DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA

APRUEBA NORMA DE OUTSOURCING DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3047

SANTIAGO, 22 DIC 2017

VISTOS:

El Decreto Supremo N° 331/2017 del Ministerio de Interior y Seguridad Pública; las facultades que me concede el Artículo 24 letra ñ) de la Ley N° 19.175, Orgánica Constitucional de Gobierno y Administración Regional; 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; el Decreto N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

1.- Que, el indicador de Seguridad de la Información es un instrumento de control de gestión en las instituciones públicas, para la exitosa implementación de un Sistema de Seguridad de la Información;

2.- Que, es importante considerar los lineamientos que establece la "Política Nacional de CiberSeguridad", la cual señala como esencial dentro de un Sistema de Gestión de la Seguridad de la Información (SGSI), la gestión del riesgo;

3.- Que, la gestión del riesgo permite la identificación de amenazas, valoración y priorización de controles que ayudan a mitigar los mismos, detectados en la institución;

4.- Que, siempre existirá un riesgo residual con el cual hay que convivir como institución, pero es importante establecer el número de controles que mitiguen éstos, hasta el nivel que el riesgo residual sea aceptable.

1617 7831

5.- Que, es decisivo que cada institución comprenda que el número de controles que decida implementar, será a partir del resultado del perfil de riesgos que cada servicio enfrenta;

6.- Que, un riesgo de seguridad de la información corresponde a una amenaza potencial que podría afectar activos de información, vinculados a los procesos de soporte institucional y/o a los procesos de provisión de Productos Estratégicos (bienes y servicios) establecidos en las definiciones estratégicas institucionales (Formulario A1 DIPRES), y por tanto causar daño a la organización;

7.- Que, los servicios deben determinar cuáles son los riesgos de seguridad que afectan sus productos estratégicos del formulario A1 DIPRES, ello permite priorizar qué controles de la Norma deberán ser implementados para mitigar éstos;

RESUELVO:

1.- DÉJESE sin efecto la Resolución N° 2857 del 30 de Diciembre de 2011, que aprobó la Norma de Outsourcing del Gobierno Regional Metropolitana.

2.- APRUEBASE la Norma de Outsourcing del Gobierno Regional Metropolitano de Santiago.

ANOTESE Y PUBLIQUESE

INTENDENCIA REGION METROPOLITANA
INTENDENTE

JUAN PABLO GOMEZ RAMIREZ
INTENDENTE (S)
REGION METROPOLITANA DE SANTIAGO

IFF/GEP/VGM/MRT/JIG

Distribución:
- Funcionario Gobierno Regional Metropolitano de Santiago
- Honorarios Gobierno Regional Metropolitano de Santiago
- Comité de Seguridad de la Información
- Oficina de Partes

Norma de Outsourcing

1 INDICE

2 OBJETIVO

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 pérdida 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 deben ser equilibrados 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.

3 ALCANCE

Las normas 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.

4 ROLES Y RESPONSABILIDADES

Administrador(a) Regional

El Gobierno Regional Metropolitano a través de su Administrador (a) Regional, 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 norma.
A su vez es responsable de los controles de mandato comercial o de seguridad para gestionar los riesgos derivados de la externalización.

El Encargado de Seguridad

El Encargado de Seguridad del Gobierno Regional Metropolitano de Santiago será quien deberá evaluar y gestionar los riesgos comerciales y de seguridad asociados a la externalización, cada vez que sea necesario, en colaboración con los Jefes de Departamentos que contraten servicios externos, Unidad Jurídica o quienes tengan las competencias.

Departamento de Informática

El Departamento de informática, será el encargado de analizar los riesgos asociados y desarrollar el proceso adecuado para la gestión de controles de cumplimientos técnicos. El Departamento de informática también es responsable de mantener ésta norma.

Departamento de Servicios Generales

El Departamento de Servicios Generales, será el encargado de analizar los riesgos asociados y desarrollar el proceso adecuado para la gestión de controles de cumplimientos técnicos para todos los servicios básicos contratados.

