Personería de Bogotá, D. C.
Al servicio de la ciudad

PLAN DE CONTINUIDAD DE NEGOCIO DE SERVICIOS TECNOLÓGICOS

03 - PL - 05

PROCESO DIRECCIONAMIENTO TIC

17-09-2018
Versión – 1

CONTROL DE CAMBIOS							
CÓDIGO DEL DOCUMENTO:	0	3	P	L	0	3	**NOMBRE DEL DOCUMENTO:** PLAN DE CONTINUIDAD DE NEGOCIO DE SERVICIOS TECNOLÓGICOS
FECHA DE VERSIÓN 1:	dd / mm / aaaa 17/09/2018						

DESCRIPCIÓN DE LA MODIFICACIÓN	
Versión	**Descripción**

CONTROL DE ACTUALIZACIONES							
Versión	**Motivo de la Modificación**	**Fecha Modificación**			**No. Páginas Modificadas**	**Responsable Solicitud Cambio**	
		DD	**MM**	**AAAA**			

Elaboró:	**Revisó:**	**Aprobó:**
Ing. Oscar Manuel Martínez/ Profesional Especializado 222-02 (E) Ing. Clara Neyra Barrios Profesional Especializado 222-02(E)	Mar Jenny Romero / Auxiliar Administrativo / Direccionamiento TIC Camilo Andrés Cruz González/ Profesional Especializado 222-07/ Direccionamiento Estratégico	Ing. Henry Díaz Dussán / Director de TIC Proceso Direccionamiento TIC German Uriel Rojas / Director de Planeación

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Como un complemento fundamental del Sistema de Gestión de la Seguridad de la Información (SGSI), el Plan de Continuidad de Negocio de servicios Tecnológicos de la Dirección de TIC de la Personería de Bogotá D.C., integra el esfuerzo de todas las áreas involucradas en el análisis de procesos, riesgos y vulnerabilidades así como la elaboración de los procedimientos para prevenir, enfrentar y mitigar los riesgos que amenazan la continuidad de las operaciones de la Entidad.

Con base en las directrices y guías del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC, se estructuró un plan que le permita a la Personería de Bogotá D.C., fortalecer su resiliencia y contar con una herramienta efectiva en caso de presentarse un evento que afecte gravemente el normal desarrollo de las operaciones. Para tal efecto se realizó un trabajo basado en la Gestión de riesgos de la Entidad y con el aporte de todas las áreas que gestionan los procesos críticos.

Este plan, que tiene como marco de acción la política de seguridad de la información y se soporta en todos los procedimientos definidos, permitirá la prevención de algunos eventos y una recuperación de los procesos críticos dentro de los tiempos definidos por la Entidad en caso de un evento disruptivo.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Preparar a la Personería de Bogotá, D. C. para responder adecuadamente ante un evento que interrumpa las operaciones, de manera que se logre restablecer los servicios críticos en el menor tiempo posible y los demás servicios en un tiempo razonable.

2.2 OBJETIVOS ESPECÍFICOS

Para el logro del objetivo principal se establecen los siguientes objetivos específicos

- Identificar los procesos, las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- Identificar al recurso humano tanto interno como externo que se requiere para la operación de los procesos y actividades críticas del negocio.
- Establecer para cada proceso los tiempos mínimos de recuperación que requiere La Personería de Bogotá D.C., para que no se afecte el servicio.
- Definir la funcionalidad mínima que requiere la Entidad en caso de presentarse un evento que interrumpa las operaciones.
- Identificar y analizar los riesgos y vulnerabilidades relacionados con la continuidad del negocio de acuerdo con la metodología y política de tratamiento de riesgos de la Entidad.
- Desarrollar para cada uno de los servicios críticos, los procedimientos y guías de operación específicos para atender efectivamente las interrupciones del servicio.
- Proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas por eventos naturales, o acciones de las personas.
- Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.
- Desarrollar e impartir la capacitación necesaria a todos los involucrados, para el correcto funcionamiento del plan.
- Establecer un plan de pruebas, gestión y mantenimiento para el cumplimiento de los objetivos y la óptima operación del Plan de Continuidad

3. ALCANCE

El Plan de Continuidad de Negocio de Servicios Tecnológicos de la Personería de Bogotá D.C., define su estrategia de recuperación basándose en el mapa de procesos definido para la Entidad, resaltando de esté los procesos misionales y los procesos que se consideran críticos para prestar sus servicios. Dentro de la estrategia se incorporan los recursos físicos, humanos, tecnológicos y de toda índole que sean necesarios para lograr recuperar los servicios o procesos críticos de la Entidad dentro de los tiempos que se

determinen como razonables por parte de la Dirección de Tecnologías de Información y Comunicación DTIC.

4. TÉRMINOS Y DEFINICIONES

Sitio alterno: Ubicación alterna de operaciones seleccionada para ser utilizada por la Personería de Bogotá D.C., cuando las operaciones normales no puedan llevarse a cabo, utilizando las instalaciones normales después de que se ha producido una interrupción.

