POLÍTICA DE GESTIÓN DE LA CAPACIDAD

1 INDICE

2 OBJETIVOS

Garantizar que la capacidad y el desempeño de la infraestructura de TI puede soportar eficientemente las demandas de los recursos tecnológicos y servicios críticos requeridos por el Gobierno Regional Metropolitano, de acuerdo con las necesidades de la Institución y que sean justificables en costos.

3 ALCANCE

Lo definido como parte de este documento es aplicable a todos los funcionarios del Departamento de Informática involucrados en el proceso de Gestión de la Capacidad de la Infraestructura de TI y todo aquel involucrado en asegurar la capacidad de la Infraestructura de TI para soportar la demanda del negocio.

4 DEFINICIONES

- **Capacidad:** Totalidad de condiciones con las que cuenta un servicio o recurso para cumplir con la demanda requerida.
- **Umbral:** Rangos de medida establecidos para identificar los límites de alerta de un comportamiento.
- **Matriz RACI (matriz de asignación de responsabilidades):** Se utiliza para relacionar actividades con recursos (individuos o equipos de trabajo) para asegurar que cada uno de los componentes del alcance esté asignado a un individuo o a un equipo. En la siguiente tabla se explica en qué consiste cada rol.

Descripción		
R	Responsable	Este rol realiza el trabajo y es responsable por su realización. Es quien ejecuta las tareas.
A	Aprobador	Este rol se encarga de aprobar el trabajo finalizado y a partir de este momento, se vuelve responsable de él. Debe asegurarse que se ejecuten las tareas.
C	Consultado	Este rol posee la información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información.
I	Informado	Este rol debe ser informado sobre el progreso y los resultados del trabajo.

5 ROLES Y RESPONSABILIDADES

A continuación, se presentan los roles que están involucrados en el proceso de la Política de Gestión de la capacidad.

Departamento de Informática (DI): Dueño del proceso de la Política de Gestión de la capacidad. Es responsable de asignar al funcionario con el rol de Administrador de la Capacidad.

Administrador de la Capacidad (AC): funcionario responsable de monitorear el desempeño y la capacidad de los componentes tecnológicos identificados para los procesos críticos del negocio.

Comité de TI (CTI): Conformado por los encargados de Unidad del DI, Jefe de Departamento DI y Analista encargado de administrar la Red, son los responsables de evaluar la Capacidad, dando su visto bueno para la adquisición de los requisitos establecidos, equipamiento o servicios necesarios.

ACTIVIDADES		ROLES		
		DI	AC	CTI
1	Realizar análisis de rendimiento actual	C/I	R/A	
2	Analizar demanda del negocio	C/I	R/A	
3	Identificar demandas futuras de capacidad	C/I	R/A	
4	Ejecutar herramientas de monitoreo	C/I	R/A	
5	Identificar y notificar desviaciones	I	R/A	
6	Determinar afectación de niveles de servicio	R/A	C/I	
7	Elaborar informe de monitoreo	C/I	R/A	
8	Analizar reportes de monitoreo	R/A	R	
9	Enviar propuesta de mejora	I	R/A	
10	Generar observaciones para mejora continua	C/I	R/A	
11	Definir compras de mejora	R		A

6 CONTROL NORMATIVO SSI

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

Código del Control	Identificación del Control	Requisito de control
A.12.01.03	Gestión de la capacidad	Se debe supervisar y adaptar el uso de los recursos y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.

7 PROCESO – ADMINISTRACIÓN DE CAPACIDAD DE LA INFRAESTRUCTURA DE TI

Con el fin de mantener un monitoreo constante de la capacidad del equipamiento en el Gobierno Regional Metropolitano el Departamento de Informática a establecido el Uso de una Aplicación de Licenciamiento libre llamado ZABBIX.

Mediante este el departamento deberá realizar un levantamiento del equipo y mantenerlo constantemente monitoreado con el fin de identificar posibles fallas en los mismos o baja en el rendimiento de los mismos.

