planes de recuperación de respaldos y procedimientos para validar periódicamente, mediante pruebas (ensayos) la efectividad del proceso y la data respaldada.

6.9.4. Los procedimientos para validar la restauración de data deberán efectuarse al menos una vez por año. Dependiendo de su criticidad, el Jefe de la Unidad de Seguridad de la Información podrá aumentar esta validación a dos o más veces dentro del año.

6.9.5. El resultado de estos procesos de restauración deberá ser registrado en un informe técnico, que deberá ser remitido al Jefe de la Unidad de Seguridad de la Información y a los dueños (responsables) de la Información o de los procesos involucrados.

6.9.6. En caso de requerirse una restauración de datos desde los respaldos, éstos deberán ser solicitados formalmente por los dueños de los procesos o jefes de áreas de negocios involucradas, al Jefe de la Subdirección de Informática y Telecomunicaciones.

6.9.7. Los medios de respaldo deben ser almacenados en un recinto distinto de donde se efectúa, produce, procesa, transmite y/o respalda la información.

6.9.8. En caso de contratarse el servicio de respaldo con proveedores externos, se deberá incorporar dentro de las cláusulas del contrato de servicio, el cumplimiento de las políticas y normas de seguridad física y ambiental, de control de acceso y la suscripción de los respectivos convenios de confidencialidad.

6.9.9. Los sistemas o herramientas de respaldo y recuperación deben probarse periódicamente, asegurándose que operan en perfecto estado, y satisfacen los requerimientos considerados en los planes de continuidad operativa.

6.9.10. Los recintos donde se almacenen los medios de respaldo deberán contar con condiciones seguridad física y ambiental que aseguren la integridad, disponibilidad de la información contenida en ellos, de acuerdo a Política de Seguridad Física y Ambiental.

6.9.11. La eliminación de medios de respaldo (cintas, CD/DVD, u otros), deberá efectuarse mediante un procedimiento formal, el cual deberá ser dictado por el Jefe de Operaciones, que asegure que éstos son borrados en forma permanente y posteriormente destruidos.

6.9.12. En relación a un activo de información sobre el cual no se ha especificado el periodo de retención y posterior disposición, se aplicarán los criterios en conformidad con la normativa legal vigente (Ley 20.285 sobre Acceso a la Información Pública u otras, según corresponda).

6.10. Administración de la Red de Datos

6.10.1. El Jefe de la Unidad de Operaciones y de Telecomunicaciones conjuntamente con el Jefe de Seguridad de la Información, deberán definir los controles necesarios para garantizar la seguridad de los datos y los servicios conectados en las redes del MOP.

6.10.2. La Unidad de Operaciones y de Telecomunicaciones, es la responsable de implementar los controles requeridos en el punto anterior.

6.10.3. El Jefe de la Unidad de Seguridad de la Información, deberá velar por la implementación y cumplimiento de estos controles.

6.11. Administración y seguridad de los medios removibles

6.11.1. El Jefe de la Subdirección de Informática y Telecomunicaciones, o quien este designe, en conjunto con el Jefe de la Unidad 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.

6.11.2. Los procedimientos de eliminación deberán contar con registros de todos los medios removibles eliminados.

6.12. Procedimientos administración de la información relativa a la plataforma TI

6.12.1. Todos los activos de información administrados por la Subdirección de Informática y Telecomunicaciones, deberán estar registrados en el inventario de activos, según lo establece la Política de Gestión de Activos.

6.12.2. 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, deberán resguardarse a efecto de prevenir el acceso no autorizado. El acceso a esta documentación deberá estar restringido sólo al personal autorizado.

6.12.3. El acceso a esta información por parte de terceros no autorizados podrán ser permitidos por el al Jefe de la Subdirección de Informática y Telecomunicaciones.

6.13. Intercambios de información o software con otras entidades

6.13.1. 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:

a) Identificación de las autoridades responsables de este convenio (de intercambio, interoperación o colaboración).

b) Inclusión de cláusulas de confidencialidad, propiedad de la información, derechos de autor, vigencia, condiciones de uso y disposición de la información (o software) involucrada.

c) Controles de seguridad a aplicar, para asegurar la integridad y confidencialidad de la información a intercambiar, si corresponde.

d) Términos y condiciones de la licencia conforme a la cual se suministra el software, si corresponde.

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

a) Servicios o medios de transporte o mensajería confiables.

b) 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.

6.13.3. En caso de requerirse la implementación de procesos de interoperación electrónica de datos entre el MOP y otras organizaciones (públicas o privadas), el Jefe de la Unidad de Seguridad de la Información deberá proponer, elaborar y velar para que se establezcan convenios de interoperación que aborden los siguientes aspectos:

a) Identificación de las autoridades responsables de este Convenio de interoperación.

b) Inclusión de cláusulas de confidencialidad, propiedad de la información, derechos de autor, vigencia, retención, uso y disposición de la información involucrada.

c) 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).

d) Controles de seguridad a aplicar, para asegurar la integridad y confidencialidad de la información. (si se requiere).

