PROCEDIMIENTO DE INFORME DE EVENTOS DE SEGURIDAD DE LA INFORMACION

DIRECCIÓN DE ARQUITECTURA

MINISTERIO DE OBRAS PÚBLICAS

Elaborado por:	Aprobado por:
Jaime Norton Maureira (titular) Claudio Olmos Chávez (suplente) Encargados Seguridad de la Información Dirección de Arquitectura **Fecha:** 03/10/19	Raul Irarrazabal Sanchez Director Nacional de Arquitectura **Fecha:** 03/10/19

Control de Cambios o Versiones

Versión	Fecha	Página	Principales Puntos Modificados
1.0	12 diciembre 2018	Todo el documento	• Primera versión del Procedimiento
2.0	13 junio 2019	Todo el documento	• Actualización y modificaciones

INDICE

1. Introducción

El presente documento se enmarca dentro de la Política de General de Seguridad de la Información del Ministerio de Obras Públicas ; la Política de Gestión de Incidentes de Seguridad de la Información del Ministerio de Obras Públicas Vigentes; y de las recomendaciones de seguridad dadas en el Decreto Supremo N° 83 del 2004 del Ministerio Secretaria General de la Presidencia "que Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos". En particular, este documento define el procedimiento para la Gestión de Incidentes de Seguridad de la Información dentro de la Dirección de Arquitectura, y de cómo se deben reportar, registrar, y gestionar las acciones destinadas a corregir, eliminar o mitigar su impacto.

2. Objetivo

Definir los canales de administración adecuados mediante los cuales se deben informar los eventos de Seguridad de la información dentro de la Dirección de Arquitectura, a modo de lograr una gestión oportuna de estos.

3. Alcance

El presente documento es aplicable a los siguientes procesos de negocio críticos de la Dirección de Arquitectura.

- Diseño de Ingeniería y/ o Arquitectura de Proyectos.
- Contratación de Obras y Consultorías.
- Ejecución de Obras.

El presente documento está dirigido a todos los funcionarios, proveedores y contratistas de la Dirección de Arquitectura, quienes tienen la obligación dentro de sus posibilidades de reportar los eventos y/o Incidentes de Seguridad (A.16.01.02). Para esto en el presente documento además de entregar el proceso para reportar el evento y/o incidente de seguridad producido, se mencionan algunos eventos y/o Incidentes.

4. Roles y Responsabilidades

Roles	Responsabilidades
Jefe/a de Servicio	Responsable de solicitar la aplicación del procedimiento al interior de la dirección por parte de los funcionarios, personal a honorarios y proveedores externos y Contratistas
Encargado/a Seguridad de la Información	Será responsabilidad del Encargado de Seguridad de la Información, recibir las notificaciones por parte del personal de la Dirección de Arquitectura que haya detectado un evento y/o un incidente de seguridad de la información, a través de los canales especificados en el presente procedimiento. Además deberá reportar el incidente a la cuenta de correo Ministerial de Gestión de Incidentes. También, dentro de sus funciones será velar por mantener el anonimato del funcionario(a) que lo solicite.
Funcionarios/as, proveedores y contratistas de la Dirección de Arquitectura	Tendrán la responsabilidad de reportar eventos y/o incidentes de seguridad de la Información a los encargados de Seguridad de la Información de la Dirección de Arquitectura.

5. Definiciones y Modo de Operación

5.1 Tipos de Incidentes de Seguridad de la Información

Debe entenderse por Incidente de Seguridad, todo hecho, vulnerabilidad o evento que ponga en riesgo la integridad, disponibilidad o confidencialidad de los activos de información de la Dirección Arquitectura del Ministerio de Obras Públicas.

Esta es una lista de posibles incidentes de seguridad, que permitirá identificarlos como tal, y los que de ser detectados deben ser informados (reportados) a través de los canales dispuestos para ello, en el menor tiempo posible.