De esta manera se podrá gestionar el Plan de compras o planificar la mejora de equipos de TI.

7.1 Métricas de desempeño

Se definió un formato para la descripción de las métricas para evaluar el desempeño de este proceso, a continuación se explica el detalle de cada uno de los campos de las tablas:

- **Índice:** Listado de equipos gestionados
- **Objetivo:** Se debe indicar claramente el motivo por el cual fue creada la métrica y las referencias que están siendo evaluadas.
- **Nivel de Riesgo:** Establece tres niveles de riesgo, los cuales son definidos previamente por el Departamento de Informática y que son específicos para cada métrica. Los niveles de riesgo se clasifican de la siguiente forma:

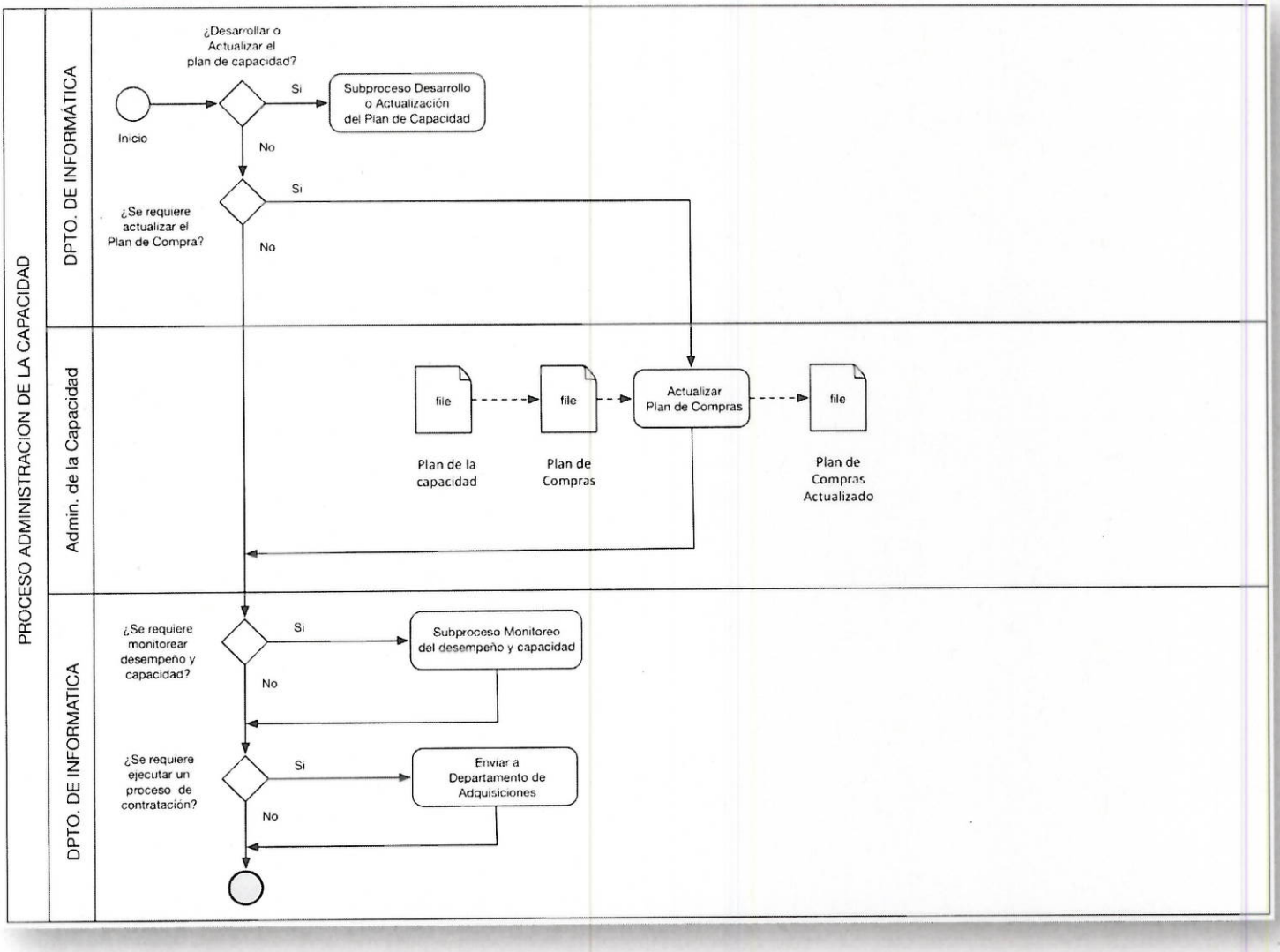
- **Unidad de medida:** Se utiliza para representar la unidad de medida con la que se expresa la métrica. Aunque es más común utilizar la unidad Porcentaje, también podrían existir unidades de medida de peso, velocidad y tiempo, entre otros.
- **Frecuencia:** La frecuencia hace referencia a la periodicidad con la que el cálculo de la métrica debe ser realizado. Valores comúnmente aceptados son horas, minutos, segundos, días, semanas, meses y años.
- **Descripción:** Relata en detalle aspectos propios de la métrica donde se pueden incluir temas sobre documentación relacionada y características de las mediciones. Se pueden hacer referencias a mejores prácticas, estándares, políticas, justificaciones y aclaraciones sobre otros campos del formulario.
- **Fórmula:** Operaciones básicas para conocer el resultado de la métrica.
- **Insumos:** Los insumos son una lista de requerimientos obligatorios que permitirán obtener la información necesaria para hacer el cálculo del resultado de la métrica. Estos insumos pueden ser el resultado de consultas a bases de datos, conteo manual de eventos, software y consultas de bitácoras, entre otros.

