DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

RESOLUCION EXENTA N° 2857

SANTIAGO, 30 DIC 2011

VISTOS:

Las facultades que me confieren el Decreto Supremo N° 591/2011 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley N° 19.175, Orgánica Constitucional de Gobierno y Administración Regional; el D.F.L. N° 1/19.653, de 2.000, del Ministerio Secretaria General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Resolución N° 1600, de la Contraloría General de la República; el DFL N° 1/19.175, que fijó el texto refundido, coordinado, sistematizado y actualizado de la ley N° 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.

3° Que, este Servicio estima pertinente crear normas y procedimientos para asegurar y velar por la Seguridad de los Activos de Información.

4° Que, este Servicio considera necesario abarcar todos los Activos de Información, no realizando diferencias entre Activos Físicos y Tecnológicos.

5° Que, debido al valor de la información de este Servicio se requiere fijar normas especificas para evitar vulnerabilidades en la Seguridad de la Información.

RESUELVO:

1.- APRUÉBENSE las siguientes normas con el objeto de asegurar, velar, gestionar y fortalecer la Seguridad de la Información del Servicio, las cuáles se adjuntan y son parte constitutiva de la presente Resolución:

- Norma de Acceso Físico
- Norma de Seguridad Informática
- Norma de Uso Navegación por Internet
- Norma de Uso Correo Electrónico

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURIDICO
REGION METROPOLITANA

- Norma de Uso Instalación Legal de Software
- Norma de Uso Identificación y Autentificación
- Norma de Uso Outsourcing

2.- PUBLÍQUESE un ejemplar de la presente Resolución y los documento citados anteriormente 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/RAH/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.

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURIDICO
REGION METROPOLITANA

NORMA DE USO

OUTSOURCING

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

Introducción

Propósito. Definir e indicar a los usuarios, sobre el manejo comercial y riesgos de la seguridad de la información asociados con los procesos de negocios de outsourcing en el Gobierno Regional Metropolitano de Santiago, los cuales exponen a perdida de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

Los beneficios comerciales de la contratación externa de las funciones clave del negocio deber equilibrada contra los riesgos comerciales y de seguridad de la información.

Los riesgos asociados con la externalización deben ser gestionados a través de la imposición de controles adecuados, que comprende una combinación jurídica, física, controles de lógica, de procedimiento y de gestión.

Alcance

Las políticas mencionadas en el presente documento aplican a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios Gobierno Regional Metropolitano de Santiago o que estén relacionados. Se incluye además, todas las dependencias que son parte de la institución o que transite por la red de Gobierno Regional Metropolitano de Santiago.

Política

Esta política especifica los controles para reducir los riesgos asociados a la seguridad de la información que conlleva el servicio de outsourcing.

Se considera como proveedores de Outsourcing quienes:

- Ofrecen soporte de Hardware y software y al personal de mantenimiento
- Consultores externos y contratistas
- Empresas TI de externalización de procesos empresariales
- Personal temporal

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.

Elección de un servicio externalizado (contratistas)

El criterio para la selección de un servicio externalizado se define y documenta, tomando en consideración lo siguiente:

- Historia y reputación de la compañía
- Calidad de los servicios provistos a otros consumidores
- Número y competencias del personal y gerencia
- Estabilidad financiera de la compañía y marca comercial
- Rango de retención de empleados de la compañía
- Garantía de calidad y normas de gestión de la seguridad que tiene actualmente la empresa (ej: certificado de cumplimiento de ISO 9000 e ISO/IEC 27001)

Evaluación de riesgos de la subcontratación

El Gobierno Regional Metropolitano de Santiago, a través de su Unidad, nombrará a un funcionario para cada función de negocio/proceso de subcontratación. El encargado, con la ayuda del equipo local de gestión de riesgos de la información, quienes en conjunto deberán evaluar los riesgos antes de la subcontratación, utilizando procesos de evaluación de riesgos estándares de la Unidad.

La evaluación del riesgo deberá, al menos, tomar en cuenta lo siguiente:

- Naturaleza del acceso lógico y físico a los activos de información del Gobierno Regional Metropolitano de Santiago y facilidades para que el servicio externalizado pueda cumplir con el contrato

- La sensibilidad, el volumen y el valor de los activos de la información de que se trate

- Los riesgos comerciales tales como la posibilidad de que el negocio de la empresa subcontratista falle completamente, o que ésta misma, no cumpla con los niveles de servicio acordados o la prestación de servicios para el Gobierno Regional Metropolitano de Santiago pueda generar conflictos de interés para los competidores en el mercado

- Facilidad de interacción entre compañías con la que actualmente emplea el Gobierno Regional Metropolitano de Santiago.

El resultado de la evaluación del riesgo se presentará a la administración para su aprobación antes de la firma del contrato de outsourcing. La administración del Gobierno Regional Metropolitano de Santiago decidirá si existe un beneficio general por la externalización de la función ofrecida por la empresa outsourcing, teniendo en cuenta tanto los aspectos comerciales, legales y de la seguridad de la información. Si los riesgos son altos y los beneficios insignificantes (por ejemplo, si los controles necesarios para gestionar los riesgos son demasiado costosos), la función o servicio no se podrá subcontratar.

