Gobierno de Chile

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

RESOLUCION EXENTA Nº 2795

SANTIAGO, 29 DIC 2011

VISTOS:

Las facultades que me confieren el Decreto Supremo Nº 591/2011 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley Nº 19.175, Orgánica Constitucional de Gobierno y Administración Regional; el D.F.L. Nº 1/19.653, de 2.000, del Ministerio Secretaria General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Resolución Nº 1600, de la Contraloría General de la República; el DFL Nº 1/19.175, que fijó el texto refundido, coordinado, sistematizado y actualizado de la ley Nº 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; y

CONSIDERANDO:

1° Que, con el objeto de contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional, de manera de asegurar la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios/clientes/beneficiarios.

2° Que, es afán de este Gobierno Regional, responder a distintos requerimientos, y en particular, lo referente a seguridad de la información.

3º Que, este Servicio estima pertinente protocolizar en forma precisa el acceso a los Activos de Información existentes y así evitar posibles vulnerabilidades en la Seguridad de la Información.

4° Que, este Servicio considera necesario instruir en forma clara, precisa y eficiente acerca de los procedimientos, procesos y acciones que se deben realizar en el momento que se produzca un incidente relacionado con la Seguridad de la Información.

5° Que, se requiere registrar, catastrar, gestionar y comunicar todos los incidentes de Seguridad de la Información que se produzcan en el Servicio, con la finalidad de poder tomar las medidas correctivas y preventivas para evitar que éstos se produzcan nuevamente.

RESUELVO:

1.- APRUÉBENSE el siguiente Protocolo e Instructivo con el objeto de asegurar, velar, gestionar y fortalecer la Seguridad de la Información del Servicio, los cuáles se adjuntan y son parte constitutiva de la presente Resolución, la que entrará en vigencia a partir de la fecha de su total tramitación:

- Protocolo para el Control y Tratamiento de la Seguridad de la Información.
- Instructivo de Contingencia.

2.- PUBLÍQUESE un ejemplar de la presente Resolución, Protocolo e Instructivo adjuntos en el Banner de Seguridad de la Información de la Intranet Institucional.

ANÓTESE, REGÍSTRESE Y COMUNÍQUESE.

INTENDENCIA REGION METROPOLITANA
INTENDENTA

CECILIA PEREZ JARA
INTENDENTA
REGIÓN METROPOLITANA DE SANTIAGO

PUM/FRW/PSL/JGG/sbq

Distribución:
Gabinete Intendencia
Administración Regional
División de Análisis y Control de la Gestión
División de Planificación y Desarrollo
División de Administración y Finanzas
Departamento Jurídico
Unidad de Auditoría Interna
Unidad de Control Interno y Rendición de Cuentas
Unidad Regional de Asuntos Internacionales
Departamento de Gestión Institucional
Departamento de Gestión de Personas
Departamento de Gestión Documental
Departamento de Gestión de Abastecimiento
Departamento de Presupuesto y Contabilidad
Departamento de Servicios Generales
Departamento de Informática
Unidad de Desarrollo
Unidad de Soporte
Departamento de Control de Proyectos de Infraestructura y Obras Viales
Departamento de Actividades de Cultura, Deporte y Seguridad
Departamento de Transferencias de Capital
Departamento de Adquisición de Activos no Financieros
Departamento de Preinversión y Proyectos
Departamento de Planificación
Oficina de Partes.

PROTOCOLO DE CONTROL Y TRATAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

El presente documento tiene por finalidad definir y normar los métodos o procedimientos de acceso para el desarrollo de actividades con terceros, de modo de considerar y establecer mecanismos y reglas de protección a la información y al equipamiento tecnológico del Gobierno Regional Metropolitano.

Dadas las actuales condiciones de avance en materia de tecnologías de información y comunicación, es que se deben definir los resguardos y garantías que permitan establecer acuerdos de confiabilidad en el desarrollo de actividades por terceros, en cualquiera sus formas posibles y, ante la necesidad de otorgar permisos de acceso a información institucional, equipos de procesamiento de información o red interna de comunicación del Servicio se deben utilizar las definiciones del presente documento.