7.2 Proceso clave en la Administración de Capacidad

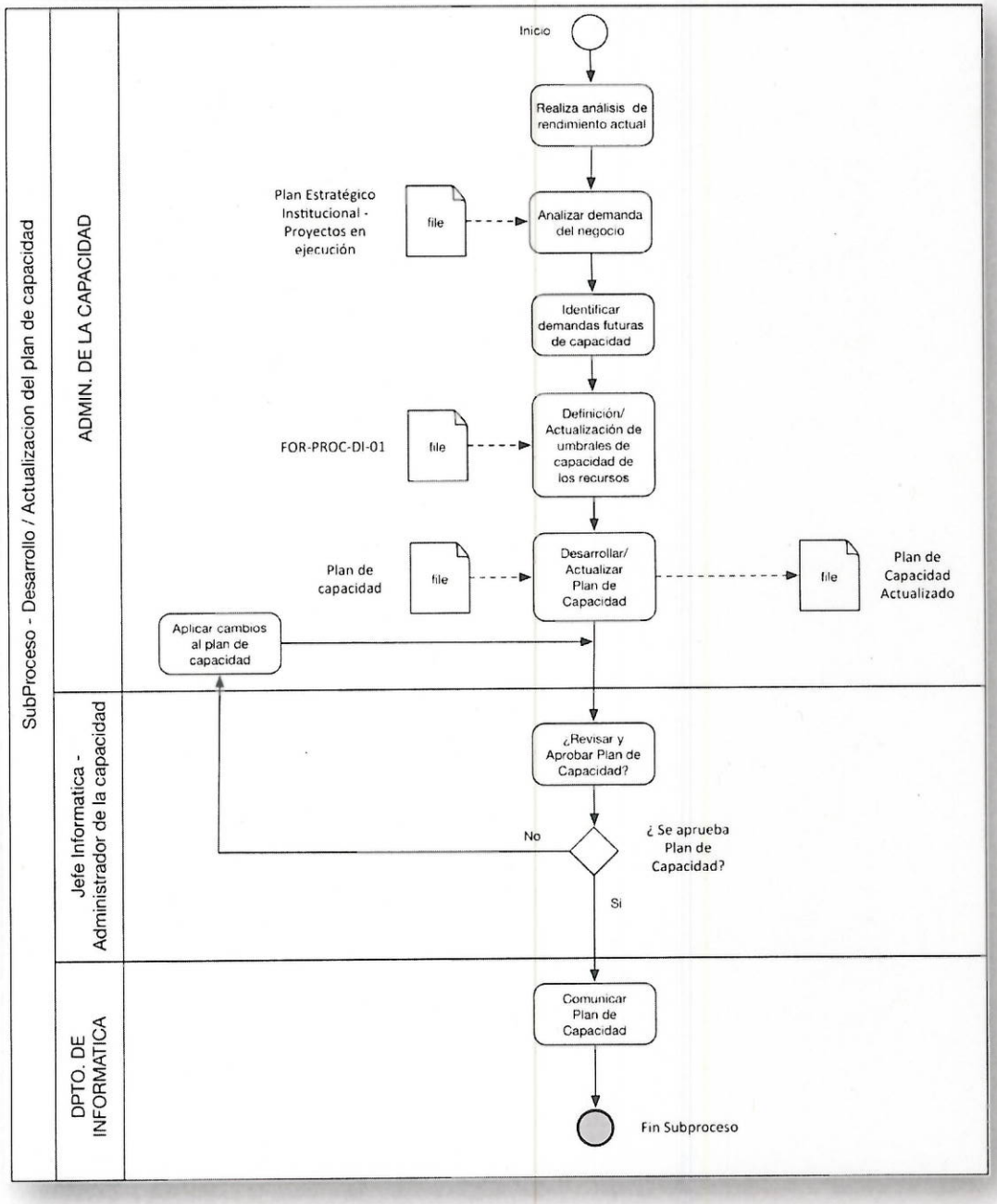
ID	ACTIVIDADES	RESPONSABLE
1	Realizar plan de capacidad mediante el Levantamiento de equipamiento según FOR-PROC-DI-01 y FOR-PROC-DI-02	DI
2	Ingreso del Equipamiento identificado en Zabbix	AC
3	Ingreso de Metrica de valores máximos o minimos	AC
4	Ejecutar herramientas de monitoreo	AC
5	Identificar y desviaciones	AC
6	Determinar afectación de niveles de servicio si es critico	AC
7	Elaborar informe de monitoreo anual	AC
8	Analizar reportes de monitoreo	CTI
9	Determinar Mejoras	CTI
10	Actualiza plan de compras	
11	Definir compras de mejora	DI
12	Envia a adquisiciones si corresponde	DI