1. **Acceso no autorizado**: Comprende todo tipo de ingreso y operación no autorizados a los sistemas, salas restringidas, bodegas u oficinas. En esta categoría se podrían mencionar los siguientes incidentes, a modo de ejemplo:
   - Intento o acceso no autorizado a lugares restringidos.
   - Pérdida de Integridad, disponibilidad o confidencialidad de un activo de Información.
   - Ingreso a computadores sin autenticación de nombre y clave.
   - Robo, borrado o alteración de información.
   - Abuso o mal uso de los servicios informáticos internos o externos que requieren autenticación.
   - Exponer (voluntaria o involuntariamente), revelar, informar o entregar copias u originales a personas no autorizadas, de información considerada confidencial.
   - Envío de correos a terceros desde una cuenta de correo institucional (MOP) que no es la propia.
   - Detectar la existencia de cuentas de acceso a sistemas (vigentes), pertenecientes a funcionarios que ya no trabajan en la Dirección.
   - Robo o pérdida de equipos de computación, celulares, notebook o similares.
   - Navegar en sitios web no autorizados por el MOP.
   - Incumplimiento de las políticas de seguridad de la información del MOP.
   - Detectar personas ajenas a la Institución sin identificación circulando por las dependencias del MOP.

2. **Código malicioso**: Comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la institución, los que son introducidos a la red mediante correos de cuentas fraudulentas de instituciones bancarias, de servicios, policiales y/o legales. En esta categoría se podrían mencionar los siguientes incidentes, a modo de ejemplo:
   - Virus informáticos.
   - Correos spam, fishing o alertas de seguridad recibidas desde cualquier organismo externo al MOP.
   - Troyanos, Gusanos informáticos.
   - Hackeo (interno o externo) de páginas, bases de datos, aplicaciones, computadores Institucionales o sistemas MOP.
   - Conexión o intento de conexión a la Red de datos MOP, sin autorización.
   - Dañar o intentar dañar sistemas de información, equipos de redes, cables de red u otros componentes relacionados con el procesamiento de información.
   - Descargar, instalar o emplear aplicaciones o herramientas de software no autorizadas.

   Es importante que ante la sospecha de haber infectado su computador por un virus informático, éste debe ser desconectado de la red y llamar de inmediato a soporte técnico para informar de la situación.

3. **Tipo administrativo**: son aquellos incidentes que involucran acciones de personas que, voluntaria o involuntariamente, ponen en riesgo los atributos de confidencialidad, integridad y disponibilidad de un activos de información:
   - Zonas con control de acceso despreocupado (puertas abiertas sin personal del área presente).
   - Exposición a personas no autorizadas de documentos con información confidencial.
   - Gabinetes o bodegas de documentos expuestas a vulnerabilidades tales como: condiciones climáticas, acceso no autorizado, entre otras.
   - Bultos en lugares sospechosos.
   - Incumplimiento de las Políticas y/o Procedimientos de Seguridad de la Información.

4. **Denegación del servicio**: Esta categoría incluye los eventos que ocasionan la pérdida de un servicio en particular. Los síntomas para determinar un incidente de esta categoría son:
   - Tiempos de respuesta muy bajos sin razones aparentes.
   - Servicios internos inaccesibles, que no se hayan bloqueado deliberadamente para resguardar activos de información.
   - Servicios externos inaccesibles, que no se hayan bloqueado deliberadamente para resguardar activos de información.
   - Detectar mal funcionamiento o sobrecarga de los sistemas críticos.

5. **Mal uso de los recursos tecnológicos**: Agrupa los eventos que atentan contra los recursos tecnológicos por su mal uso. En esta categoría se pueden mencionar los siguientes eventos, a modo de ejemplo:
   - Mal uso o abuso de servicios informáticos internos o externos.
   - Violación de las normas de acceso a internet.
   - Mal uso del correo electrónico institucional.
   - Dañar o intentar dañar sistemas de información, equipos de redes, cables de red u otros componentes relacionados con el procesamiento de información.
   - Descargar, instalar o emplear aplicaciones o herramientas de software no autorizadas.
   - Cambios de sistemas NO controlados.

6. **Escaneos, intento de obtención de información de la red o de un servidor**: Agrupa los eventos que buscan obtener información sobre la infraestructura tecnológica de la institución. Se pueden mencionar, a modo de ejemplo:
   - Sniffers (programa informático que registra la información que envían los periféricos).
   - Detección de Vulnerabilidades

7. **Sistemas de información**: incidentes relacionados con el uso de los sistemas, tales como:
   - Un sistema despliega información no solicitada (ejemplo: un reporte con datos que no se solicita o que no corresponde).
   - Mensajes o resultados erróneos o que no corresponden a lo esperado según la aplicación, o la opción de menú a la cual accedió.