Gestión de continuidad de negocio (BCM): Proceso general de gestión holístico (involucra a todas las áreas de la Entidad) que identifica las amenazas potenciales a una organización y el impacto que estas podrían causar a las operaciones de la Entidad en caso de materializarse. Provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de la Entidad así como las partes interesadas claves, reputación, marca y actividades de creación de valor.

Plan de Continuidad de Negocio (BCP por sus siglas en inglés): Conjunto de procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido una vez presentada la interrupción.
NOTA: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio. [Fuente: ISO 22301]

Análisis del impacto al negocio (BIA por sus siglas en inglés): Proceso del análisis de las actividades y las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300]

Nivel de Criticidad: Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Interrupción: Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

Recuperación de desastres de tecnología y telecomunicaciones (ITCTIC): Habilidad o capacidad de los elementos de tecnología y telecomunicaciones (ITC) de las TIC de la organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción.

Plan de recuperación de desastres de las TIC (ICT DRP): Plan claramente definido y documentado el cual permite recuperar las capacidades de tecnología y Telecomunicaciones LAS TIC cuando se presenta una interrupción.

NOTA: En algunas organizaciones es llamado el plan de continuidad de tecnología y telecomunicaciones las TIC.

Modo de falla: Manera o forma en la cual una falla es observada (generalmente describe la manera en que la falla ocurre y su impacto para en la operación del sistema).

Preparación de las TIC para la continuidad de negocio (IRBC): Capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a una interrupción así como la recuperación de sus servicios de TIC.

Objetivo mínimo de continuidad de negocio (MBCO): Mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.

Punto objetivo de recuperación (RPO): Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

Tiempo objetivo de tiempo de recuperación (RTO): Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

Resiliencia: Habilidad o capacidad de una organización para resistir cuando es afectada por una interrupción.

Disparador o detonante: Evento que hace que el sistema inicie una respuesta (evento activador).

Registro vital: Registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados, sus usuarios, clientes y sus partes interesadas.

5. CONDICIONES GENERALES

Para los acontecimientos que rara vez se presentan como terremotos, incendios, inundaciones, atentados, robo, pérdida masiva de comunicaciones y fallas eléctricas de proporciones graves; Se aplicaran as prevenciones y correcciones, con sus correspondientes etapas, solamente a las estructuras patrimoniales como demanda la ley en este aspecto.

La Personería de Bogotá D.C., cuenta con un plan de mitigación de desastres en el caso de presentarse cualquiera de los acontecimientos anteriores, y para el evento de una contingencia informática se aplicaran las medidas de recuperación de operaciones, contando con las actividades desarrolladas en este plan para cada uno de los responsables, previa declaración de la emergencia.

Como no existe un centro de datos alterno, se dejara la nube para que reciba las operaciones necesarias para la atención integral al ciudadano, ya que las bases de datos y aplicaciones están allí y así cumplir con la mitigación o prevención, continuidad y recuperación de negocio.

6. DOCUMENTOS DE REFERENCIA

Este plan se encuentra enmarcado en las disposiciones y recomendaciones contenidas en las políticas de seguridad informática de la Entidad aprobada.

De igual forma, es de aplicación obligatoria la legislación vigente relacionada con el tema, la cual se encuentra publicada en la Intranet y en la cual se relacionan las siguientes:

- Constitución Política de Colombia articulo 61 y 74, ley 527 1999, articulo 12; ley 1437 2011, articulo 3, articulo 8; ley 594 2000, articulo 19, 20 y 21; decreto 2693 2012, articulo 3; Ley 1273 2009; principios y fundamento de la Estrategia del Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, recomendaciones del estándar internacional de la ISO 27001 versión actualizada 2013, Ley de propiedad intelectual, Ley Especial de Telecomunicaciones.
- Resolución 318 de 2015 por la cual se adopta la política de seguridad Informática de la Personería de Bogotá D.C.

- Resolución 580 del 18 de agosto de 2017, por la cual se articulan los Sistemas de Gestión de la Entidad en el Modelo Integrado de la Personería de Bogotá D.C., MIPER.

- Decreto 93 del 13 de enero de 1998 el cual adopta el Plan Nacional para la Prevención y Atención de Desastres, tiene como objetivo “orientar las acciones del Estado y de la sociedad civil para la prevención y mitigación de los riesgos, los preparativos para la atención y la recuperación en caso de desastre, contribuyendo a reducir el riesgo y el desarrollo sostenible de las comunidades vulnerables ante los eventos naturales y antrópicos”.

