Plan de continuidad

1 INDICE

2 INTRODUCCION

El Gobierno Regional Metropolitano reconoce que existen amenazas significativas ante la posibilidad de la ocurrencia de un incidente o desastre que afecte la operación, como también la necesidad de recuperarse en el menor tiempo posible, garantizando la continuidad del Servicio.

La Administración del Plan de Continuidad de Negocios se deberá implementar, para responder organizadamente a eventos que interrumpen la normal operación de sus procesos y que pueden generar impactos sensibles en el logro de los objetivos.

Nuestro país es un país acostumbrado a los desastres naturales, es por esto que el Plan de Continuidad es una herramienta que mitiga el riesgo de no disponibilidad de los recursos necesarios para el normal desarrollo de las operaciones, ofreciendo como elementos de control la prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal. Este plan de Continuidad representa un amplio espectro de actividades enfocadas a sostener y recuperar servicios críticos de TI después de una emergencia.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Asegurar que el Gobierno Regional Metropolitano esté preparado para responder a emergencias, recuperarse de ellas y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios críticos para su operación.

3.2 OBJETIVOS ESPECIFICOS

- Lograr un nivel de preparación frente a incidentes que permita asegurar que puede proteger la integridad de las personas y bienes del Servicio en forma adecuada, realizando una buena administración de la crisis.
- Minimizar la frecuencia de interrupciones de la operación de los procesos del negocio.
- Asegurar una pronta restauración de las operaciones afectadas por el evento.

Minimizar las decisiones a tomar en caso de contingencia para evitar cometer errores.

4 ALCANCE

La Administración del Plan de Continuidad de Negocios es una disciplina que prepara al Servicio para poder continuar operando durante un incidente o desastre, a través de la implementación de un plan de continuidad, el cual contempla los lineamientos de la administración, el desarrollo de fases que componen el plan de continuidad y las metodologías definidas por el Gobierno Regional Metropolitano para su ejecución, como también el desarrollo de los planes de contingencia, que se realizan de acuerdo con las prioridades establecidas por el Servicio y se aplicará a todo los funcionarios del Gobierno Regional Metropolitano, no importando su calidad jurídica, asi como también a los proveedores que presten algún tipo de servicio a este Gobierno Regional.

De la misma manera, el desarrollo de los planes de continuidad se apoya en las capacidades con las que cuenta el Gobierno Regional Metropolitano para enfrentar situaciones que amenacen o afecten la integridad física de sus funcionarios e instalaciones, tales como el Plan de Emergencias, Instructivo Correctivo Preventivo, Política de Gestión de Incidentes de Seguridad y los demás sistemas de gestión.

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.17.01.01	*Planificacion de la continuidad de la Seguridad de la Información.*	*La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestion de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.*
A.17.01.02	*Implementación de la continuidad de la seguridad de la información.*	*La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.*
A.17.01.03	*Verificacion, revision y evaluacion de la continuidad de la seguridad de la información.*	*La organización debe verificar, de manera periódica, los controles de la continuidad de la seguridad de la información definida e implementada para asegurar que ellos son válidos y eficaces durante situaciones adversas.*
A.17.02.01	*Disponibilidad de las instalaciones de procesamiento de la informacion.*	*Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad.*

6 DEFINICIONES

Administración del Plan de Continuidad de Negocios: Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio.
Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.

Incidente de Trabajo: Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.

Problema de Continuidad de Negocio: Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

Planes de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de Continuidad de Negocio (PCN): Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Plan de Recuperación de Desastres (DRP): Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso.

Amenaza: Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.

Vulnerabilidad: Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros.

Riesgo: Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para el Servicio.

Frecuencia: Estimación de ocurrencia de un evento en un período determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.

Impacto: Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperabilidad.

Control: Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.

Riesgo inherente: Es el cálculo del daño probable a un activo de encontrarse desprotegido, sin controles.

Riesgo residual: Riesgo remanente tras la aplicación de controles.

7 CAUSAS DE INTERRUPCION

Los planes de contingencia se definen de acuerdo con las causas de las posibles interrupciones y a partir de ellas se referencian las acciones a seguir en caso que las mismas se presenten. Estas se pueden unificar en los siguientes escenarios:

Ausencia de Personal: Se presenta cuando el funcionario o contratista que ejecuta el proceso no puede asistir a trabajar para desarrollar las actividades propias de su cargo.

No acceso al sitio normal de trabajo: Se presenta cuando por algún evento como desastre natural, enfermedad contagiosa, actividad terrorista, problemas de transporte, huelgas, entre otros, el personal no puede acceder a su lugar de trabajo para desarrollar las actividades propias de su cargo. En este caso y con el ánimo de no interrumpir la operación del proceso crítico se debe contar con un sitio alterno de trabajo, el cual puede ser:

- Suministrado por el Servicio, Ejemplo: Otra sede.
- Suministrado por un proveedor, contratista o aliado estratégico.

Caída de los sistemas tecnológicos: Se presenta cuando el hardware y/o software presenta falla(s) o cuando haya interrupción prolongada de las comunicaciones, ocasionados por: datos corruptos, fallos de componentes, falla de aplicaciones y/o error humano.

No contar con los Proveedores Externos: Se presenta cuando una o varias actividades del proceso crítico son realizadas por el proveedor y cualquier falla de éste, generaría la no realización efectiva del proceso. En este caso se debe garantizar que en el contrato con el proveedor se especifique la existencia de un Plan de Continuidad del Negocio documentado, adicional, sea probado en conjunto con los funcionarios del Servicio y aprobado por el Gobierno Regional Metropolitano.

Para cualquier contacto con proveedores externos remitirse a documento "INSTRUCTIVO CORRECTIVO Y PREVENTIVO CONTRA FALLASDE ENERGÍA Y OTRAS FALLAS DE SERVICIOS" código INS-SSI-001.

8 PLANIFICACION DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION

El objetivo de la administración de continuidad del negocio es planificar las acciones necesarias para responder de forma adecuada ante un incidente de trabajo, desde el momento en que se declare la contingencia hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto sobre el negocio.

Los lineamientos se sustentan en un conjunto de principios que han sido formulados basándose en las necesidades del negocio y en el entendimiento de los riesgos asociados, ellos son:

- El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.

- Todo el personal del Servicio debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Contingencia del Negocio.

- En caso de presentarse un incidente significativo se deben aplicar los mecanismos de comunicación apropiados, tanto internos como externos, de acuerdo con la Política de Gestión de Incidentes de Seguridad.

- Las etapas de la Administración de PCN deben ser ejecutadas por cada uno de los Departamentos del Servicio, con la guía y coordinación del Director de Continuidad.

- Los Jefes de Departamento deben designar un Líder de Plan de Continuidad del Negocio, quien es responsable de apoyar las actividades del Programa de Plan de Continuidad de Negocios para el área que representa.

- Las diferentes etapas que conforman la fase de Prevención deben ser ejecutadas con la siguiente frecuencia:

  - El monitoreo a los riesgos de continuidad se efectuará de manera anual.
  - Pruebas anuales deben realizarse en lo posible a todas las estrategias de contingencia definidas.
  - Las estrategias se revisarán cada vez que el Líder del Proceso lo considere o como resultado del análisis de riesgos se determine el ajuste o implementación de estrategias de contingencia.