Aquellos eventos y/o incidentes reportados erróneamente serán reclasificados como **Soporte Estándar**, correspondiendo a un problema técnico que no reviste riesgo en la seguridad de los procesos o activos de información relacionados, por ejemplo: falla de impresora, equipo de usuario con problemas técnicos, lentitud o falla en un sistema y/o aplicación.

5.2 Modo de Operación

5.2.1 Reportar Evento de Seguridad

Debe entenderse por evento o incidente de Seguridad de la Información toda ocurrencia identificada que afecte la integridad, disponibilidad y confidencialidad de los activos de información o una violación a las Políticas y/o Procedimientos de Seguridad de la Información, que deberán ser inmediatamente informadas a través de uno de los siguientes canales definidos:

a) Vía Correo Electrónico:

Para: Encargado de Seguridad de la Información

CC.: Subrogante Encargado de Seguridad de la Información

Asunto: Evento de Seguridad de la Información

Cuerpo del Correo: Describir el evento con el mayor detalle posible, adjuntando (si corresponde) algún documento que ayude a describir el incidente en cuestión, indicando de acuerdo al punto 5.1 la categoría del incidente y/o evento.

b) Vía Contacto Telefónico

Para estos efectos debe informar el evento y/o incidente de seguridad a los siguientes números telefónicos:

- Encargado de Seguridad de la información:

  Directo: (+56) 22 449 3711

- Subrogante de Seguridad de la Información:

  Directo: (+56) 22 449 3657

c) Presencial

Se puede dirigir a las siguientes Oficinas ubicadas en Edificio Corporativo, Morande 59.

- Encargado de Seguridad de la Información: Oficina 919, piso 9.
- Subrogante Encargado de Seguridad de la Información: Oficina 1006, piso 10.

Una vez que el Encargado de Seguridad o su Subrogante sean notificados del evento y/o incidente de Seguridad, deberán proceder a reportar el incidente a la cuenta de correo Gestión Incidentes Ministerial gestion.incidentes@mop.gov.cl. El sistema devolverá automáticamente un número de Ticket (Recepción de la solicitud) para el seguimiento del reporte de dicho incidente.

6. Registro de Operación

Identificación	Responsable de Registrar	Tiempo de Retención	Formato del Informe	Medio de Soporte	Lugar de Almacenar
Evidencia del envío del correo informando evento y/o incidente de seguridad	Encargado de Seguridad de la Información/ o Subrogante	1 año	Libre	Digital - PDF	Carpeta Personal con acceso restringido
Correo electrónico con número de Ticket que se genera como respuesta automática de la cuenta Gestión Incidentes	Encargado de Seguridad de la Información/ o Subrogante	1 año	Libre	Digital - PDF	Carpeta Personal con acceso restringido

7. Revisión y Actualización del Procedimiento

Este Procedimiento de la Dirección de Arquitectura se deberá revisar cada dos años o cuando se produzcan hechos relevantes, tales como modificaciones a la Política de General de Seguridad de la Información del Ministerio de Obras Públicas ; la Política de Gestión de Incidentes de Seguridad de la Información del Ministerio de Obras Públicas Vigentes, instrucciones de DIPRES o cualquier cambio significativo, para garantizar que el procedimiento este actualizado y su aplicación sea adecuada, eficaz y suficiente. El Encargado/a de Seguridad de la Información de la Dirección de Arquitectura será el responsable de la revisión, actualización de este procedimiento.

8. Difusión del Procedimiento

Se informará por medio de correo electrónico la revisión y/o actualización del presente procedimiento, el que deberá encontrarse publicado en la Intranet de la Dirección para su difusión interna.

9. Glosario

Activo de Información
Personas, archivos físicos, documentos electrónicos o cualquier otro activo identificado en el inventario de activos de información.

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 relacionada a la seguridad de la información.

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.

- **Confidencialidad**, Los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello. Corresponde a la clasificación Pública o Reservada de acuerdo a lo establecido en la Ley N°20.285 sobre acceso a la información pública.

- **Integridad**, El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

- **Disponibilidad**, Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.