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.

Los contratos y acuerdos de confidencialidad

Deberá existir un contrato formal entre el Gobierno Regional Metropolitano de Santiago y el contratista para proteger ambas partes. El contrato definirá con claridad el tipo de información intercambiada y el propósito para ello.

Si se intercambia información que es confidencial, se deberá generar un documento/acuerdo de confidencialidad entre el Gobierno Regional Metropolitano de Santiago y el subcontratarte, ya sea como parte del contrato de externalización en sí o un acuerdo de confidencialidad por separado (que puede ser necesario antes de que el contrato principal es negociado).

La información deberá ser clasificada y controlada de acuerdo a las políticas del Gobierno Regional Metropolitano de Santiago.

Cualquier información recibida por parte del subcontratista hacia el Gobierno Regional Metropolitano de Santiago que está obligado por contrato o acuerdo de confidencialidad estará protegida por la adecuada clasificación y etiquetado.

Después de la terminación del contrato, los acuerdos de confidencialidad serán revisados para determinar si la confidencialidad debe ampliase más allá de la tenencia del contrato.

Todos los contratos se presentarán a la Unidad Jurídica para revisar el contenido exacto, el lenguaje y la presentación de estos.

El contrato definirá claramente las responsabilidades de cada parte hacia el otro mediante la definición de las partes en el contrato, la fecha efectiva, las funciones o servicios prestados (por ejemplo, define los niveles de servicio), el pasivo, las limitaciones en el uso de subcontratistas y asuntos legales normales a cualquier contrato. Dependiendo de los resultados de la evaluación de riesgos, varios controles adicionales deberían ser incorporados o referenciados en el contrato, tales como:

- Legales, reglamentarias y otras obligaciones de terceros, como protección de datos y las leyes de privacidad, etc.

- Obligaciones de seguridad de la información y los controles, tales como:

  - Las políticas de seguridad de la información, procedimientos, normas y directrices, normalmente en el contexto de un Sistema de Gestión de Seguridad de la Información tal como se define en la norma ISO / IEC 27001

  - Revisar los antecedentes de los empleados o terceros que trabajan en el contrato (véase sección contratación y capacitación de los empleados)

  - Controles de acceso para restringir la divulgación no autorizada, modificación o destrucción de la información, incluyendo controles de acceso físico y lógico, los procedimientos para conceder, revisar, actualizar y revocar el acceso a los sistemas, datos e instalaciones, etc (véase sección Control de Acceso)

  - Procedimiento de manejo de Incidentes de Seguridad de la Información incluyendo reportes obligatorios de incidentes.

  - Devolución o destrucción de todos los activos de información por parte del subcontratista después de la finalización de la actividad externa o cuando el bien ya no es necesario para apoyar la actividad de contratación externa.

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.

- Derecho de autor y patentes de protección similar para cualquier propiedad intelectual compartida por el subcontratista o desarrollados en el curso del contrato

- Especificación, diseño, desarrollo, prueba, implementación, configuración, gestión, mantenimiento, apoyo y uso de controles de seguridad asociados con los sistemas TI, además del depósito en garantía del código fuente

- Controles anti-spam, anti-spyware y similares

- El cambio de TI y la gestión de configuración, incluyendo la administración de vulnerabilidades, parches y verificación de los controles de seguridad del sistema antes de su conexión a las redes de producción.

➢ El derecho del Gobierno Regional Metropolitano de Santiago para controlar todo acceso a la utilización de las instalaciones de Gobierno Regional Metropolitano de Santiago, redes, etc., los sistemas, y para verificar la conformidad del subcontratista con el contrato, o contratar a un auditor independiente de común acuerdo (tercero) para este fin.

➢ Acuerdos de continuidad del negocio como situaciones de crisis y gestión de incidentes, capacidad de recuperación, copias de seguridad TI y de recuperación de desastres (DRP)

Aunque los subcontratistas estén certificados conforme con la ISO / IEC 27001 se debe prever de un sistema de manejo de seguridad de la información efectivo en el lugar, incluso, puede ser necesario para el Gobierno Regional Metropolitano de Santiago verificar los controles de seguridad que son esenciales para hacer frente a los requisitos específicos de seguridad del Gobierno Regional Metropolitano de Santiago, generalmente cuando son auditados (véase sección Auditorías de Seguridad)

Contratación y capacitación de los empleados

Empleados, subcontratistas y consultores que trabajan en nombre del Gobierno Regional Metropolitano de Santiago serán sometidos a verificaciones de antecedentes equivalentes a las realizadas a los empleados del Gobierno Regional Metropolitano de Santiago. En esa selección se tendrá en cuenta el nivel de confianza y la responsabilidad asociada con la posición y (si lo permitiese la ley):

- Prueba de identidad de la persona (ej: pasaporte)
- Prueba de sus calificaciones académicas (ej: certificados)
- Prueba de su experiencia de trabajo (ej: resumen/CV y referencias)
- Verificación de antecedentes penales
- Verificación de situación financiera

Para la seguridad de la información y la educación en ella, será facilitada a todos los empleados y terceras partes del contrato, aclarando sus responsabilidades en materia de políticas de seguridad de la información, normas, procedimientos y directrices del Gobierno Regional Metropolitano de Santiago (por ejemplo política de privacidad, la política de uso aceptable, el procedimiento para la comunicación de incidentes de seguridad de la información, etc.) y todas las obligaciones definidas en el contrato.