1) Autenticación
2) Autorización
3) Encriptación

e) 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.

f) Información sobre la propiedad de la información suministrada y las condiciones de su uso.

6.13.4. Se deberán implementar controles para reducir los riesgos en el servicio de correo electrónico institucional, contemplando, por ejemplo, amenazas como las siguientes:

a) Intercepción o alteración de contenido, ataques informáticos, como negación de servicio (DoS), u otros similares, desde internet que puedan interrumpir este servicio.

b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transmisión involucrados.

c) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.

d) El impacto de un cambio (o mantención) del servicio de correo electrónico institucional.

e) Las implicancias de la publicación externa de listados de casillas y datos de funcionarios.

f) El acceso de usuarios remotos a las cuentas de correo electrónico.

6.13.5. Elaborar normativas de uso adecuado del servicio de correo electrónico institucional por parte de los funcionarios.

6.13.6. Se deberán tomar precauciones en términos de disponibilidad e integridad de la información que el MOP publica electrónicamente en sitios web o aplicaciones internet.

6.13.7. Se deberán incluir en los portales MOP, u otros sitios web ministeriales donde se publique información al público en general, así como en su contenido (cuando corresponda), cláusulas de uso y destino de la información en ellos expuesta o contenida.

6.13.8. Debido a restricciones impuestas por el Decreto Supremo N° 83, de 3 de Junio del 2004, se prohíbe el uso o contratación de servicios de repositorios electrónicos de datos (o documentos) que operen en internet, cuando se trate de información de carácter reservado, estratégico y/o crítica.

6.13.9. Las excepciones al punto 6.13.8, deberán ser autorizadas por el Comité de Seguridad de la Información.

6.13.10. Por razones de buen servicio, respaldo de datos, soporte técnico y/o lineamientos tecnológicos, se debe evitar el uso de sistemas de información o aplicaciones provistos por terceros.

6.13.11. Las excepciones a esta normativa deberán cumplir con las siguientes condiciones:

a) Que el sistema de información (o aplicación) provisto externamente (por un organismo del estado) sea parte de una directriz o normativa de gobierno.

b) Que el sistema de información (o aplicación) provisto externamente (por un organismo del estado) tenga características técnicas y funcionales más ventajosas para el MOP que una solución interna (existente) o desarrollada para ello.

c) Que el sistema o aplicación en cuestión sea provisto, soportado y mantenido por otro organismo público, que cuente con políticas, normas y procedimientos que aseguren la integridad, confidencialidad, y disponibilidad de la información, y sea soportado por la institución proveedora del sistema.

6.13.12. En caso de autorizarse, el uso sistemas o servicios de información externos, se debe cumplir con las siguientes condiciones:

a) Deberán suscribirse contratos de servicio y convenios de confidencialidad, con representante legal con domicilio en territorio chileno.

b) El servicio deberá contar con políticas y procedimientos de respaldo y recuperación, que aseguren disponibilidad de la información.

6.13.13. Para resguardar otras formas de intercambio de información, como es el caso de sistemas de radio, telefonía, fax, u otros, se deben implementar las siguientes acciones:

a) Informar y capacitar a los funcionarios respecto de las precauciones y resguardos que deben adoptar cuando se tiene acceso, manipula, transmite o procesa información sensible, en relación a su divulgación, ya sea verbal o escrita, en cualquier soporte.

b) No dejar mensajes con información sensible en contestadoras telefónicas automáticas.

c) Recordar periódicamente a los funcionarios no dejar información sensible, tales como documentos u otros en impresoras, o máquinas de fax, de acceso libre o sin control de acceso.

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

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

8. Difusión de la Política de Gestión de las Operaciones y las Comunicaciones

El Director General de la Dirección General de Obras Públicas, es responsable de publicar y difundir la Política de Gestión de las Operaciones y las Comunicaciones.

GLOSARIO DE TÉRMINOS

Activo de Información

Personas, 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 de 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 del 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.

Dueño o Responsable de Activo de Información

El la persona designada como responsable de la integridad, confidencialidad y disponibilidad de un activo de información.

Dirección General de Obras Públicas
Ministerio de Obras Públicas
Gobierno de Chile

3082

ORD.: Nº_____/

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 continúo 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.

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

- 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 Publicas

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 Nº 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.

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 Nª120 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 Publicas 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.

DE OBRAS PUBLICAS
SUBSECRETARIA
CHILE

MARIA LORETO SILVA ROJAS
Subsecretaria de Obras Públicas

Gino Curotto Godoy
Jefe División
Subdirección General de Obras Públicas
Dirección General 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. Maria 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° 5338229

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