POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

1 INDICE

2 OBJETIVO

Promover 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.

3 ALCANCE

La presente política es aplicable a todo el Gobierno Regional Metropolitano de Santiago y aplica a todos los funcionarios, no importando su calidad jurídica, proveedores, contratistas, personal que esté vinculado con la organización y que presten servicios al Gobierno Regional Metropolitano de Santiago o que estén relacionados. Se incluye, además, todas las dependencias que son parte de la institución.

Los incidentes más comunes que pueden suceder son:

- Fallas del sistema de información y pérdida del servicio
- Código malicioso
- Negación del Servicio
- Errores resultantes de data e incompleta o inexacta
- Violación de la confidencialidad e integridad
- Mal uso de los sistemas de información
- Falla de Servicios Básicos (Los Servicios básicos están descritos en el Instructivo correctivo preventivo)

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

Es responsabilidad de cada funcionario reportar cualquier incidente de seguridad o reportar alguna vulnerabilidad en la seguridad que fuera detectada. Esta debiera ser reportada a sus superiores de manera oportuna y evitar una incidencia mayor o utilizar los medios establecidos para denuncias.

El Departamento de Informática será el responsable de investigar cualquier reporte de incidentes de Seguridad.

El Departamento de Servicios Generales será responsable de cualquier incidente que ocurra con los servicios básicos.

El Comité de Seguridad será responsable de la revisión de los incidentes de seguridad.

El Jefe de Servicio, será el portavoz ante las autoridades.

5 CONTROL NORMATIVO SSI

La siguiente política tiene por finalidad dar cumplimiento a los siguientes controles de la politica NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.16.01.01	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de la seguridad de la información.
A.16.01.02	Informe de eventos de seguridad de la información	Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados.
A.16.01.03	Informe de las debilidades de seguridad de la información	Se debe requerir a todos los empleados y contratistas que usen los sistemas y servicios de información de la organización, que observen e informen cualquier debilidad (observada o que se sospeche) en la seguridad de la información de los sistemas o los servicios.
A.16.01.04	Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información.
A.16.01.05	Respuesta ante incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.
A.16.01.06	Aprendizaje de los incidentes de seguridad de la información	Se debe utilizar conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.
A.16.01.07	Recolección de evidencia	La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información que pueda servir de evidencia.

6 DEFINICIONES

6.1 Responsable del procedimiento

Los propietarios de los activos de información, empleados y contratistas, deben informar lo antes posible al Encargado de Seguridad quien será el responsable 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 eventos de seguridad de la información.

6.2 Procedimiento ante evento de Seguridad

Ante el informe de eventos de seguridad se realizará el siguiente procedimiento de captura de datos:

Numero de evento
Fecha del reporte
Fecha del evento
Hora de reporte
Nombre de quien reporto
Nombre de quien sufrió el evento
Tipo de evento
Descripción del evento
Grado de criticidad
Tiempo estimado de solución
Tareas a realizar para dar solución
Registro de avisos a Encargado de Seguridad, Jefaturas Depto. de Gestión de Personas, Depto. de Informática o Depto. de Servicios Generales (Debiéndose en estos casos señalar a quién se informó, la fecha y la hora de la comunicación)

Esta información nos permitirá desarrollar un procedimiento de evaluación seguro con respecto a los eventos de seguridad, este consistirá en los siguientes pasos:

- Informe de eventos o debilidades en la Seguridad de la Información
- Evaluación y Decisión de Eventos y debilidades
- Respuesta ante incidentes de seguridad de la información y comunicación interna/externa.
- Aprendizaje de los incidentes de seguridad
- Recopilación de evidencias

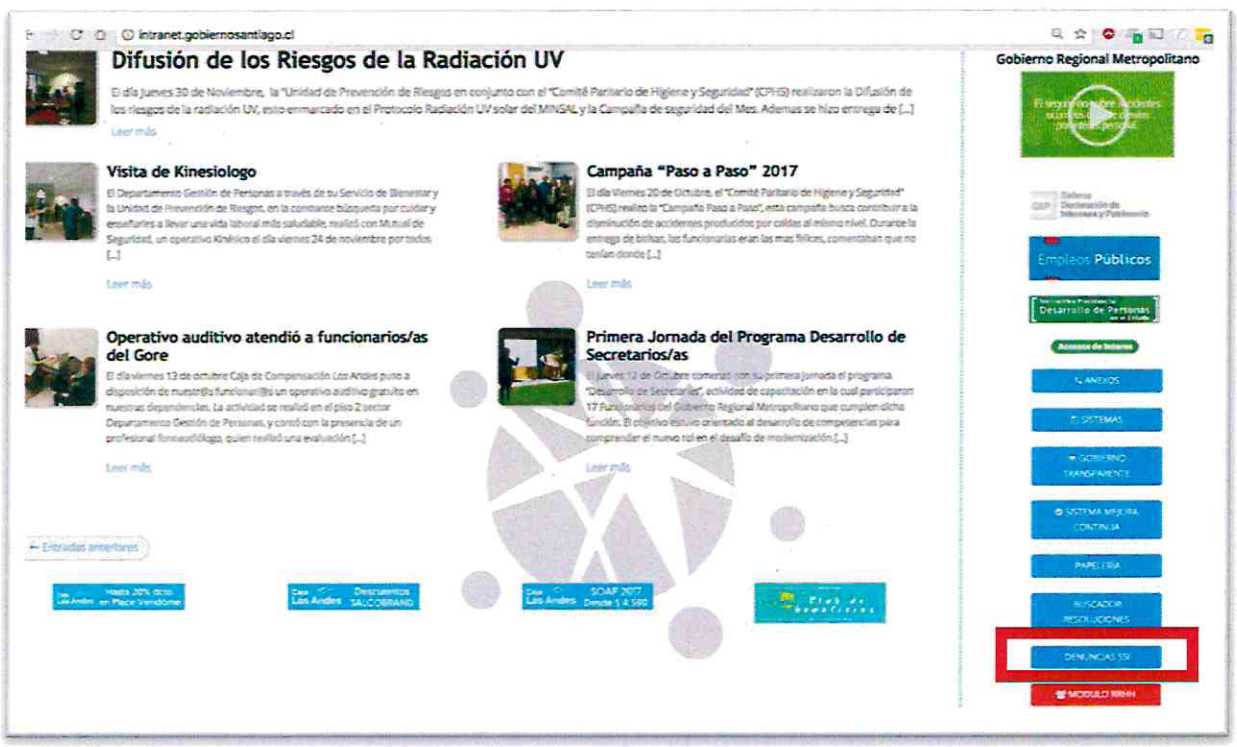
6.3 Informe de eventos o debilidades en la Seguridad de la Información