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.

Control de acceso

Con el fin de evitar el acceso no autorizado a los activos de información del Gobierno Regional Metropolitano de Santiago por el subcontratista o subcontratistas, los controles de seguridad a utilizar, se describe en esta sección. Los detalles dependen de la naturaleza de los activos de información y los riesgos asociados, lo que implica la necesidad de evaluar los riesgos y diseñar una arquitectura de los controles adecuados.

Los controles de acceso técnicos incluirán:

- **Identificación y autenticación de usuarios**

  - Autorización de acceso, generalmente a través de la asignación de roles de usuarios para tener definidas las funciones adecuadas y los derechos de acceso lógico y controles

  - El cifrado de datos en conformidad con las políticas de encriptación que posee el Gobierno Regional Metropolitano de Santiago y las normas de definición Standard de algoritmos, longitudes de claves, claves de gestión, etc.

  - Registro de control de acceso a contabilidad / auditoria, además de las alarmas / alertas de violaciones de intento de acceso de acuerdo al caso

- **Control de acceso**
  - se documentarán en los procedimientos, directrices y documentos relacionados e incorporados a la sensibilización, formación y actividades educativas. Esto incluye:

    - Elección de contraseñas seguras
    - Determinar la configuración adecuada y los derechos de acceso lógico
    - Revisar y, si es necesario, revisar los controles de acceso para mantener el cumplimiento de los requisitos

- **El control de acceso físico**

  Deberá incluir:

  - Controles de capas que cubren el perímetro y las barreras internas

  - Instalaciones fuertemente construidas

  - Bloqueos adecuados para los procedimientos de gestión de claves / contraseñas

  - Registros de acceso automatizado cuando es utilizada una tarjeta-llave magnética, los registros de los visitantes a las instalaciones, etc.

  - Alarmas de intrusión / alertas y los procedimientos de respuesta.

Si partes del Gobierno Regional Metropolitano de Santiago están hosteados en datacenters de terceros, el operador de Data Centers se asegurará de que los activos del Gobierno Regional Metropolitano de Santiago estén física y lógicamente aislados de otros sistemas.

El Gobierno Regional Metropolitano de Santiago velará por que todos los activos de información entregados al contratista durante la vigencia del contrato (además de las copias hechas a partir del principio, incluyendo copias de seguridad y archivos) sean debidamente recuperados o destruidos en el momento apropiado antes de la terminación del contrato. En el caso de que los activos de la información altamente confidenciales, se requiere el uso de un calendario o un registro y un

proceso mediante el cual el subcontratista formalmente acepte la rendición de cuentas por los activos en la reunión final del proyecto / proceso.

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.

Auditorías de seguridad

Si el Gobierno Regional Metropolitano de Santiago debiese contratar una función de negocio de outsourcing con base en otra ubicación diferente, se auditarán las instalaciones físicas del subcontratista periódicamente para el cumplimiento de las políticas de seguridad del Gobierno Regional Metropolitano de Santiago, de ésta forma, garantizar que se cumplan los requisitos definidos en el contrato.

La auditoría deberá también tener en cuenta los niveles de servicio acordados en el contrato, para determinar si se han cumplido sistemáticamente y revisar los controles necesarios para corregir cualquier discrepancia.

La frecuencia de las auditorías será determinada por los integrantes de Auditoría Interna, Gestión de Seguridad de la Información y la Unidad Jurídica.

Responsabilidades

Administración

La administración es responsable de la adecuada designación de los encargados de los procesos de negocio que se subcontraten, la supervisión de las actividades de subcontratación y de garantizar que adhiera a ésta política.

La administración es responsable de los controles de mandato comercial o de seguridad para gestionar los riesgos derivados de la externalización.

Procesos de negocio de los subcontratistas

El Gobierno Regional Metropolitano de Santiago, será el encargado de evaluar y gestionar los riesgos comerciales y de seguridad asociados a la externalización, cada vez que sea necesario, en colaboración con los encargados de Seguridad de la Información, Unidad Jurídica o quienes tengan las competencias.

Seguridad de la Información

El equipo de Seguridad de la información, será el encargado de analizar los riesgos asociados y desarrollar el proceso adecuado para la gestión de controles de cumplimientos técnicos como también jurídicos.

El equipo de Seguridad de la información también es responsable de mantener ésta política.

Auditoría Interna

El área de Auditoria Interna está autorizada por la administración para evaluar el cumplimiento de todas las políticas corporativas en cualquier momento.

A su vez, podrá ayudar con las auditorías de los contratos de outsourcing de seguridad, incluyendo auditorías de cumplimiento, y asesorar en la gestión de los riesgos y los controles relativos a la contratación externa.

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.

Anexos

Historial de revisiones

VERSIÓN	ELABORADO	REVISADO	APROBADO	AUTORIZADO	FECHA

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.