5 CONTROL NORMATIVO SSI

El siguiente procedimiento tiene por finalidad dar cumplimiento a los siguientes controles de la norma NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.13.02.02	Acuerdos sobre transferencia de información	Los acuerdos deben abarcar la transferencia segura de la información de negocio entre la organización y terceros.
A.13.02.04	Acuerdos de confidencialidad o no divulgación	Se debe identificar y revisar regularmente los requerimientos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización.
A.15.01.02	Abordar la seguridad dentro de los acuerdos del proveedor	Todos los requisitos de seguridad de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.
A.15.01.03	Cadena de suministro de tecnologías de la información y comunicaciones	Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones y la cadena de suministro del producto

6 DESARROLLO DE LA NORMA

Esta norma específica los controles para reducir los riesgos asociados a la seguridad de la información que conlleva el servicio 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.
- Empresas que proveen servicios.

6.1 Evaluación de riesgos de la subcontratación.

El Gobierno Regional Metropolitano de Santiago, a través de la Unidad que corresponda, 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.

6.2 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.

6.3 Acuerdo de transferencia de información

Si se intercambia información que es confidencial, se deberá generar un documento/acuerdo de confidencialidad entre el Gobierno Regional Metropolitano de Santiago y el subcontratante, 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 sea negociado).

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

6.4 Acuerdo de confidencialidad

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 ampliarse 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 con 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.

6.5 Seguridad dentro de los acuerdos con los proveedores

- 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.

6.6 Control de desarrollo externalizado

- 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.

- 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.

6.7 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

6.8 Acuerdos con los proveedores y cadena de suministros

Para la seguridad de la información y la educación en ella, será facilitada a todos proveedores, sus empleados y terceras partes del contrato, aclarando y acordando 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.

6.9 Controles 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 Informática / contabilidad / auditoria, además de las alarmas / alertas de violaciones de intento de acceso de acuerdo al caso.
- **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 Center 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 acepto la rendición de cuentas por los activos en la reunión final del proyecto / proceso.

6.10 Auditorias 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 el 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, Departamento de Información y la Unidad Jurídica.

7 REGISTRO DE CONTROL

El Departamento de Informática y Departamento de Servicios generales deberán emitir un informe que dé cuenta de:

- A.13.02.02 Informe respecto de transferencias de archivos
- A.13.02.04 Informe de Acuerdo de no divulgación con Contratistas
- A.15.01.02 Informe de acuerdo con proveedores
- A.15.01.03 Informe de requisitos de seguridad acordados con el proveedor en la cadena de suministros

El informe deberá ser enviado al Encargado de Seguridad de manera semestral.

Todo documento deberá venir formalizado por quienes sean responsables del proceso (Debe contener logo del Servicio, fecha de creación, nombre, cargo y firma del responsable).

8 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.

9 REVISIÓN

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

10 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Virginia Saavedra** Jefa de Departamento de Servicios Generales **Carolina Hidalgo M.** Jefa Departamento de Gestión Institucional	**Mayuri Reyes Torres** Presidente Comité de Seguridad

11 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	11-08.16	Creación Documento
02	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
03	Mauricio Marín	todas	13-09-17	Modificación de Formato, se agrega índice, Revisión, Difusión.

Acta de Reunión
Comité de Seguridad de la Información

Asistentes:

- Sra. Mayuri Reyes Torres - Jefa División de Administración y Finanzas
- Srta. Carolina Hidalgo Mandujano – Jefa Departamento de Gestión Institucional
- Sra. Valentina Guerra Monsalve - Jefa Departamento Jurídico
- Sra. María Macarena Miranda Nuñez - Jefa Departamento de Gestión Documental
- Sr. José Ignacio Gutiérrez - Encargado de Seguridad de la información
- Sr. Hector Salinas Murúa – Jefe (s) Departamento de Informática
- Sr. Carlos Hernández Arancibia – Analista Departamento de Informática
- Sr. Mauricio Marín Vera – Analista Departamento de Informática
- Srta. Paulina Vilches Vásquez– Encargada Unidad de Transparencia
- Sr. Juan Catalán Farías – Depto. Servicios Generales
- Sr. Ariel Lagos Vásquez – Prevencionista de Riesgos