El Comité de Seguridad, junto con el Encargado de Seguridad, debe reconocer las situaciones que serán identificadas como emergencias o desastres para la institución, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

El Comité de Seguridad, junto con El Encargado de Seguridad, debe 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.

Ante los eventos sucedidos o debilidades detectadas los funcionarios o personal externo deberán informar mediante el formulario de denuncias SSI establecido en la Intranet o mediante correo electrónico al Encargado de Seguridad a la brevedad para así evitar un incidente mayor.



6.4 Evaluación y Decisión de Eventos y debilidades

Procedimientos para la evaluación de Incidentes de la Seguridad

- 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.

Evaluación de los Incidentes de Seguridad

El Encargado de Seguridad debe evaluar todos los eventos de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente. El Comité de Seguridad serán quienes valorarán los eventos de seguridad de información y decidirán si han de ser clasificados como incidentes de seguridad de la información. Deberán 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.

Cuando se detecte un evento de seguridad de la información, se deberá comunicar en forma inmediata al Jefe del Departamento afectado, quien deberá destinar la disponibilidad de personal y los recursos necesarios para poder determinar el origen del Incidente, el motivo por el que se produjo y dimensionar el impacto del mismo.

El Departamento de Servicios Generales será el encargado de valorar todo evento o incidente de Seguridad que tenga relación con los servicios básicos o con la seguridad física.

El Departamento de Informática será el encargado de valorar todo evento o incidente de Seguridad que tenga relación con redes, servicios de datos, internet, correos u otros que le competan.

6.5 Respuesta ante incidentes de seguridad de la información 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 de Santiago 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.

6.6 Prevención y corrección de Incidentes

El Servicio ha dispuesto de un documento llamado **Instructivo Correctivo Preventivo** el cual deberá servir como guía ante posibles eventos o incidentes reportados.

6.7 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

6.8 Canales de comunicación Interno/externo

El Jefe de Servicio, el 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

6.9 Aprendizaje de los incidentes de seguridad

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, los incidentes de Seguridad pueden usados como medio de capacitación o concientización a todos los funcionarios de lo que podría suceder y como podría evitarse en el futuro.

6.10 Recopilación de evidencias

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, de manera de recolectar la mayor cantidad posible de datos, información o evidencia del Incidente de Seguridad y poder preservarla para su análisis, posterior estudio o propósitos de acciones legales y disciplinarias si corresponde.

7 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

8 PERIODICIDAD DE EVALUACION Y REVISIÓN

La siguiente Política será revisada, evaluada y/o actualizada según corresponda y aprobada su vigencia una vez al año por el Comité de Seguridad de la Información, en cuanto a su funcionamiento y correcta aplicación en la Institución.

9 FORMALIZACION EXTERNA

Mediante el acta fecha 12 de julio año 2019, se aprueba por parte del Comité de Seguridad de la Información, la Política de gestión de incidentes de seguridad.

10 REGISTRO, REVISION Y ACTUALIZACION HISTORICO

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	11-08.16	Creación Documento
02	Carlos Hernández	todas	29-06-2017	Se cambia formato y se actualiza documento
03	Carlos Hernández	todas	10-07-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI • Se incorpora registro de control
04	Mauricio Marín	todas	2-08-2018	Se agrega en Registro de Control el siguiente párrafo: En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo. Se cambia título 6 por Definiciones. Se cambia título 7 por Registro de Operaciones. Se cambia título 9 por Periodicidad de evaluación y revisión
05	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
06	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Política de gestión de incidentes de seguridad año 2019.

11 FORMALIZACIÓN INTERNA

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Paulo Mendoza** Encargado Unidad de Soporte **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Alejandro Segura B.** Presidente Comité de Seguridad