9 IMPLEMENTACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO

Para asegurar una adecuada administración de la continuidad del negocio el Servicio implementó una estructura, que incluye la definición de los roles y responsabilidades, tanto de los Líderes de Proceso, como de las Jefaturas de División y Jefes de Departamentos. Esa administración está conformada por:

9.1.1 COMITE DE CONTINGENCIA

La gestión de la continuidad de negocio requiere de una estructura organizacional, encargada de promover el desarrollo de los lineamientos definidos en este capítulo. El Comité de Contingencia, será el responsable de administrar la continuidad de la operación del Servicio. A continuación, se mencionan los integrantes del comité, su rol y responsabilidad frente a este item:

COMITÉ DE CONTINGENCIA	ROLES DE CONTINGENCIA
Jefatura División Administración y Finanzas	Director de Continuidad
Jefe Departamento Servicios Generales	Director Subrogante Líder de Administración / Recuperación Infraestructura Física
Prevencionista de Riesgo	Lider de Implementacion de medidas correctivas
Jefe Departamento Informática	Líder de Recuperación Tecnológica
Encargado Unidad Soporte	Coordinadores de Recuperación
Encargado Unidad de Desarrollo	
Jefe Departamento de Gestión Documental	
Encargado de Infraestructura	
Jefe Departamento Auditoria Interna	Tareas de apoyo, control y cumplimiento
Jefe Departamento Jurídico	
Jefe Departamento de Abastecimiento	
Jefe Departamento de Finanzas	
Jefe Departamento de Gestión de Personas	

En caso en que el Comité active el plan de continuidad, podrá invitar a otros funcionarios responsables de actividades que impacten la operación del Servicio.

10 ROLES Y RESPONSABILIDADES

A continuación, se describen los roles y responsabilidades de los integrantes del Comité en lo respectivo al plan de continuidad; vale aclarar las personas nombradas como principales y sus subrogantes tienen las mismas responsabilidades.

Director de Continuidad

El Director de Continuidad es el encargado de dirigir y liderar todas las actividades del plan de continuidad del Servicio. Es responsable de declarar la contingencia ante el escenario de interrupción de lugar de trabajo, con base en las decisiones tomadas por el Comité de Contingencia o en situaciones donde amerite realizar su activación inmediata.

Responsabilidades

- Delegar de manera expresa en el Comité de Contingencia, la responsabilidad de actualizar, mantener y probar el plan de continuidad.
- Evaluar y aprobar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia del Servicio.
- Liderar las reuniones del Comité de Contingencia.
- Advertir sobre nuevos riesgos que afectan la continuidad de la operación normal del Servicio y que ponen al descubierto debilidades del plan de continuidad.
- Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia.
- Velar por la seguridad del personal que actúa en el área del evento.
- Establecer los objetivos de recuperación y activar el plan de continuidad ante el escenario de interrupción de lugar teniendo en cuenta el resultado de la evaluación
- Velar por la ejecución del debido análisis causa – raíz del evento que ocasionó la contingencia.

Director subrogante de Continuidad

Asumir el rol y cumplir con las responsabilidades de Director de Continuidad cuando éste no se encuentre disponible.

Es responsable de declarar la contingencia ante un incidente tecnológico de algún aplicativo (contingencia específica), con base en el análisis realizado por el Departamento de Informática.
Realizar las actividades que le sean asignadas por el Director de Continuidad.

Líder Administrativo

El Líder Administrativo ayuda a coordinar los aspectos logísticos internos cuando el Servicio se encuentre operando bajo contingencia. Es quien ayuda a gestionar en cada una de las instalaciones el suministro de elementos esenciales para asegurar el desarrollo de la operación.

Responsabilidades

- Coordinar el suministro de elementos esenciales como transporte, servicios básicos, recursos de infraestructura y papelería.
- Gestionar la consecución y adecuación de los centros alternos de operaciones según la Política de Gestión de Incidentes de Seguridad y el Plan de emergencias.
- Mantener informado al Comité de Contingencia sobre incidentes por falta de suministros.

Líder de Recuperación Tecnológica

Es la persona encargada de liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas. Es el contacto directo entre el Departamento de Informática y el Comité de Contingencia; además, apoya las decisiones tomadas por el Director de Continuidad durante la declaración y activación de la contingencia.

Responsabilidades

- Liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas.
- Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal del Servicio y que ponen al descubierto debilidades del plan de continuidad.
- Mantener comunicación constante entre Coordinadores de Recuperación del Negocio durante el estado de contingencia.
- Colaborar en la comunicación a los proveedores de los temas o servicios de su competencia, sobre el estado de contingencia en que se encuentra el Servicio, esto previa decisión y autorización del Director de Continuidad, mediante comunicado elaborado en conjunto con la Unidad de Comunicaciones.
- Entregar los reportes correspondientes al Comité de Contingencia sobre el estado de la recuperación.
- Velar por la actualización de la Estrategia Tecnológica en los casos que se presenten situaciones como: cambios en los aplicativos, cambio en la infraestructura, roles y responsabilidades, disponibilidad de los recursos, entre otros.
- Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos en las mismas.
- Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas e implementadas.

Coordinadores de Recuperación

Los Coordinadores de Recuperación son personas encargadas de liderar la recuperación de procesos críticos de TI, basados en las estrategias de contingencia. Son el contacto directo entre los procesos de TI y el Lider de Recuperacion Tecnológica; además, colaboran con las decisiones tomadas por él y el Comité de Contingencia durante la declaración y activación de la contingencia.

Responsabilidades

- Liderar las reuniones del equipo de recuperación, para diagnosticar y evaluar las interrupciones que están afectando la prestación del servicio.
- Ejecutar los planes de contingencia ante el incidente presentado.

- Identificar los posibles riesgos que afectan la continuidad de la operación normal del Servicio y que ponen al descubierto debilidades del plan de continuidad.
- Mantener comunicación constante durante el estado de contingencia.
- Colaborar en la comunicación a los proveedores sobre el estado de contingencia en que se encuentra el Servicio, esto previa decisión y autorización del Líder de Recuperación.
- Entregar los reportes correspondientes al Lider de Recuperacion y éste al Comité de Contingencia sobre el estado de la recuperación de sus áreas.
- Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos en la misma.
- Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas e implementadas.

Responsable de tareas de apoyo, control y cumplimiento

Responsabilidades

- Realizar las actividades que le sean asignadas durante la declaración de contingencia.
- Advertir sobre riesgos que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del plan.

10.1.1.1 LINEA DE SUCESION

Se identifica los responsables asignados a los diferentes roles del plan de continuidad y sus alternos en caso de que estos no puedan asumir las actividades y/o tareas.

CARGO PRINCIPAL	CARGO SUBROGANTE
Jefatura División Administración y Finanzas	Jefe Departamento Servicios Generales
Jefe Departamento Servicios Generales	Prevencionista de riesgo
Prevencionista de riesgo	Asistente Servicios Generales
Jefe Departamento Informática	Analista Departamento de Informática
Encargado Unidad Soporte	Analista Departamento de Informática
Encargado Unidad de Desarrollo	Analista Unidad de Desarrollo
Jefe Departamento de Gestión Documental	Asistente Depto. Gestión de Documental
Jefe Departamento Auditoria Interna	Subrogante Dpto. Auditoría
Jefe Departamento Jurídico	Subrogante Dpto. Jurídico
Jefe Departamento de Abastecimiento	Subrogante Dpto. de Abastecimiento
Jefe Departamento de Finanzas	Subrogante Dpto. de Finanzas
Jefe Departamento de Gestión de Personas	Subrogante Dpto. de Gestión de Personas

Línea de sucesión

10.1.2 LIDERES PCN

Cada área cuenta con un Líder de PCN, quien tiene las siguientes responsabilidades en la administración del plan de continuidad sobre los procesos / procedimientos a cargo:

- Actuar como punto focal del área para todos los asuntos de continuidad del Servicio.
- Cumplir con las actividades y fechas establecidas del Cronograma de PCN.
- Mantener informados a todos los funcionarios de sus respectivas áreas, los planes de contingencia que les compete.
- Asegurar la aplicación correcta del PCN.
- Revisar el impacto en el área durante el incidente.

La tabla con el detalle de los funcionarios con rol Líder PCN se encuentra en el anexo "Equipo de trabajo del PCN".

10.1.3 Unidad de Prevención de Riesgo

La Unidad de Prevención de Riesgo tiene a cargo las siguientes funciones en el plan de continuidad:

- Definir e implementar los instrumentos, metodologías y procedimientos tendientes a gestionar efectivamente el PCN.
- Suministrar los programas de capacitación de PCN.
- Coordinar, apoyar y hacer seguimiento a la gestión de PCN en cada área.
- Guiar en el desarrollo de las diferentes etapas del PCN.

