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 esta 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 DEFINICION Y MODO DE OPERACION

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 OPERACION

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.

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.

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 ANEXOS

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

DEPARTAMENTO DE INFORMATICA

Acuerdo de no divulgacion

En Santiago a xxxxxxx de 2018, entre el Gobierno Regional Metropolitano en adelante el Servicio y la empresa: XXXXXXXXXXX., en adelante el proveedor, se establecen y acuerdan los siguientes requisitos de seguridad de la información.

En el Marco Legal vigente nuestro legislador en la Ley 19.913 de 2003 crea la unidad de análisis financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos, la que fue modificada por la ley 20.818, de 2015 y la Ley sobre Protección de Datos de Carácter Personal Nº19.628 de 1999, dentro de este marco legal el Proveedor deberá guardar confidencialidad de todos los antecedentes que conozca con motivo del contrato y no podrá hacer uso de éstos para fines ajenos al contrato y bajo ninguna circunstancia podrá, por cualquier título y/o medio revelar, difundir, publicar, vender, ceder, copiar, reproducir, interferir, interceptar, alterar, modificar, dañar, inutilizar, destruir, en todo o en parte esta información ya sea durante la vigencia del Contrato como después de su finalización.

Esta prohibición afecta al proveedor, su personal directo e indirecto, sus consultores, subcontratistas y al personal de éstos, en cualquier calidad, que se encuentren ligados al contrato en cualquiera de sus etapas, y su responsabilidad será solidaria, incluso después de la expiración del Contrato.

El proveedor sólo podrá copiar o reproducir la información que sea necesaria para dar cumplimiento al contrato, del mismo modo puede acceder, procesar, almacenar, comunicar o proporcionar componentes de Infraestructura de TI para la información del Gobierno Regional Metropolitano.

Se establece y se documenta este acuerdo con el proveedor para garantizar que no existen malos entendidos entre el Servicio y el proveedor en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

Se incluyen los siguientes términos con el fin de satisfacer los requisitos de seguridad de la información mencionados a continuación:

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

DIVISION DE ADMINISTRACION Y FINANZAS
DEPARTAMENTO DE INFORMATICA

1. EL proveedor tendrá acceso a la sala de Servidores pero deberá ser acompañado de un funcionario del Departamento de informática mientras duren sus labores.

2. El proveedor deberá dejar por escrito la razón de sus trabajos y la necesidad de acceder a la Sala de Servidores.

3. El proveedor se compromete a la protección de datos y a mantener la privacidad sobre los activos de información, los derechos de propiedad intelectual, derechos de autor del Servicio.

4. El Servicio en cumplimiento de la Política de acceso Físico cumplirá todo lo mencionado en ella con el fin de dar cumplimiento a esta a proveedores o personal.

5. EL proveedor se compromete a mantener reglas de uso aceptable de la información, incluido en uso inaceptable en caso de ser necesario.

6. EL proveedor deberá facilitar una lista explícita del personal autorizado para acceder a la Sala de Servidores del Servicio.

7. EL Proveedor se compromete a seguir las políticas de seguridad de la información pertinentes a su contrato específico para el manejo y manipulación de los activos de la Información.

8. EL proveedor se compromete a capacitar y concientizar a todo su personal de la importancia de los Activos de Seguridad de la información del Servicio y a dar una respuesta apropiada y oportuna ante incidentes o eventos de la Seguridad Informática.

9. En caso de Subcontratación el proveedor será el responsable de los trabajos realizados como también de cualquier incidente o evento de la Seguridad de la Información y no podrá delegar la responsabilidad del trabajo asignado y deberá guiarse por las normativas pertinentes para la subcontratación, incluidos los controles que se deberían implementar incluida una persona de contacto para los asuntos de seguridad de la información.

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

DIVISION DE ADMINISTRACION Y FINANZAS
DEPARTAMENTO DE INFORMATICA

10. El Proveedor autoriza al Servicio a auditar todos los procesos y los controles del proveedor relacionados al acuerdo.

11. Ante eventuales incidentes o eventos de la Seguridad de la Información el proveedor junto con el Encargado de Seguridad acordaran la resolución de conflictos que pudiesen resultar de los trabajos realizados.

