DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA

APRUEBA NORMA DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE PROYECTOS DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3027

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.

16177866

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° 3001 del 29 de noviembre de 2016, que aprobó la Norma de Seguridad de la Información para la Gestión de Proyectos del Gobierno Regional Metropolitana.

2.- APRUEBASE la Norma de Seguridad de la Información para la Gestión de Proyectos 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 la seguridad de la información para la gestión de proyectos

1. INDICE

Contenido

2. OBJETIVO

Asegurar la entrega de los resultados de los proyectos en el tiempo, con el presupuesto y la calidad acordados y considerando también el adecuado alineamiento con los planes estratégicos del Servicio y de TI.

3. ALCANCE

El presente documento permitirá la correcta planificación y ejecución de los Proyectos provistos por el Gobierno Regional Metropolitano de Santiago, facilitando el manejo de control de cambios, minutas, , procesamiento y almacenamiento de la información conforme a su clasificación quedando finalmente todo documentado para la finalización y entrega misma del proyecto.

Esta Norma es aplicable a todos los funcionarios (planta, contrata, código del trabajo, reemplazos y suplencias) personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios en el Gobierno Regional Metropolitano.

4. ROLES Y RESPONSABILIDADES

Cada uno de los integrantes del equipo de trabajo deberán tener claro los roles, responsabilidades y autoridad que le corresponde antes de iniciar el proyecto, para evitar conflictos durante la realización del mismo.

Los miembros del equipo de trabajo deben contar preferentemente con experiencia en proyectos similares, conocimientos, familiaridad con proyectos relacionados y disponibilidad.

Comité de Seguridad de la Información: Aprobar los proyectos y priorizar la ejecución de los mismos.

Funcionarios encargados y terceros: Conocer y aplicar lo estipulado en esta política.

Jefe de Proyecto: Funcionario a cargo de coordinar la planificación y ejecución del proyecto.

5. CONTROL NORMATIVO SSI

Código del Control	Identificación del Control	Requisito de control
A.06.01.05	Seguridad de la información en la gestión de proyecto.	Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.

6. PAUTAS

a) El Jefe de Proyecto debe realizar un análisis de factibilidad para la ejecución de los proyectos, considerando la posibilidad técnica, operativa, de recursos y económica para ejecutarlo. Se deben incluir los objetivos de seguridad de la información en los objetivos del proyecto

b) El Jefe de proyecto será el encargado de presentar al Comité de Seguridad de la Información la Planificación del proyecto.

c) El Comité de Seguridad de la Información será el responsable de aprobar o denegar los proyectos.

d) El Jefe de Proyecto deberá contar con una metodología para la Administración de proyectos basada en la metodología de Gestión de proyectos Institucional aplicable a todos los proyectos que involucren al Servicio. Esta metodología se deberá revisar de forma anual para verificar que esté siendo funcional y realizar aquellos cambios que se consideren necesarios, siempre y cuando estos sean aprobados por el Comité de Seguridad de la Información.

e) La metodología debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos. Dicha metodología debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y

post-implantación después de la instalación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio. Se debe contemplar la realización de una Evaluación de riesgos de la seguridad de la información en una etapa temprana para identificar los controles necesarios.

f) La metodología de Administración de Proyectos debe ser aplicada a todos los proyectos. Si se determina que en algún proyecto no aplica alguna de las etapas, se deberán documentar las razones y ser aprobadas por la jefatura del Departamento de Informática.

g) Si se desea realizar algún cambio en la metodología de Administración proyectos, se deberá presentar una solicitud al Comité de Seguridad de la Información el cual hará el estudio de factibilidad y aprobará o rechazará la solicitud.

h) Se debe establecer un plan del proyecto que contemple el alcance que tendrá el mismo para tener un entendimiento común entre todos los interesados del proyecto, además para tener una visión de la forma en que se relaciona con otros proyectos dentro del programa global de inversiones

i) Se debe realizar una reunión al inicio del proyecto para aclarar los roles, responsabilidades y plan a seguir y se deberán programar reuniones periódicas para supervisar el avance del proyecto.

j) Se documentarán minutas detalladas de todas las reuniones que se realicen durante el proyecto.

k) Previo al inicio del proyecto, deben establecerse y documentarse los criterios de aceptación para cada uno de los entregables con el responsable de este. Dichos criterios deben incluir el tiempo de entrega y requisitos de funcionalidad y calidad del mismo.

l) Se deberá desarrollar una Evaluación de riesgos de la seguridad de la información que permita identificar posibles eventos que impacten negativamente el proyecto, además de identificar la forma en que se evaluarán y se les dará respuesta a dichos riesgos.

m) Cualquier duda, recomendación u observación que se considere pertinente durante la ejecución del proyecto, deberá tratarse directamente con el Jefe del Proyecto.

n) Los entregables producidos en cada fase del proyecto deben ser aprobados formalmente por el Jefe del Proyecto.

o) Se debe contar con un control de cambios apropiado para cada proyecto, de forma tal que todos los cambios al proyecto de cualquier tipo (costos, cronograma, alcance, calidad) se revisen, aprueben e incorporen de manera apropiada al plan del proyecto.

p) Todo cambio en el proyecto debe quedar debidamente documentado y aprobado.

q) Para el cierre del proyecto, el Jefe del Proyecto debe aprobar formalmente la finalización y entrega a satisfacción del mismo.

r) Al final del proyecto, el Jefe del Proyecto se reunirá con las áreas involucradas para discutir los resultados del proyecto, problemas que surgieron y hacer recomendaciones para futuros trabajos similares.

s) Se deberá informar al Comité de Seguridad de la Información la finalización del proyecto y se entregará una copia de la documentación del mismo al Encargado de Seguridad Institucional.

t) Toda la información relativa al control en la ejecución de los proyectos de Tecnologías de Información deberá ser documentada y almacenada en un lugar seguro.

7. REGISTRO DE CONTROL

El Departamento de Informática deberá emitir un informe que dé cuenta de los proyectos desarrollados, mencionando los siguientes puntos:

- A.06.01.05 Informe de los proyectos realizados de acuerdo a los siguientes ítems
  - Proyectos Desarrollados
  - Tipo de Proyecto

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. DIFUSION

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. REVISION

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

10. APROBACION

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Héctor Salinas Murua.** Encargado Unidad de Desarrollo	**Mayuri Reyes Torres** Presidente Comité de Seguridad

Carolina Hidalgo M.

Jefa Departamento de

Gestión Institucional

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

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