10.2 ELEMENTOS QUE CONFORMAN LA ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO

La Administración del Plan de continuidad del Negocio está conformada por los siguientes elementos:

- Plan de Emergencias, ante emergencias de carácter interno o externo.
- Instructivo Correctivo Preventivo, ante fallas de servicios.
- Política de Gestión de Incidentes de Seguridad, para el análisis de eventos de seguridad.

Estos elementos complementan el plan de continuidad y los procesos que contempla este plan.

10.3 ENTRENAMIENTO

En el éxito del Plan de Continuidad es fundamental contar con la participación y el compromiso del personal involucrado en el mismo. La administración de continuidad debe asegurar que todos los funcionarios involucrados reciban entrenamiento sobre los procedimientos a seguir en caso de incidentes o desastres, lo cual permite tomar conciencia de la importancia del plan, ya que serán los encargados de ponerlos en funcionamiento en caso de presentarse un evento no deseado. A los Jefes de Departamento también se les capacita y concientiza, ya que son los responsables de la correcta ejecución de los planes.

10.4 ETAPA DE ESTRATEGIA DE CONTINUIDAD

CONCEPTO

Corresponden a las acciones que se deben tomar con el objetivo de restablecer las operaciones del negocio, en el plazo determinado, una vez que ocurra alguna interrupción o falla en los procesos o funciones críticas indicada en el capítulo 7 "CAUSAS DE INTERRUPCION".

Es necesario identificar las diferentes estrategias de continuidad y seleccionar las más adecuada para la Institución, para lo cual el Líder de PCN de cada área junto con el Profesional del tema en la Unidad de Prevención de Riesgo analizarán las variables de:

- La criticidad del proceso a proteger
- El costo de la estrategia
- El tiempo de recuperación objetivo (RTO)

OBJETIVOS

- Permitir al Servicio trascender ante la crisis y recomponerse en el menor tiempo posible, con un aceptable nivel de servicio.
- Garantizar que los Funcionarios:
  - ✓ Estén protegidos
  - ✓ Comprenden su papel
  - ✓ Saben a dónde ir
  - ✓ Saben qué hacer
  - ✓ Saben qué recursos necesitan
  - ✓ Entienden la secuencia de las tareas críticas

- Ayudar a planificar la recuperación y reanudación de las operaciones.

- Validar asuntos de recuperación del Servicio, como:

  - ✓ Necesidades de telecomunicaciones durante y después del desastre.
  - ✓ Lugar alterno para continuidad/recuperación y reanudación.

ALCANCE

La selección de los métodos alternativos de operación que deben ser utilizados ante una interrupción para mantener o reanudar las actividades del Servicio y sus dependencias.

Las diferentes situaciones para las cuales se deben definir estrategias de recuperación son:

- Ausencia de personal
- Sitio alterno
- Fallas tecnológicas

ESTRATEGIAS POR AUSENCIA DE PERSONAL

Se presenta cuando el funcionario que ejecuta los procesos no puede asistir a trabajar para desarrollar las actividades propias de su cargo. Se debe establecer la siguiente cadena de comunicación:

El funcionario ausente activa la Cascada Telefónica y se comunica con el Jefe inmediato.

El Jefe inmediato comunica el evento al Jefe del Departamento y activa la contingencia por "Ausencia de Personal".

Distribuye procesos claves o asigna funciones al funcionario subrogante. De ser necesario, solicita al Encargado de Seguridad la reasignación de perfiles, a través correo electrónico para acceso a carpetas compartidas o información privilegiada.

El Jefe inmediato confirma al Jefe del Departamento la continuidad exitosa de los procesos.

El documento denominado Cascada Telefónica cuenta con la información básica de los funcionarios y proveedores con el ánimo de utilizarlos en un evento de contingencia, como es:

Funcionarios: Mantener la información de los funcionarios permite comunicarse con ellos en el evento que se encuentren fuera de las instalaciones.

Proveedores: Para comunicarse con los proveedores en un sitio alterno donde se carece de la información de contacto.

Cada Unidad cuenta con la información de "Cascada Telefónica", la cual está conformada por:

- Cascada: Contiene los datos básicos de los funcionarios: nombres, cargo, número de teléfono personal. Se encuentran descritos en el orden que serán llamados ante un evento.
- Personal mínimo: En este se relaciona las personas críticas sobre las cuales depende la ejecución de la actividad. Se encuentran relacionados los funcionarios que participarán en la contingencia por cada procedimiento.
- Contacto Externo: Relaciona los datos básicos de los proveedores: nombre del proveedor, nombre del procedimiento/proceso del Servicio en el cual participa, nombre del contacto personal, teléfono de la oficina y móvil y correo electrónico.

En el Anexo "Cascada Telefónica", se encuentra dicho formato. La información de cada Unidad la conserva el Líder de PCN y la consolidación de la misma reposa en la Unidad de Prevención de Riesgo.

11 DISPONIBILIDAD DE LAS INSTALACIONES, ESTRATEGIA DE SITIO ALTERNO

La alternativa de traslado del personal se presenta en el evento que los funcionarios no puedan acceder a las instalaciones del Gobierno Regional Metropolitano y de esta manera se afronta un evento de contingencia permitiendo la continuidad de las operaciones de los procesos críticos del Gobierno Regional Metropolitano desde un sitio alterno de operación.

El Gobierno Regional Metropolitano deberá contar con un sitio alternativo según lo indiquen las condiciones de operación.

Las alternativas deben contemplar:
Servicios básicos, servicios de Internet, servicios telefónicos (móviles o fijos via IP), red eléctrica disponible para la cantidad de funcionarios definida por el Comité de Contingencia.
Un lugar definido para la atención de público y recepción de documentos de instituciones privadas como también de otros Servicios Públicos

Instalaciones en Sitios Alternos

El Gobierno Regional Metropolitano deberá contar con a lo menos un Sitio Alterno disponible en caso de desastres naturales, inundaciones, o cualquier situación que impida el normal desarrollo de las actividades de su personal en las dependencias de calle Bandera 46. Para esto trasladará un número definido de funcionarios hacia el Sitio Alterno.

El sitio debe contar con: Servicios de Internet, computadores, escritorios, sillas, Servicio de Telefonia, Servicios Básicos, entre otros.

El sitio alterno deberá permitir que el grupo definido como Personal Crítico pueda trabajar y seguir operando en condiciones suficientes como para que el Servicio pueda seguir funcionando.

Una vez ubicado el personal crítico en las instalaciones del sitio alterno se procederá a levantar el servidor de respaldo.

SALA DE SERVIDORES EN SITIO ALTERNO

Ante la eventualidad de una falla en la Sala de Servidores, este Gobierno Regional deberá contar con una sala de servidores como sitio alterno definida en un Sitio diferente al propio o provista por un tercero de manera de poder continuar con las operaciones de forma normal y minimizar así los riesgos de operación.

