APRUEBA POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD.

RESOLUCIÓN EXENTA N° 3089

SANTIAGO, 15 DIC 2015

VISTOS:

Las facultades que me confieren el Decreto Supremo Nº 674/2014 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley Nº 19.175; el DFL N° 29 de 2004 del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, Estatuto Administrativo; la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; lo dispuesto en la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma; el Decreto N° 181/2002 que aprueba el Reglamento de la Ley N° 19.799; el Decreto Supremo N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1.600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

1.- Que, se requiere de acciones, métodos y procedimientos a seguir ante las posibles incidentes relacionados con la seguridad de la información y que afecten el normal y correcto desempeño de la Institución de manera tal de poder dar una respuesta eficaz frente a una contingencia.

2.- Que, no existe documento en el que se indiquen las acciones, métodos y procedimientos a seguir en caso de incidentes a la seguridad de la información.

3.- Que, la institución está implementando un programa de mejoramiento de la gestión basado en la NCH-ISO 27001.Of 2013, la cual solicita procedimientos documentados respecto de este tipo de eventos.

15684414

RESUELVO:

1. **APRUÉBASE** la Política de Gestión de Incidentes de Seguridad, que se anexa a esta Resolución y forma parte integrante de ella.

2. **DIFÚNDASE** al personal a través de la intranet institucional y/o los medios declarados para este fin.

ANÓTESE, REGISTRESE Y COMUNIQUESE.

INTENDENCIA REGION METROPOLITANA
INTENDENTE

CLAUDIO ORREGO LARRAÍN
INTENDENTE
REGIÓN METROPOLITANA DE SANTIAGO

MEL/RZE/MRT/CCM/JGG

Distribución:

- Administración Regional
- División de Administración y Finanzas
- División de Análisis y Control de Gestión
- División de Planificación y Desarrollo
- Departamento Jurídico
- Departamento de Gestión Institucional
- Departamento de Informática
- Departamento de Gestión Documental
- Departamento Jurídico
- Encargada de la Unidad de Transparencia
- Oficina de Partes.

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

1.- POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

El GOBIERNO REGIONAL METROPOLITANO promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

Planificación de respuesta y tratamiento de incidentes de seguridad

Los propietarios de los activos de información, empleados y contratistas, deben informar lo antes posible al Encargado de Seguridad quien será el punto de contacto para la detección y notificación de incidentes de seguridad, los eventos de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

El Encargado de Seguridad debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

El Encargado de Seguridad debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.

Vigilancia, detección, análisis y presentación de informes de eventos e incidentes

El Comité DE SEGURIDAD, junto con El Encargado de Seguridad, deben reconocer las situaciones que serán identificadas como emergencia o desastre para el instituto, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

El Comité DE SEGURIDAD, junto con El Encargado de Seguridad, deben liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres

El Encargado de Seguridad debe convocar a la brevedad posible al Comité de Seguridad e informar de eventos o incidentes que se generen o sean reportados.

El Encargado de Seguridad debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

Respuesta, escalamiento, recuperación controlada de un incidente y Comunicación interna/externa.

El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo al Encargado de Seguridad para que se registre y se le dé el trámite necesario.

Es responsabilidad de los funcionarios del GOBIERNO REGIONAL METROPOLITANO y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

El Señor Intendente, Comité de Seguridad o el Encargado de Seguridad, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas. Así mismo serán los únicos autorizados para mantener contacto con grupos de interés externos o foros que se encargan de los asuntos en relación con los incidentes de seguridad de la información

Evaluación y Decisión de Eventos y debilidades

Los funcionarios y contratistas que utilizan los sistemas y servicios de información deben observar y reportar cualquier debilidad de seguridad de información observada o sospechada en los sistemas o servicios.

Se debe evaluar el Análisis de riesgos enfocado específicamente a valorar el impacto de incidentes que comprometen la continuidad del negocio teniendo en cuenta que este impacto será mayor cuanto más dure el incidente. Los pasos a seguir para realizarlo son los habituales de un análisis de riesgos:

- Se identifican los procesos críticos de negocio.
- Se identifican los eventos que pueden provocar interrupciones en los procesos de negocio de la organización.
- Se evalúan los riesgos para determinar la probabilidad y los efectos de dichas interrupciones en cuanto a tiempo, escala de daños y período de recuperación.
- Identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información en el ámbito del sistema de gestión de la seguridad de información, y estableces acciones de control y responsables de contribuir en la mitigación de los riesgos.

La Dirección Técnica de Información y Tecnología es la encargada de valorar los eventos de seguridad de información y decidir si han de ser clasificados como incidentes de seguridad de la información. Debe garantizar un enfoque coherente y eficaz para la gestión de incidentes en la seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

Los empleados deberán estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de la Política de Seguridad de la Información o alguno de los elementos que la soportan. En cualquier caso se hará un seguimiento de acuerdo con los procedimientos establecidos para el manejo de incidentes de seguridad

Análisis de Pruebas forenses

El Encargado de Seguridad debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo que esto vuelva a suceder.

El personal designado por el Encargado de Seguridad deberá tener competencia para manejar los temas relacionados con los incidentes de seguridad de información dentro de la organización

Registro de actividades de gestión de incidencias

El Encargado de Seguridad debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

HOJA DE REVISIÓN

FECHA	OBSERVACIONES	ENCARGADO DE SEGURIDAD	FIRMA
21-12-15	REVISAR AÑO 2016	JOSE IGNACIO GUTIERREZ	

HOJA DE ACTUALIZACIÓN

FECHA	HOJAS MODIFICADAS	ENCARGADO DE SEGURIDAD	FIRMA