2. ALCANCES

El presente documento se debe considerar para todo tipo de trabajo que involucre acceso a la información de la Institución, así como facilitar cualquier tipo de acceso a equipamiento de éste en cualquiera de sus formas. Se deben utilizar las normativas que aquí se definen, de modo de asegurar la protección e integridad de la información como de los equipos de procesamiento de información del Servicio.

3. DISPOSICIÓN INICIAL PARA EL ACCESO A TERCEROS

Toda solicitud de acceso a información, equipos de procesamiento de esta o red interna de datos debe ser elevada y canalizada formalmente al encargado de seguridad del Gobierno Regional Metropolitano. En ésta se deben especificar los siguientes puntos:

- Motivo del acceso.
- Método requerido.
- Período para el cual se requiere de acceso.
- Horarios en los que se efectúa el acceso.
- Periodicidad.
- Tipo de información o tipo de acceso requerido.
- Responsable de la solicitud del tercero.
- Contraparte interna del Gobierno Regional Metropolitano para el acceso.

Con esta información el encargado de seguridad deberá solicitar antecedentes a la contraparte interna del Gobierno Regional Metropolitano, quien deberá responder formalmente en no más de 15 días hábiles, el ámbito de intervención interno de la solicitud, siendo como mínimo los siguientes:

- Identificación de las áreas o unidades de procesamiento interna responsables de la información o de orientación que originan el motivo de la solicitud.
- Impacto del acceso ya sea aprobado o rechazado, debe definir el impacto al interior del Servicio como a la ciudadanía.
- Análisis del valor o criticidad de la información solicitada (Extremo – Alto – Medio – Bajo)
- Definición de intereses involucrados que puedan ser afectados por la solicitud.

Una vez recibidos los antecedentes, el Encargado de Seguridad podrá conformar un comité de evaluación que estará integrado como mínimo por el Encargado de Unidad responsable de la información, Jefatura del Departamento de Informática, Analista del Departamento de Informática y Abogado del Departamento Jurídico, quienes deberán desarrollar un informe de evaluación de solicitud en el ámbito de seguridad de la información y de las disposiciones legales que afectan o involucran en la petición.

De acuerdo a esto, el Encargado de Seguridad procederá a autorizar o rechazar la solicitud, fundamentando la decisión.

4. TIPOS DE ACCESO

Al aceptar una solicitud conforme al punto anterior, se debe establecer claramente el tipo de acceso requerido, el cual debe normarse de acuerdo a uno de los siguientes enfoques:

4.1. Acceso físico a medios de procesamiento de información

El acceso a la entidad o empresa estará representado en una o más personas las que deberán portal una credencial de visita solo para el piso y lugar correspondiente al desarrollo de sus funciones. Se evaluará la posibilidad de otorgar una credencial permanente en caso que el acceso sea mayor a 1 mes. El Departamento de Informática en conjunto con el Encargado de Unidad responsable de la información realizará:

a) Acta de recepción de los bienes inventariables involucrados para uso del tercero en el Gobierno Regional Metropolitano.

b) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.

c) Evaluación de activos comprometidos, solo en caso que el acceso no sea solo lectura. Se deberá identificar uno a uno los datos a los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultantes (reportes, cálculos) a los que se podría ver afectada la integridad de la información.

d) Descripción de los servicios de información disponibles para el tercero.

e) Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al encargado de seguridad quien registrara las actividades.

f) Definición de un método específico de protección de la integridad de la información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Control de Acceso, la Política de Seguridad y del Procedimiento de Acceso Controlado a Oficinas e Instalaciones del Gobierno Regional Metropolitano.