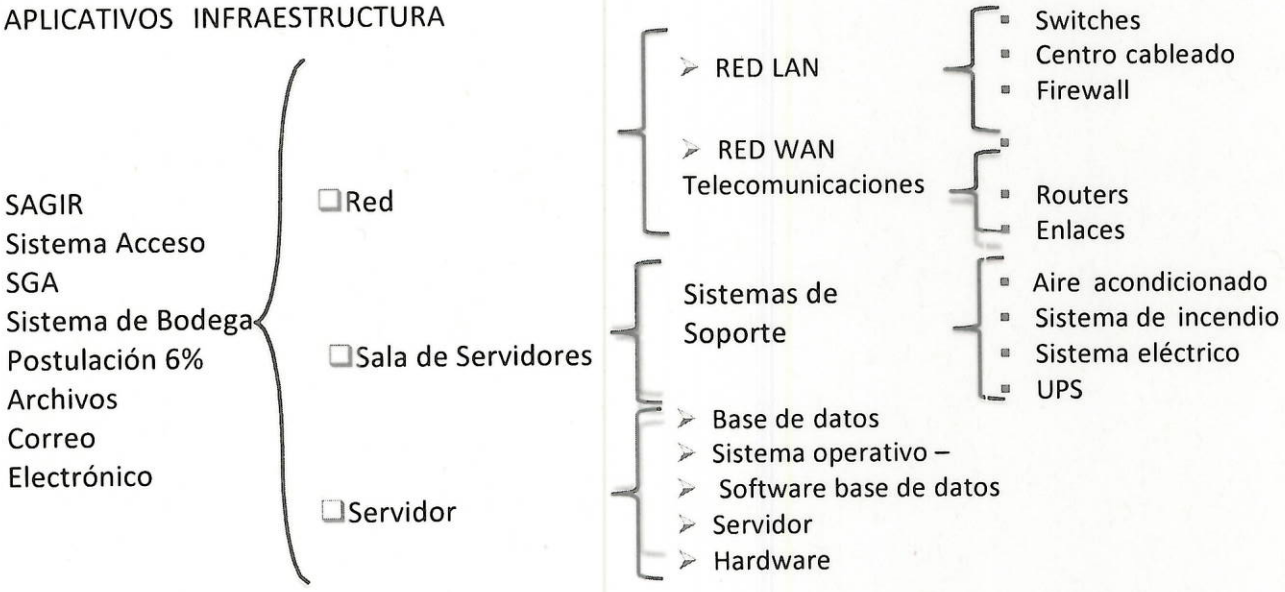
En esta sala deberán estar todos los equipamientos necesarios para poder operar sin problemas, esto es, una réplica o redundancia de los Servidores y equipos de comunicaciones listos para operar

También deberá contar con una FO de respaldo para disponer de alta disponibilidad de los servicios de Internet la que deberá ser suministrada por el proveedor de servicios de Internet y Telecomunicaciones. Esta segunda FO deberá venir de nodos diferentes.

ESTRATEGIA TECNOLOGICA

La contingencia se presenta cuando el hardware y/o software presenta fallas, o por interrupción prolongada de telecomunicaciones.

El Departamento de Informática tiene estructurado el siguiente Plan de Continuidad para los aplicativos e infraestructura del Servicio:



Este cuadro presenta las partes de infraestructura tecnológica que deberá ser replicada en el sitio alternativo.

Para el desarrollo de la recuperación de la estrategia tecnológica remitirse al anexo "Estrategia Tecnologica".

- Estrategia Tecnológica de Base de Datos
- Estrategia Red WAN
- Estrategia Red LAN – Switches
- Estrategia tecnológica de software servidor
- Estrategia por problemas en los sistemas

11.1 ETAPA DE PRUEBAS

CONCEPTO

Consiste en probar la efectividad de las estrategias diseñadas y permitir el continuo mejoramiento del PCN del Servicio. Esta etapa le da a la Institución la oportunidad de identificar y prevenir problemas y fallas con su plan de continuidad de manera que puedan ser atendidas, preparando el Servicio para la emergencia real.

Con el fin de probar la efectividad del Plan de Continuidad en lo que respecta a los sitios alternos es que el Gobierno Regional Metropolitano hará pruebas desde los sitios alternos para comprobar la operatibilidad durante la contingencia.

OBJETIVOS

- Practicar los procedimientos ante un incidente o desastre.
- Identificar áreas que necesitan mejora.
- Permitir al PCN permanecer activo, actualizado, entendible y usable.
- Demostrar la habilidad de recuperación.

ALCANCE DE LAS PRUEBAS

Las pruebas deben ejecutarse durante un tiempo en el que las afectaciones a la operación normal sean mínimas y deben comprender los elementos críticos y simular condiciones de proceso, aunque se realicen fuera del horario laboral del Servicio. Las pruebas deben incluir las siguientes tareas:

- Verificar la totalidad y precisión del Plan.
- Evaluar el desempeño del personal involucrado.
- Evaluar la coordinación entre los miembros del grupo de contingencia, proveedores y otros terceros.
- Identificar la capacidad de recuperar registros e información vital.
- Medir el desempeño de los sistemas operativos y computacionales.

Durante esta etapa se debe establecer un programa de pruebas con escenarios simulados, planeados en el tiempo, teniendo en cuenta los requerimientos de cada prueba y con una revisión exhaustiva de los resultados de las mismas, para generar mejoras a los planes.

Para esto se trasladará un número definido de funcionarios hacia el Sitio Alterno.

- Las pruebas se harán con computadores portátiles y se conectaran a través de la red Local del Sitio Alterno a la Red Lan del Gobierno Regional Metropolitano.
- Se harán pruebas de comunicacion hacia los servidores, específicamente hacia aplicaciones como SAGIR, SGA, Postulacion 6% y Carpetas de Archivos alojadas en los servidores.

- Se hará una simulación de compras al Sistema de Mercado Publico para verificar que en casos de desastres aun esta operativa la plataforma.
- Se harán pruebas de correo electrónico.

TIPO DE PRUEBAS

En la siguiente grafica se ilustra la metodología que se debe utilizar para la realización de las pruebas del plan de continuidad de negocio del Gobierno Regional Metropolitano:

TIPO DE PRUEBA	TECNICA UTILIZADA	OPERACIÓN
Integrada	• Creación de un escenario • Seguimiento en vivo de todas las estrategias de recuperación • Con previo aviso. • Apoyo de los proveedores de recuperación	Prueba integrada con todos los elementos que hacen parte del plan de contingencia.
Componentes	• Creación de un escenario • Seguimiento de las estrategias de recuperación • Con previo aviso.	Se ejecutan las estrategias y procedimientos de recuperación de cada uno de los componentes de la infraestructura tecnológica.
Escritorio	• Con previo aviso. • Creación de un escenario.	Se realiza un ejercicio de papel de un escenario de desastre que toma lugar en un salón de conferencia.

PLAN DE PRUEBAS

Para la realización de una Prueba de Estrategia de Continuidad es necesario diligenciar el documento "Plan de Pruebas", conformado por los siguientes pasos:

- Fecha de las pruebas: La fecha será definida y comunicada con a lo menos 15 dias de anticipación
- Horario: El horario y tiempo de la prueba dependerá de los tiempos que se demore la conexion, pero empezará a contar desde las 9 am.
  Una vez hecha la conexión, se mantendrán las pruebas por un tiempo mínimo de dos horas con una finalización aproximada de las 14 horas.

- Notificacion: La notificación respecto de la Prueba de Contingencia del Plan de Continuidad será hecha via correo electrónico a todos los funcionarios

- Guion de pruebas: Es el documento mediante el cual se plasma la intención de efectuar la revisión de la estrategia de continuidad estimada para el proceso o servicio determinado, donde se relacionan aspectos de: Objetivo y alcance de la misma, el escenario de interrupción, los resultados esperados, los integrantes de las pruebas y los riesgos asociados a la ejecución de la prueba. Este documento debe desarrollarlo previo a la ejecución de la prueba el Líder de PCN responsable del proceso a probar con la guía del funcionario encargado en la Unidad de Prevención de Riesgo.

- Paso a paso de la planeación: Este documento relaciona las actividades a efectuar durante la prueba, indicando además los responsables de realizar tales actividades, así como los recursos mínimos necesarios y los tiempos de su realización, para la estimación completa del tiempo de la prueba. Adicional, se deben mencionar los aspectos adicionales que son necesarios para la adecuada realización de la prueba. Al igual que en el anterior ítem, este informe debe ser adelantado previo a la ejecución de la prueba por el Líder de PCN responsable del proceso a probar con la guía del funcionario encargado en la Unidad de Prevención de Riesgo.

- Paso a paso de la ejecución: Este documento contiene las actividades realizadas en el desarrollo de la prueba, que deben ser semejantes a las planeadas a menos que se presenten algún incidente dentro de la prueba. Adicionalmente, se describen los recursos mínimos necesarios, los responsables y los tiempos de ejecución de las actividades. Este informe es elaborado en el momento de la prueba por el Líder de PCN responsable del proceso a probar con la guía del funcionario encargado de la Unidad de Prevención de Riesgo.