8 DIAGRAMAS DE FLUJO DE LOS PROCESOS

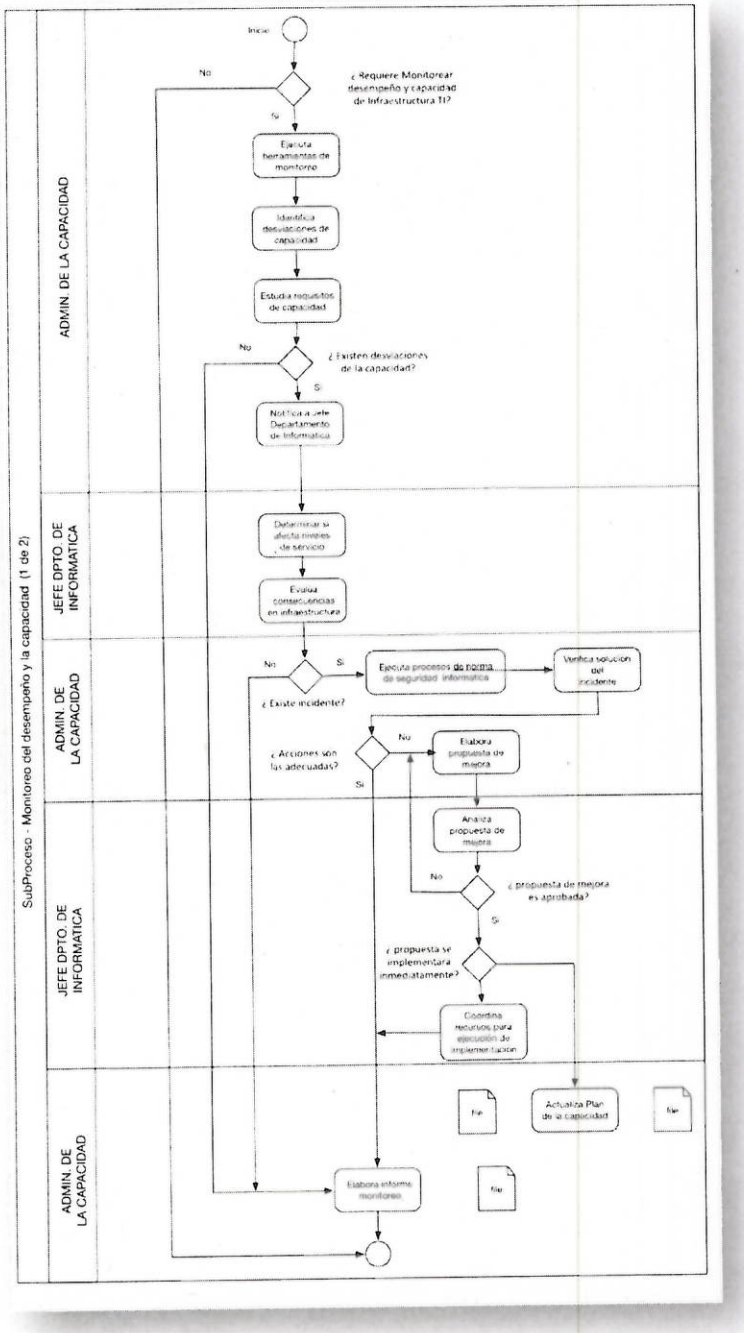
8.1 Proceso: Administración de Capacidad