4.2. Acceso lógico desde la red institucional del Gobierno Regional Metropolitano

El acceso a la entidad o empresa estará representado en una o más personas las que deberán portal una credencial de visita solo para el piso y lugar correspondiente al desarrollo de sus funciones. Se evaluará la posibilidad de otorgar una credencial permanente en caso que el acceso sea mayor a 1 mes. El Departamento de informática en conjunto con el Encargado de Unidad responsable de la información realizará:

a) Acta de recepción de los bienes inventariables involucrados para uso del tercero en el Gobierno Regional Metropolitano.

b) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.

c) Declaración del o los sistemas a los que se concederá el acceso.

d) Para cada uno de los sistemas involucrados se debe proporcionar:

- Evaluación de activos comprometidos, solo en caso que el acceso no sea solo lectura. Se deberá identificar uno a uno los datos a los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultantes (reportes, cálculos) a los que se podría ver afectada la integridad de la información.
- Descripción de los servicios de información disponibles para el tercero.
- Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al encargado de seguridad quien registrará las actividades.

- Definición de un método específico de protección de la integridad de la información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.
- Fundamentar las razones en términos de beneficios y riesgos de los accesos otorgados.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Control de Acceso, la Política de Seguridad y del Procedimiento de Acceso Controlado a Oficinas e instalaciones del Gobierno Regional Metropolitano.

4.3. Acceso lógico remoto a la red institucional del Servicio

Solo estará permitido para esta modalidad el uso de Web- Services donde se deberá aplicar:

a) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.

b) Evaluación de activos comprometidos, solo en caso que el acceso no sea solo lectura. Se deberá identificar uno a uno los datos a los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultantes (reportes, cálculos) a los que se podría ver afectada la integridad de la información.

c) Descripción de los servicios de información disponibles para el tercero.

d) Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al Encargado de Seguridad o quien éste defina, el cual registrará las actividades como mecanismo de control.

e) Definición de un método específico de protección de la integridad de los activos de información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.

f) Fundamentar las razones en términos de beneficios y riesgos de los accesos otorgados.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Control de Acceso y la Política de Seguridad del Gobierno Regional Metropolitano.

5. ACUERDO DE PROTECCIÓN DE ACTIVOS

Se deberá establecer con el tercero un acuerdo formal de protección a la información el que será vinculado, de acuerdo a la índole del tercero, a través de un oficio si es con otro servicio público o del contrato si corresponde a un prestador de servicios, el que debe incluir las siguientes cláusulas de protección mínimas:

a) Se realizará el monitoreo o seguimiento de las actividades realizadas por el tercero, el que tendrá una evaluación periódica y permitirá evaluar si se cumplen las solicitudes de acceso autorizadas pudiendo detectar anomalías de acceso, carga errónea de información o cualquier actividad que pudiera afectar la información o equipamiento del Gobierno Regional Metropolitano lo que ocasionará la revocación inmediata de los permisos otorgados, desencadenando las acciones legales que se estimen pertinentes.

b) No se permitirá en ningún caso extraer información no especificada en la solicitud de acceso como tampoco realizar divulgación, venta o copia de ésta.

c) No se podrán realizar instalaciones o desinstalaciones de software de cualquier tipo sin previa autorización escrita por la Jefatura del Departamento de Informática.

d) El tercero declara conocer la Política de Seguridad de la Información del Gobierno Regional Metropolitano.

e) Se deberá enviar mensualmente al Encargado de Seguridad o quien éste defina y, si no aplica el período, al menos una vez, el detalle de actividades realizadas identificando usuario, fecha, información intervenida o alcanzada y resultados obtenidos.

f) El mantenimiento del equipamiento de procesamiento de información será única y exclusivamente mantenido por personal del Departamento de Informática del Gobierno Regional Metropolitano. Estará estrictamente prohibido conectar computadores portátiles o cualquier dispositivo de procesamiento de propiedad del tercero a la red de datos del Gobierno Regional Metropolitano, sin contar con una autorización por escrito emitida por el Departamento de Informática.