- Paso a paso del retorno: En este reporte se relacionan las actividades que se ejecutan para retornar a la operación normal, caso devolución a los puestos de trabajo, captura de las operaciones que no se procesaron en un aplicativo, entre otras.

- Mitigacion del Impacto en el Público: Para mitigar el impacto en la atención de público se dejará un aviso publicado en que se señale el lugar y dirección del Sitio Alterno, con su respectivo horario de atención indicando que se están haciendo pruebas en caso de desastres que asi lo requieran de manera de mantener la continuidad del Servicio

- Encuesta de satisfacción: Este informe lo realizan diferentes integrantes de la prueba, donde se busca determinar el grado de satisfacción de la prueba. La conforman aspectos como: duración de la prueba, preparación de la prueba y la comunicación de la misma, y dificultades que se identificaron.

- Acta de reunión: En este documento se establecen los objetivos, conclusiones de la prueba, las actividades sobresalientes resultantes y/o pendientes a considerar, los logros obtenidos en la

ejecución de la prueba y los riesgos asociados identificados en la ejecución de la prueba, así como las acciones mitigantes que mejorarán la estrategia de continuidad del proceso revisado. Este informe debe ser firmado por cada uno de los integrantes a la prueba.

Luego de cada prueba el Encargado de Seguridad debe enviar copia del documento "Acta de reunión" dirigido a los participantes y al jefe responsable de proceso.

Para la finalización y control de las pruebas remitirse al anexo "Resultado Pruebas de Sitio Alterno"

12 ETAPA DE MANTENIMIENTO

CONCEPTO

Es la revisión periódica de lineamientos, estrategias, técnicas y planes, capacitación a personal para que el PCN permanezca actualizado con el objetivo de ser capaz de lograr la recuperación de actividades de misión crítica dentro de los objetivos de tiempo de recuperación asegurando una continuidad de sus servicios y productos.

OBJETIVOS

- Verificación y validación de lineamientos, estrategias y planes de PCN.
- Detalles de todos los cambios de estrategias del PCN con el historial de control de versiones.

FACTORES DE ACTUALIZACION

Pueden ocurrir ciertos eventos no programados al interior del Gobierno Regional Metropolitano o fuera de éste, que afectan el PCN. A continuación, se relaciona una lista de eventos que pueden generar una revisión al PCN:

- Requerimientos legales.
- Nuevos productos.
- Nuevo hardware, plataformas, aplicativos u otros cambios de tecnología (Sistemas Operativos, Bases de Datos).
- Cambios en las telecomunicaciones (voz o datos).
- Quiebra y/o cambio de un proveedor crítico.
- Cambio de instalaciones.
- Cambios en el personal o reubicación del mismo.
- Transferencia de funciones entre sitios existentes.

- Consolidación o tercerización de funciones.
- Cambios en proveedores externos críticos.
- Resultados de las pruebas del Plan de Continuidad del Negocio.
- Cambios en el Sistema de Gestión de Calidad y Procesos.

13 FASE DE ADMINISTRACION DE CRISIS

CONCEPTO

En esta fase se gestiona efectivamente el manejo de la crisis, durante y después de la misma; un buen manejo de la crisis minimiza los impactos de una interrupción.

OBJETIVOS

Integrar los procedimientos de continuidad del negocio con el plan de emergencias y el instructivo correctivo preventivo.
Identificar tipos de emergencias y las respuestas necesarias.

ALCANCE

Este plan de administración de crisis se ejecuta teniendo como premisa las decisiones del Comité de Contingencia. Todas las comunicaciones serán dirigidas por el Director de Continuidad del Servicio.

13.1 Etapa de Evaluación

La evaluación constituye la etapa de valoración preliminar de un evento de interrupción que afecta de forma considerable el Servicio. La evaluación se hace en el sitio, teniendo en cuenta los perfiles y competencias necesarios para determinar: causa de la interrupción, población de usuarios afectada, apreciación de la magnitud, valoración del daño, escenario de soluciones, recursos involucrados y tiempo estimado de la solución.

13.2 Etapa de Activación

Se describen las actividades requeridas para declarar y comunicar el desastre de forma tal que se active la contingencia y se comunique la interrupción a los equipos responsables de recuperar el servicio.
Para activar el plan utilizar el anexo "FORMATO DE ACTIVACION Y SEGUIMIENTO DEL PLAN".

13.3 Etapa de Retorno a la Normalidad

Consiste en definir la forma y/o procedimientos a utilizar para restaurar la operación a la normalidad, una vez superada la contingencia y recuperados los servicios de la Institución.

14 REGISTRO DE OPERACION

El Director de Continuidad deberá emitir un informe que dé cuenta de:

- A.17.01.01 Informe de Planificacion de la continuidad de la Seguridad de la Información
- A.11.01.02 Informe de Implementación de la continuidad de la seguridad de la información
- A.17.01.03 Informe de Verificacion, revision y evaluacion de la continuidad de la seguridad de la información
- A.17.02.01 Informe de Disponibilidad de las instalaciones de procesamiento de la informacion.

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).

15 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.

16 REVISIÓN

EL siguiente Plan será revisado, evaluado y/o actualizado según corresponda anualmente por el Comité de Seguridad de la Información, en cuanto a su funcionamiento y correcta aplicación en la Institución.

17 ANEXOS

17.1 CASCADA TELEFONICA

CASCADA TELEFONICA PCN GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO					
CONTACTOS PERSONAL DEL EDIFICIO			**Fecha de actualización: 05/04/2018**		
ROL	Nombre	Cargo	ANEXO	Correo Electrónico	Celular
Contacto de Emergencia Primario para todas los Departamentos del Servicio	Maria Macarena Miranda Nuñez	Jefe Depto de Gestión Documental	165	mmirandan@gobiernosantiago.cl	9-87569141
	José Torres	Supervisor de Seguridad	231	supervisorhm@gobiernosantiago.cl	Averiguar
	Héctor Muñoz R	Jefe Depto Servicios Generales	104	hmunoz@gobiernosantiago.cl	9-91406387
	Juan Catalan Farías	Jefe Subrogante Depto Servicios Generales	234	jcatalan@gobiernosantiago.cl	9-99978666
	Jose Ignacio Gutierrez Garcia	Jefe Depto Informática	266	jgutierrez@gobiernosantiago.cl	9-99978656
	Ariel Lagos Vasquez	Prevencionista de Riesgos	242	alagos@gobiernosantiago.cl	9-79822401
	Jennifer Lueiza	Jefa Depto Gestión de Personas	201	jlueiza@gobiernosantiago.cl	9-91322580
	Miguel Collio Chávez	Jefe Depto Gestión de Abastecimiento	449	mcollio@gobiernosantiago.cl	9-81384255
	Marcelo Manriquez	Jefa Depto de Finanzas	308	mmanriquez@gobiernosantiago.cl	9-33776896
	Alejandro Linay Carrasco	Jefe Departamento de Transferencias de Capital	412	alinay@gobiernosantiago.cl	9-93498122
	Susana Seguel Barra	Jefa Depto Actividades Cultura, Deporte y Seguridad	494	sseguel@gobiernosantiago.cl	9-76682407
	Rosa Aranda Stuardo	Jefa Departamento de Gestión de Iniciativas de Inversión y Activos no Financieros.	150	raranda@gobiernosantiago.cl	9-82296106
	José Tomás Bartolucci Schiappacasse	Jefe Depto Jurídico	220	jbartolucci@gobiernosantiago.cl	9-88598512
	Francisca Penna Bustos	Jefa Unidad Regional de Asuntos Internacionales	301	fpenna@gobiernosantiago.cl	9-77090928
	Carolina Hidalgo Mandujano	Jefa Departamento de Planificación y Control Institucional	433	chidalgo@gobiernosantiago.cl	9-97893897
	Claudia Amigo Cádiz	Jefa Departamento de Integridad y Ética Institucional	205	camigo@gobiernosantiago.cl	9-76751521
	Jorge Caro Fernandez	Jefe Secretario Ejecutivo CORE	363	jcaro@gobiernosantiago.cl	9-92266795
Contacto de Emergencia secundario	Alejandro Segura	Jefe División Administración y Finanzas	401	jasegura@gobiernosantiago.cl	9-32423800
Jefaturas de División	Cristian Valdes Contreras	Jefe División de Planificación y Desarrollo	495	cvaldes@gobiernosantiago.cl	9-66180958