12. el proveedor se obliga cumplir con los requisitos de seguridad de la organización.

_____ _____

Héctor Muñoz
Jefe Departamento de
Servicios Generales

Proveedor

11 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Juan Catalan F** Jefe(s) de Departamento de Servicios Generales **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Alejandro Segura B** Presidente Comité de Seguridad

12 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.
04	Mauricio Marín	11, 12, 13, 14	01-08-2018	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 agrega Anexo : Acuerdo de no Divulgación Se cambia título 6 por Definición y Modo de Operación Se cambia título 7 por Registro de Operación
05	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información aprueba revisión año 2019.

ACTA DE REUNIÓN: Comité Seguridad de la Información	
Objetivo:	Situación SSI primer semestre 2019.
Fecha y Hora:	12 de Julio de 2019 10:00 horas
Lugar:	Sala de Reunión 6º Piso

PUNTOS DE LA REUNIÓN

- Bienvenida
- Actualización de Controles SSI, correspondiente a cada departamento.
- Cumplimiento SSI 2019 primer semestre.
- Vulnerabilidades primer semestre 2019.
- Phishing GORE.
- Afiche SSI
- Revisión documentación vigente.

DESARROLLO DE LA PRESENTACIÓN

Se le recuerda al Comité los controles comprometidos para dar cumplimiento a PMG-SSI 2019. También se informa la fecha de entrega al departamento de informática (18 al 24 de Julio 2019) y cuando se tiene que hace el reporte a la red de expertos (Primera semana de Agosto).

Implementación de plataforma https://onlyoffice.gobiernosantiago.cl , para hacer la entrega de controles. La cual Carlos Hernández envío una invitación al correo electrónico de los integrantes del comité.

Sebastián Benussi enviará modificación de "Procedimiento de Controles de Auditorías de Sistemas de la Información".

En el Segundo semestre 2019, se trabajará en la unificación del "Manual de Gestión de Archivos", "Política Manejo de activos", "Política clasificación de activos" y "Norma de Eliminación de Activos" del Departamento Gestión Documental.

Se exponen las vulnerabilidades presentadas durante el primer semestre del 2019; corte de luz, FTP y Central telefónica.

Se informó del Phishing enviado a los funcionarios y se evidenció los resultados que se obtuvieron en este ejercicio.

Se presentó Afiche SSI implementado en el mes de julio.

Revisión de documentación SSI vigente:

- Política de correo electrónico e Internet
- Política de dispositivos móviles
- Política de Derechos de propiedad Intelectual

- Política Gestión de Personas
- Instructivo correctivo preventivo
- Manual de gestión de archivos
- Norma de acceso a la Red
- Norma de la Seguridad de la información para la Gestión de Proyectos
- Norma de Outsourcing
- Norma de Trabajo Remoto
- Norma de uso identificación y autentificación
- Norma de uso de instalación legal de software
- Norma de reutilización y devolución de activos
- Plan de emergencia Institucional
- Política clasificación de activos
- Política de acceso físico
- Política de desarrollos de sistemas
- 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 general de seguridad de la información
- Política gestión de claves
- Política manejo de activos
- Política sobre el uso de controles criptográficos
- Procedimiento de control de las vulnerabilidades técnicas
- Procedimientos de Auditoria de Sistemas de Información
- Protocolo y control de tratamiento de SSI

Asistencia a Reunión Comité Seguridad de la Información

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	Asistentes Comité de Seguridad de la Información	Página 1 de 1
		Fecha: 12/07/2019

	Nombre	Unidad	Firma
1	Jose Gutierrez	Departamento de Informática	
2	Alejandro Segura	Div. Administracion y Finanzas	
3	Fernando Fuenzalida	Departamento Jurídico	
4	Carolina Hidalgo	Planificacion y Control Institucional	
5	Jennifer Lueiza	Depto. De Gestion de Personas	
6	Sebastian Benussi	Depto. Auditoria Interna	
7	Juan Catalan	Depto. De Servicios Generales	
8	Silvana Torres	Depto. De Gestion Documental	
9	Ariel Lagos	Depto. De Gestion de Personas	
10	Carlos Hernandez	Departamento de Informática	
11	Matías Benitez	Departamento de Informática	
12			
13			
14			
15			