Norma de seguridad de la información para la gestión de proyectos

1. INDICE

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. DEFINICIONES

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 OPERACION

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 anual.

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. 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. FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Norma de seguridad de la información para la gestión de proyectos.

11. REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

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	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 cambia título 6 de "pauta" por "Definiciones" Se cambia título 7 "Registro de Control" por "Registro de Operación". Se cambia periodicidad del informe de semestral a anual y se revisa ortografía
04	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.

05	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019.
06	Carlos Hernández	8	15-11-2021	Se agrega capítulo 10 formalización externa Se actualiza índice
07	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

12. FORMALIZACION

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Héctor Salinas M.** Encargado Unidad de Desarrollo **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Mayuri Reyes T.** Presidente Comité de Seguridad

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**ACTA DE REUNION** **COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 3 Fecha 23/11/ 2021

ACTA DE REUNION: Comité de Seguridad de la Información	
Objetivo	Situación SSI año 2021
Fecha y Hora	23-11-2021, 15:00
Lugar	Sala de Reunión 2° Piso

PUNTOS DE LA REUNION

1. Bienvenida
2. Actualización de Documentos
3. Vulnerabilidades año 2021
4. 67 vulnerabilidades detectadas en sitios y páginas webs
    a. Caída de Switch piso 5 - 13 de septiembre 2021
    b. Caída de Switch piso 1 - 27 de septiembre 2021
5. Envío Correo Phishing
6. Protectores de Pantalla
7. Capacitación SSI
8. Mejoras
    a. Switch
    b. GTD Ancho Banda
9. SGD, 0 Papel
10. Eliminación Activos
11. Necesidades Tecnológicas

Aprobación los siguientes documentos

1. **Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio**
2. **Manual de gestión de archivos**
3. **Norma de acceso a la Red**
4. **Norma de Eliminación de Activos**
5. **Norma de la Seguridad de la información para la Gestión de Proyectos**
6. **Norma de Outsourcing**
7. **Norma de Trabajo Remoto**
8. **Norma de uso identificación y autentificación**
9. **Norma de uso de instalación legal de software**
10. **Norma de reutilización y devolución de activos**
11. **Plan de Continuidad**
12. **Plan de emergencia Institucional**
13. **Política clasificación de activos**
14. **Política de acceso físico**
15. **Política de correo electrónico e Internet**
16. **Política de Derechos de propiedad Intelectual**
17. **Política de desarrollos de sistemas**

18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

DESARROLLO DE LA PRESENTACION

José Ignacio da la bienvenida y explica brevemente que es el SSI y las funciones del comité

Se da detalle al comité respecto a las vulnerabilidades CSIRT y las caídas de los switch

Claudio Muñoz y Mayuri Reyes, solicitan al comité la revisión de funcionamiento de cámaras de seguridad del Gore. Debido a problemas que existen actualmente

José Ignacio informa que esta demora se ha debido a que se necesita realizar una revisión inicial de todas las cámaras y su funcionamiento.

Se detallan las mejoras tecnológicas a realizar con carácter de importancia

- Cambios en los switch
- Importancia de dejar el sistema de cámaras en un circuito cerrado fuera de la red

Se recalca la importa de incluir SSI en la inducción a nuevos funcionarios

Se menciona a comité que se enviara cazabobos y que de ahí se realizara una capacitación a quienes caigan en él.

Se establece que el cambio de contraseñas debiera ser cada 6 meses de forma obligatoria empezando con un cambio masivo en marzo. Aplicándose tanto en AD como en sistemas.

Comité solicita que los mensajes de los protectores de pantalla sean un poco más "Rudos" refiriéndose a la gravedad de lo que podría ocasionar una vulneración importante de sistemas

Silvana Torres entrega información

- **Acerca del expurgo de documentos**
- **2022 se enviará soporte en papel a archivo nacional**
- **Se está digitalizando documentación antigua**
- **Menciona que para todo envío a archivo nacional o eliminación debe haber un testigo que vise la correcta digitalización de documentos, transformación digital 21808**

José Ignacio retoma la palabra e indica al comité la importancia dentro de todo el proceso de 0 papel de contar con una cloud de respaldo para toda la gran cantidad de archivos que se está generando

Explica que se continuara siempre con el respaldo en cintas. Indica que se necesita realizar respaldo en cintas como parte de SSI

Se aprueban políticas y documentación SSI

Carolina Hidalgo solicita curso de ciberseguridad a comité y participantes

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	**ACTA DE ASISTENTES COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 1 Fecha 23/11/ 2021

N°	NOMBRE	DEPARTAMENTO O UNIDAD	FIRMA
01	José Ignacio Gutiérrez	Departamento de Informática	
02	Mayuri Reyes T.	División Administración y Finanzas	
03	Héctor Valladares	Departamento Jurídico	
04	Carolina Hidalgo	Departamento Planificación y Control Institucional	
05	Silvana Torres	Departamento de Gestión Documental y Activos	
06	Claudio Muñoz	Departamento de Servicios Generales	
07	Paulo Serrano	Departamento de Gestión de Personas	
08	Luz Magaly Nuñez	Unidad de Transparencia	
	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	DAF	
11			
12			
13			