	Carlos Schultze Esturillo	Jefe División de Análisis y Control de la Gestión	485	cschultze@gobiernosantiago.cl	9-74081953
Contacto de Emergencia Final Administrador Regional	Felix Allendes Vasquez	Administrador Regional	500	Fallendes@gobiernosantiago.cl	9-78079299

17.2 FORMATO DE ACTIVACION Y SEGUIMIENTO DEL PLAN

FORMATO DE ACTIVACIÓN Y SEGUIMIENTO DEL PLAN		
Activación	Hora	DD/MM/AA
Retorno	Hora	DD/MM/AA
Finalización	Hora	DD/MM/AA
Activación de los planes de:		

COMUNICACIÓN DE LA ACTIVACIÓN DEL PLAN					
Cargo	**Informado**	**No informado**	**Secretaria General**	**Informado**	**No informado**

FORMATO DE ACTIVACIÓN Y SEGUIMIENTO DEL PLAN ***Observación (describa la hora vs las actividades y/o decisiones tomadas***				
Hora		***Actividad***		

17.3 EQUIPO DE TRABAJO DEL PCN

Equipo de Trabajo del PCN

Dependencia	*Área*	*Líder PCN*	*Líder Proceso*
Administración Regional	Coordinación	Félix Allendes Vásquez	Félix Allendes Vásquez
Departamento de Gestión Institucional		Carolina Hidalgo M	Carolina Hidalgo M
Departamento Jurídico		José Tomás Bartolucci	Maria Duran
	Unidad de Auditoria Interna	Sebastian Benussi	Luz Magaly Núñez
Depto. de gestión Documental		Silvana Torres	Silvana Torres
			Javier Namuncura T
	OF Partes (at. Público)		Pedro Legua
Departamento de Informática		José Gutiérrez García	José Gutiérrez García
	Unidad de Soporte		Paulo Mendoza
	Unidad de Desarrollo		Héctor Salinas
	Infraestructura		Carlos Hernández
Departamento de Servicios Generales		Héctor Muñoz R	Héctor Muñoz R
			Juan Catalán F
	Conducción		Mauricio Cuadros
	Conducción		Luis Azua G
División de Adm y Finanzas	Administración	Daniel Wiegand	Daniel Wiegand
	Finanzas		Marcelo Manriquez
	Presupuesto		Dario Salinas
	Contabilidad		Alfonso Vallejos N
	Tesorería		Maritza Pacheco
Departamento de Abastecimiento		Miguel Collio	Miguel Collio
			Jaime Martin L

Dependencia	*Área*	*Líder PCN*	*Líder Proceso*
Departamento de Gestión de Personas		Jennifer Lueiza	Jennifer Lueiza
			Mayerling Uribe
	Prevención de Riesgos		Ariel lagos V
	Remuneraciones		Viviana Abarca R
División de Planificación y Desarrollo		Cristian Valdes	Cristian Valdes
Departamento de Planificación			Alvaro Jordán
	Unidad de Fomento e Innovación		Ana Pérez S
	Unidad de Asuntos Indígenas		Marcial Marin F
	Unidad de Iniciativas de Int Regional		Carolina Infante F
Departamento de Espacios Públicos		Valeria López	Valeria López
División de Análisis y Control		Carlos Schultze	Carlos Schultze
Depto. de Gestión de Iniciativas de Inv. Y Act. no Finan		Rosa Aranda	Rosa Aranda
Departamento de Transferencia de Capital		Alejandro Linay C	Alejandro Linay C
Depto. de Act. Y Cultura, Deporte y Seg.		Susana Seguel B	Susana Seguel B

17.4 ESTRATEGIA TECNOLOGICA

- Estrategia Tecnológica de Base de Datos
- Estrategia Red WAN
- Estrategia Red LAN – Switches
- Estrategia tecnológica de software servidor
- Estrategia por problemas en los sistemas

17.4.1 ESTRATEGIA TECNOLÓGICA DE BASE DE DATOS

OBJETIVO

Recuperar un servidor de base de datos por daño en el sistema manejador de la base de datos que se encuentra en el Datacenter del Gobierno Regional Metropolitano.

ALCANCE

El procedimiento aplica para los siguientes escenarios:

- Daños o fallas en algún servidor que afecte servicios dentro de los cuales esta soportado por una base de datos.
- Falla a nivel de Software de Base de datos.

ACTIVIDADES

No. Act	Descripción de la Actividad	Observaciones	Responsable
1	Llamar al encargado Responsable	Contactar al Administrador de Bases de datos o el Jefe Departamento de Informática	Administrador de la base de datos
2	Diagnóstico de la situación.	Se efectúa un diagnóstico del estado de la base de datos.	Administrador de la base de datos
3	¿Se puede recuperar el servicio en la misma máquina?	De acuerdo al diagnóstico se decide sobre el mejor procedimiento para restablecer el servicio. En caso afirmativo pasa al punto 5 de lo contrario al punto 6.	Administrador de la base de datos

4	Proceder a restablecer el servicio	Se restablece el servicio en el mismo servidor y se pasa al paso 10	Administrador de la base de datos
5	Crear la base de datos en el servidor de contingencia.	Toma la hoja de vida y con los comandos de la consola de administración crea la base de datos con los parámetros descritos en la hoja de vida.	Administrador de la base de datos.
6	Recuperar ultima copia de la base de datos.	Tomar ultima copia de seguridad disponible de la base de datos y proceder a su restauración en la base de datos creada recientemente.	Administrador de la base de datos.
7	Definir los usuarios del sistema en el nuevo servidor.	Tomar de la hoja de vida los usuarios requeridos para su correcto funcionamiento y definirlos asignándoles los perfiles requeridos	Administrador de la base de datos.
8	Verificar que la base de datos opera adecuadamente.	Si los resultados son satisfactorios se sigue al paso 10, sino vuelve al paso 4.	Administrador de la base de datos
9	Se informa al Coordinador de Infraestructura o al Director de Tecnología del restablecimiento del servicio	Reporte de funcionamiento y se documenta el proceso efectuado.	Administrador de la base de datos.
10	Reporte de servicio restablecido.	El Administrador de la Red o el Jefe Departamento de Informática, informan que la contingencia ha sido superada.	Coordinador de Infraestructura, Administrador de la Red o el Jefe Departamento de Informática

SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE

17.4.2 ESTRATEGIA TECNOLÓGICA DE RED WAN

OBJETIVO

Recuperar un enlace de comunicación entre Gobierno Regional / Intendencia / ISP

ALCANCE

El procedimiento aplica para los siguientes escenarios:

Daños o fallas en algún enlace que afecte servicios dentro de los cuales esta soportado por la redWAN.