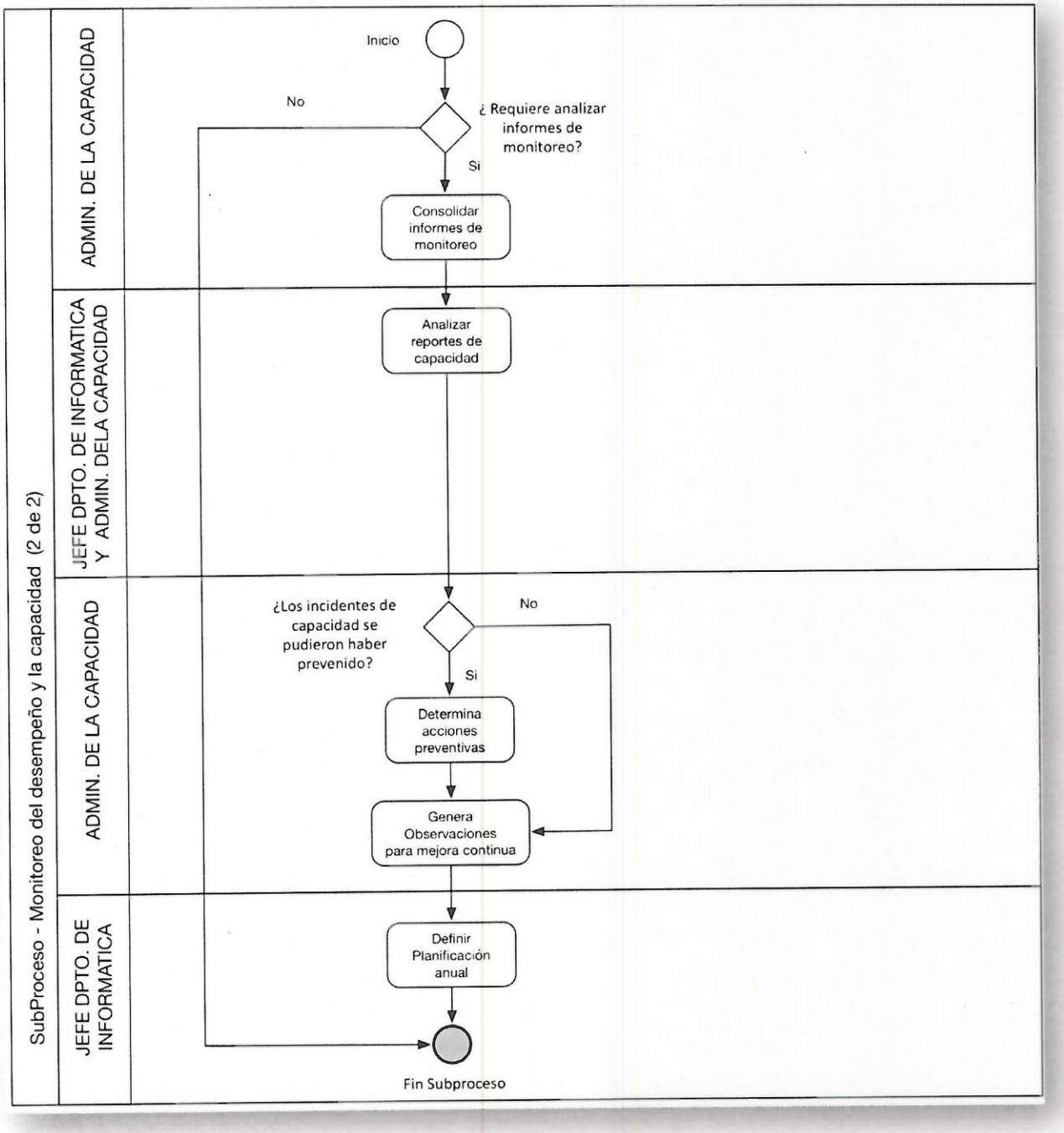


8.2 Subproceso – Desarrollo / Actualización del Plan de Capacidad



8.3 Subproceso – Monitoreo del desempeño y capacidad




SubProceso - Monitoreo del desempeño y la capacidad (2 de 2)
ADMIN. DE LA CAPACIDAD
JEFE DPTO. DE INFORMATICA Y ADMIN. DELA CAPACIDAD
ADMIN. DE LA CAPACIDAD
JEFE DPTO. DE INFORMATICA
Inicio
¿ Requiere analizar informes de monitoreo?
No
Si
Consolidar informes de monitoreo
Analizar reportes de capacidad
¿Los incidentes de capacidad se pudieron haber prevenido?
No
Si
Determina acciones preventivas
Genera Observaciones para mejora continua
Definir Planificación anual
Fin Subproceso

9 ANEXOS

9.1 Formulario FOR-PROC-DI-01

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

Formulario FOR-PROC-DI-01

Componentes críticos y requisitos de capacidad y desempeño

Elaborador por:		Fecha de Elaboración:	

N° de servidor	
Nombre	
Máquina Virtual	
Dir. IP	
DIR. MAC	
Nombre host	
Sistema Operativo	
Servicios en escucha	
Descripción	

9.2 Formulario FOR-PROC-DI-02

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

Formulario FOR-PROC-DI-02

TABLA SWITCHS

La Tabla deberá contener a lo menos las siguientes descripciones

Elaborador por:		Fecha de Elaboración:	

Marca
Modelo
ID producto
Nº serie
Default user
Default pass
Default IP
USER
PASS
IP
Nombre Switch
Pass telnet

10 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.

11 PERIODICIDAD DE EVALUACION Y REVISIÓN

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

12 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política de gestión de la capacidad.

13 REGISTRO, 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 V.	11	2-08-2018	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 9 por Registro de Operación y se señala que el informe será de carácter anual Se cambia título 11 por Periodicidad de evaluación y revisión
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	13	17-11-2021	Se agrega capítulo 12 formalización externa
07	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

14 FORMALIZACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Paulo Mendoza R.** Encargado Unidad de Soporte **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

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			