Tabla:

1. Se ratifica al Jefe del Departamento de Informática como Encargado de Seguridad de la Información.

2. Se acuerda incorporación a este Comité de los siguientes funcionarios:
   a. Jefe Departamento de Servicios Generales
   b. Jefe Departamento de Gestión de Personas
   c. Prevencionista de Riesgos Institucional

3. Se revisa y evalúa la correcta ejecución de los contratos de mantenimiento del Gobierno Regional Metropolitano (GORE RM).

4. Se revisan y validan por parte de este Comité los siguientes documentos:

   - Política General de Seguridad de la Información
   - Resolución Encargado de Seguridad de la Información
   - Resolución de nombramiento Comité de Seguridad de la Información
   - Instructivo Correctivo Preventivo
   - Manual de Gestión de Archivos
   - Norma de Acceso a la Red
   - Norma de Eliminación de Activos
   - Norma de Seguridad de la Información para la Gestión de Proyectos
   - Norma de Uso Outsourcing
   - Norma de Trabajo Remoto
   - Norma de Uso Instalación Legal de Software
   - Norma de Uso Identificación y Autentificación

- Norma de Uso Navegación por Internet
- Norma de Uso para los Equipos Tecnológicos Portátiles
- Norma de Reutilización y Devolución de Activos
- Plan de Emergencia Institucional
- Política de Clasificación de Activos
- Política de Acceso físico
- Política de Correo Electrónico
- Política de Desarrollos de Sistemas
- Política de Dispositivos Móviles
- Política de Escritorios y Pantallas Limpias
- Política de Gestión de Incidentes de Seguridad
- Política de Gestión de la capacidad
- Política de la Seguridad Informática
- Política de Respaldo de la Información
- Política Gestión de Claves
- Política Manejo de Activos
- Política para la Privacidad y Protección de la Información e Identificación Personal
- Política sobre el Uso de Controles Criptográficos
- Política y Proceso de Selección de Personal
- Procedimiento de Control de las Vulnerabilidades Técnicas
- Protocolo de Control y Tratamiento de SSI
- Reglamento sobre Infracciones al SSI

5. Se toma conocimiento y valida el informe "Procesamiento y Confidencialidad de los Activos de Información", elaborado por el Encargado del Seguridad de la Información, el cual da cuenta de la no ocurrencia de incidentes de seguridad durante el período 2017.

6. Se informa por parte del Encargado de Seguridad de la Información respecto de la participación en distintas instancias en materias relativas al Sistema de Seguridad de la Información:

   - Exposición para el Sector Público de Expertos en materia de Seguridad informática (Subsecretaría del Interior)
   - Reunión bipartita GORE RM-Red de Expertos
   - Jornada de Capacitación Indicador SSI (Ministerio Secretaría General de la Presidencia)

7. Se dan a conocer por parte del Encargado de Seguridad de la información las medidas de difusión del Sistema de Seguridad de la Información a través de:

   - Correo electrónico a todo el personal.
   - Banner corporativo en Intranet Institucional.

8. Se acuerda que el Comité de Seguridad tenga una próxima sesión durante el primer semestre del próximo año para evaluar lo reportado durante 2017 y revisar los compromisos 2018.

Aprueban:

Sra. Mayuri Reyes Torres
Jefa División de Administración y Finanzas

Srta. Carolina Hidalgo Mandujano
Jefa Departamento de Gestión Institucional

Sra. Valentina Guerra Monsalve
Jefa Departamento Jurídico

Sra. María Macarena Miranda Nuñez
Jefa Departamento de Gestión Documental

Sr. Hector Salinas Murúa
Jefe (s) Departamento de Informática

Srta. Paulina Vilches Vásquez
Encargada Unidad de Transparencia

Sr. José Ignacio Gutiérrez García
Encargado de Seguridad de la Información