ACTIVIDADES

No. Act	Descripción de la Actividad	Observaciones	Responsable
1	Identificar la falla y realizar un diagnóstico interno		Profesional Departamento de Informática y Proveedor de servicios de la red
2	Llamar al Encargado	Llamar a las líneas:- Las que se encuentren en el documento de contacto del Encargado en el anexo "Cascada Telefónica".	Encargado de Infraestructura o Profesional de Departamento de Informática
3	Diagnóstico de la situación por parte de administrador de la red o del contratista	Se efectúa un diagnóstico del estado del enlace de comunicaciones.	Encargado de Infraestructura o Profesional de Departamento de Informática o contratista
4	Se puede recuperar el servicio empleando el canal de contingencia	De acuerdo al diagnóstico se decide sobre el mejor procedimiento para restablecer el servicio	Encargado de Infraestructura o Profesional de Departamento de Informática o contratista
5	Proceder a restablecer el servicio	Se restablece el servicio y se pasa al paso 7	Encargado de Infraestructura o Profesional de Departamento de Informática o contratista
6	Establecer canal de comunicación alterno	Enviar equipo de trabajo, revisar el firewall, el enlace	Encargado de Infraestructura
7	Validar la configuración	Establecer QoS, parámetros de configuración, enrutamiento, etc.	Encargado de Infraestructura
8	Verificar que el enlace opera adecuadamente	Si los resultados son satisfactorios se sigue al siguiente paso sino vuelve al paso No 5 y verifica	Coordinador de Infraestructura o Profesional de Departamento de Informática o contratista

9	Se informa al Encargado de infraestructura o al Lider de Recuperación Tecnológica, del restablecimiento del servicio	Reporte de funcionamiento y se documenta el proceso efectuado	Encargado de Infraestructura o Profesional de Departamento de Informática
10	Reporte de servicio restablecido	El Encargado de infraestructura o Lider de Recuperación Tecnológica informan que la contingencia ha sido superada.	Encargado de infraestructura, Administrador de la red o Lider de Recuperación Tecnológica

SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE

17.4.3 ESTRATEGIA TECNOLÓGICA DE LAN - SWITCHES

OBJETIVO

Recuperar un Switch que se encuentra en la red del Gobierno Regional Metropolitano.

ALCANCE

El procedimiento aplica para los siguientes escenarios:

- Daños o fallas en alguno de los Switches.
- Falla a nivel de Hardware o Software.

ACTIVIDADES

No. Act	Descripción de la Actividad	Observaciones	Responsable
1	Identificar la falla y realizar un diagnóstico interno		Encargado de Infraestructura
2	Llamar al Encargado responsable del mantenimiento o tomar uno de los switch del stock disponible para asignar un recambio	Llamar a las líneas: - Las que se encuentren en el documento de contacto del Encargado en el anexo "Cascada Telefónica".	Encargado de Infraestructura
3	Tomar el Switch de recambio		Profesional Depto. de Informática
4	Verificar que el swicth opera adecuadamente	Se conecta el switch y se efectúan las pruebas de enrutamiento necesarias.	Encargado de Infraestructura
5	El switch opera adecuadamente	Si los resultados son satisfactorios se sigue al siguiente paso sino vuelve al paso No 4 y verifica	Encargado de Infraestructura
6	Se informa al Encargado de infraestructura o al Director de tecnología, del restablecimiento del servicio	Reporte de funcionamiento y se documenta el proceso efectuado	Encargado de Infraestructura
7	Reporte de servicio restablecido	El Encargado de infraestructura o el Jefe del Dpto. De Informática informan que la contingencia ha sido superada.	Encargado de infraestructura, Administrador de la red o el Líder de Recuperación Tecnológica

SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE

17.4.4 ESTRATEGIA TECNOLÓGICA DE SOFTWARE SERVIDOR

OBJETIVO

Recuperar un servidor de base de aplicaciones por daño en el sistema.

ALCANCE

El procedimiento aplica para los siguientes escenarios:

- Daños o fallas en algún servidor que afecte servicios dentro de los cuales esta soportado por un servidor web o servidor de aplicaciones.
- Falla a nivel de Software Base del servidor.

CONDICIONES GENERALES

Para llevar a cabo el siguiente procedimiento es necesario tener los siguientes recursos disponibles:

Contrato vigente de soporte servidores

DESCRIPCIÓN ACTIVIDADES

No. Act	Descripción de la Actividad	Observaciones	Responsable
1	Identificar la falla y realizar un diagnóstico interno		Encargado de Infraestructura
2	Llamar al Encargado de la Unidad de Desarrollo	Llamar a las líneas: Las que se encuentren en el documento de contacto del Encargado en el anexo "Cascada Telefónica".	Encargado de Infraestructura
3	Diagnóstico de la situación por parte del administrador del servidor o del contratista	Se efectúa un diagnóstico del estado del software base.	Encargado de Infraestructura
4	Se puede recuperar el servicio en la misma máquina	De acuerdo al diagnóstico se decide sobre el mejor procedimiento para restablecer el servicio	Encargado de Infraestructura
5	Proceder a restablecer el servicio	Se restablece el servicio en el mismo servidor y se pasa al paso 9	Encargado de Infraestructura

6	Recuperar la hoja de vida del servidor	La extraerá del repositorio de plantillas de hojas de vida de los servidores	Encargado de Infraestructura, Líder de Recuperación Tecnológica
7	Actualizar la configuración en el servidor de contingencia	Toma la hoja de vida y con los comandos de la consola de administración instala, configura los servicios con los parámetros descritos en la hoja de vida.	Encargado de Infraestructura
8	Definir los usuarios del sistema en el nuevo servidor	Tomar de la hoja de vida los usuarios requeridos para su correcto funcionamiento y definirlos asignándoles los perfiles requeridos	Encargado de Infraestructura
9	Verificar que el servidor la aplicación, el servidor web o servidor de aplicaciones opera adecuadamente	Si los resultados son satisfactorios se sigue al siguiente paso sino vuelve al paso No 5 y verifica	Encargado de Infraestructura
10	Se informa al Encargado de Infraestructura, Líder de Recuperación Tecnológica, del restablecimiento del servicio	Reporte de funcionamiento y se documenta el proceso efectuado	Encargado de Infraestructura
11	Reporte de servicio restablecido	El Encargado de Infraestructura, Líder de Recuperación Tecnológica, informan que la contingencia ha sido superada.	Encargado de Infraestructura, Líder de Recuperación Tecnológica

SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE

17.4.5 ESTRATEGIA POR PROBLEMAS EN LOS SISTEMAS

OBJETIVOS

Definir un procedimiento para la atención de los incidentes o problemas presentados en los sistemas o aplicativos que manejan las unidades usuarias.

Definir responsabilidades en cuanto a la declaración de contingencias por incidentes oproblemas presentados.

A continuación, se detalla el procedimiento para el manejo de incidentes por problemas de sistemas:

Funcionario de la Unidad

Detalla en forma precisa el evento o incidente que se presenta e informa al Líder de PCN de la dependencia.

Líder PCN de Unidad

Verifica si el mismo evento se le está presentando a otros funcionarios de la misma Unidad y si sus tareas afectan a otras dependencias, se debe validar con las mismas si el problema es general.

Una vez tenga claridad sobre el evento que se está presentando y los funcionarios involucrados, debe clasificarlo teniendo en cuenta las siguientes definiciones para determinar si es un incidente o un problema:

Incidente: Afecta puntualmente a una persona o grupo de personas.

Problema: Afecta de manera general a todo El Gobierno Regional Metropolitano o a los clientes.

Ingresa en el aplicativo de reporte de incidencias del Servicio. Esto con el fin que el Departamento de Informática pueda dejar reportado el evento en el Control de Incidentes.

Envía al correo electrónico al Prevencionista de Riesgo y Encargado de Infraestructura del Departamento de Informática e informa el incidente de PCN.

Encargado de Infraestructura – Departamento de Informática

Define la solución al incidente (tiempo y estrategia de recuperación) y da respuesta sobre la gravedad del evento y tiempo de recuperación. Si el daño es importante, el Jefe del Departamento de Informática decide la activación del plan de contingencia de tecnología afectado (servidores backup, sistemas de recuperación de información, enlaces de comunicación), e informa al Líder de Recuperación Tecnológica.

Líder de Recuperación Tecnológica

Informa la situación al Líder de PCN de la Unidad afectada.

Si el tiempo de recuperación es menor al Tiempo Objetivo de Recuperación (RTO) del proceso afectado deberá esperar, de lo contrario declara la contingencia mientras se soluciona definitivamente el incidente o problema presentado.

Líder de PCN unidad afectada

Desarrolla la estrategia de contingencia de acuerdo a los parámetros establecidos para eventos de similares características.

Encargado de Infraestructura – Departamento de Informática

Una vez solucionado el incidente o problema por parte del Departamento de Informática, informa al Líder de Recuperación Tecnológica y al Líder PCN de la Unidad afectada para que se levante la contingencia.

Líder de Recuperación Tecnológica

Solicita levantar la contingencia del incidente presentado y retorno a la normalidad.

Líder PCN de Unidad

Asegura el retorno a la normalidad de las operaciones de acuerdo con lo establecido "Retorno a la normalidad" via mail y ejecuta las acciones que permitan que los usuarios no se vean afectados en los procesos de la Unidad.

Una vez se haya solucionado el incidente, completar el formato "Incidentes de Contingencia" (ver anexo "Incidentes de contingencia"), lo entrega al Líder de Recuperación Tecnológica, con copia al Líder del Proceso responsable de la Unidad afectada.

17.5 ESCENARIO DE CONTINGENCIA A SITIO ALTERNO

Director de Continuidad o Director Subrogante de Continuidad

Activa la contingencia a sitio alterno.

Prevencionista de Riesgo

Activa la cascada telefónica y comunica el evento de incidente mayor a la Jefatura o Encargado de cada área, quien a su vez informa al colaborador de siguiente jerarquía de su área acerca del incidente ocurrido y las instrucciones de activación de la contingencia de lugar.

Jefe Departamento de Servicios Generales (Líder Administración Recuperación Infraestructura Física)

El Jefe Departamento de Servicios Generales con apoyo del Comité de Contingencia, contacta a los proveedores de las alternativas seleccionadas, definen el sitio alterno en el cual se mantendrá la operación del Servicio en momento de contingencia.

Acuerda con el proveedor la utilización de sus instalaciones por el período de tiempo que dure la contingencia, según las necesidades del Gobierno Regional Metropolitano descritas por el Coordinador y el Comité de Contingencia en ese momento.

Coordina el traslado del personal al centro de operaciones establecido para operar en contingencia.

Coordinadores de recuperación

Convoca al personal identificado como personal crítico (equipo de recuperación), e informa el incidente ocurrido, solicitando el desplazamiento al "Lugar alterno de trabajo". El equipo de recuperación se encuentra detallado en el documento "Cascada Telefónica", que posee el Líder de PCN de cada área.

Una vez instalados en el centro de operaciones alterno, realiza un chequeo del personal mínimo que se encuentra en el sitio, en caso de ser necesario llamará al personal suplente requerido.

Solicita el kit de contingencia (recursos de escritorio) y al personal crítico que inicie la conectividad a los programas requeridos.

Confirma al Director Subrogante de Continuidad o su suplente la correcta continuidad de los procesos.

Jefe Departamento de Servicios Generales (Líder Administración Recuperación Infraestructura Física)

Realiza una evaluación del sitio alterno, para validar que los recursos requeridos se encuentren disponibles en el sitio.

Director de Continuidad o Director Subrogante de Continuidad

Solicita a los diferentes Coordinadores de Recuperación un estado del evento y como ha transcurrido la operación en contingencia, se debe de usar el formato de Activación y Seguimiento de la Activación.

El Comité de Contingencia analiza los resultados del estado de la contingencia y, procede a decidir:

"**NO** terminar la contingencia": Los equipos de recuperación deben seguir ejecutando la operación en contingencia.

"**SI** terminar la contingencia": Basado en la información suministrada por los Coordinadores y el análisis realizado por los miembros del Comité, el Director de Continuidad decide terminar la contingencia, da la orden de activar el proceso de retorno, confirma la disponibilidad y funcionabilidad del sitio normal de trabajo y se informa a los diferentes equipos la decisión.

Coordinadores de recuperación del negocio

Devuelve el "kit de contingencia" para su custodia nuevamente.

Comunicar al personal que participó en la contingencia, el "Retorno a la normalidad" y coordina el desplazamiento al "Sitio base de trabajo".

17.6 FORMATO DE INCIDENTES DE CONTINGENCIA

REPORTE DE INCIDENTES DE CONTINGENCIA

Información de Identificación			
Fecha del incidente		Hora de ocurrencia	
Duración del Incidente		Proceso afectado	
Nombre del Área		Lugar donde se presentó el incidente	

Medidas Contingentes Adoptadas		
Acción	Participantes	
	Nombre	Cargo

Descripción del Riesgo

Descripción del incidente

Causas del Incidente

Retorno a la Operación Normal

17.7 Resultado Pruebas de Sitio Alterno

Resultados de la Prueba de Plan de Continuidad

Tipo de Prueba	
Sitio Alterno	
Fecha y hora de Inicio de pruebas	
Fecha y hora de Finalizacion de pruebas	
Coordinador	
Usuarios participantes	
Duración efectiva de la Prueba	
Servicios testeados	
otros	

Descripción.

Prueba Realizada en el Sitio Alterno que valida este escenario como prueba ante desastres

Objetivos

La realización de esta prueba se realizó con el propósito de verificar y validar la conectividad hacia y desde el Data Center del Gobierno Regional Metropolitano

Procedimientos

Verificar que todos los procedimientos que apuntan a una buena conexión entre el Sitio Alterno sean claros y tecnológicamente eficientes de manera de validar todos los recursos usados en esta prueba

Documentación

Verificar que toda la documentación que se ha dispuesto sea valida

Validación de Ambientes

Validar que en ambientes de desastres o contingencia todos los servicios y aplicaciones funcionaron correctamente.

Alcance

Esta prueba ha sido programada para que su activación comience el día XX del mes XX del presente año. Comenzará a las XX am y se prolongará hasta las XX horas del mismo día.

Incluirá realizar pruebas de conexión, comunicación telefónica, conexión e intercambio de información con bases de datos, aplicaciones y archivos contenidos en los servidores del Gobierno Regional Metropolitano ubicados en el propio Data Center

Resultados

Funcionalidad
Verificar si los sistemas, correos, telefonía y conexión a Base de Datos funcionaron correctamente.
Verificar si se presentó algún problema de conexión dentro de las primeras horas, pero solucionado de manera apropiada.
Verificar si estos problemas quedaron documentados para prevenir estos hechos en eventos futuros.

Procedimientos

Verificar si los procedimientos se ajustaron a lo previsto, de acuerdo a lo definido en cada uno para determinar el resultado exitoso de la prueba.

Tiempos

Verificar si los tiempos de conexión se ajustaron a los esperados.

CONCLUSIONES

Verificar si la prueba se realizó de manera exitosa, de acuerdo a lo estimado y programado.

Verificar el funcionamiento de los aparatos telefónicos identificando el número de llamadas
Si se recibieron llamadas telefónicas y si se hicieron, y si todas ellas fueron exitosas.

Si se conectaron equipos portátiles y navegaron por internet sin problemas pudiendo además acceder a la red LAN del Gobierno Regional Metropolitano.

Si se trabajó en las aplicaciones SAGIR, SGA, y Sistema de bodega.

Si se accedió a archivos localizados en diferentes servidores con un tiempo más que aceptable.

Si se validaron los accesos del personal de manera electrónica (tarjetas de Identificación).

Respecto de la atención de público, si se recibieron documentación y de que tipo, y si es que fueron ingresadas en sus respectivas bases de datos sin problemas.

18 REGISTRO DE OPERACION

El Departamento de Informática deberá emitir un informe que dé cuenta de:

A.17.01.01	Informe de planificación de la continuidad de la seguridad en la información.
A.17.01.02	Informe de implementación de la continuidad de la seguridad en la información
A.17.01.03	Informe de verificación revisión y evaluación de continuidad de la seguridad de la información.
A.17.02.01	informe de disponibilidad de las instalaciones de procesamiento de la información.

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)

19 FORMALIZACION EXTERNA

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

20 REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

Versión	Autor	Página o Seccion	Fecha Modificación	Motivo
01	Carlos Hernandez	todas	01-10-18	Creación Documento
02	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019.
03	Carlos Hernandez	49	15-11-2021	Se agrega capítulo 19 formalización externa Se actualiza índice
04	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021.

21 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

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			