- Resolución reglamentaria a nivel de organismos de control para la creación del plan Decreto 1537 de 2001, por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las Entidades y organismos del Estado que en el

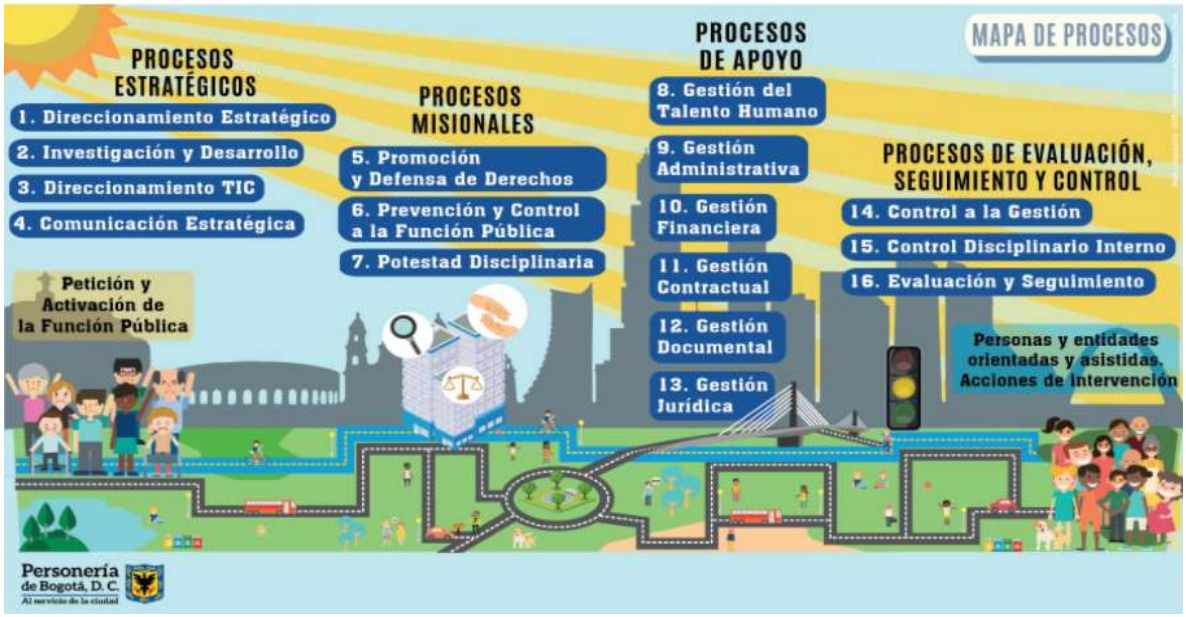
parágrafo o del 13 artículo 4º señala los objetivos del sistema de control interno define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones y en su artículo 3º establece el rol que deben desempeñar las oficinas de control interno que se enmarca en cinco tópicos valoración de riesgos.

- Ley 1581 2012 por la cual se debe reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas.

- Decreto 2573 2012: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

7. PROCESOS DE LA ENTIDAD

La Personería de Bogotá D.C., ha definido el siguiente mapa de procesos de acuerdo con las funciones y servicios que presta a la ciudad.



7.1 DEFINICIÓN DE PROCESOS CRÍTICOS

Para la definición de los procesos críticos de la Entidad se llevó a cabo un análisis detallado con los líderes de los diferentes procesos y de acuerdo con los criterios de la Gestión de Riesgos de la Entidad se establecieron los siguientes procesos críticos los cuales se deben formalizar con el comité directivo MIPER

PROMOCIÓN Y DEFENSA DE DERECHOS: Tiene como propósito promover, proteger y asegurar la efectividad de los derechos de los habitantes del Distrito Capital. Fue considerado como critico porque forma parte de los procesos misionales de la Entidad.

PREVENCIÓN Y CONTROL A LA FUNCIÓN PUBLICA: El proceso revisión a la gestión pública permite cumplir la función de veeduría que busca advertir oportunamente a los grupos de interés sobre riesgos y posibles irregularidades en la gestión pública distrital, que puedan afectar la protección de intereses de la sociedad y la materialización de los derechos. Este proceso fue considerado como critico porque forma parte de los procesos misionales de la Entidad.

POTESTAD DISCIPLINARIA: Proceso encargado de investigar y juzgar oportuna y consistentemente las conductas de los servidores públicos distritales. Este proceso fue considerado como critico porque forma parte de los procesos misionales de la Entidad

DIRECCIONAMIENTO TIC: Proceso encargado de garantizar que la Entidad cuente con una infraestructura tecnológica actualizada y moderna para brindar a los usuarios internos y externos, las herramientas apropiadas para que la información se gestione en condiciones de seguridad y confiabilidad. Este proceso se consideró como critico porque soporta toda la infraestructura tecnológica (hardware y software) que requieren todos los demás procesos para su normal operación.

GESTION DEL TALENTO HUMANO: Con este proceso se garantiza la provisión oportuna del recurso humano idóneo y competente para la operación eficaz, eficiente y efectiva del Sistema Integrado de Gestión de la Personería de Bogotá D.C. Se consideró como critico por la evidente necesidad del recurso humano en la gestión y control de los diferentes procesos y procedimientos de la Entidad.

7.2 INCIDENTES EN APLICACIONES Y PLATAFORMAS CRÍTICAS

Incluye el respaldo de los elementos referentes a los sistemas de información, infraestructura (dispositivos, servidores y servicios), personal a cargo, y otros recursos de apoyo, y esta direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de la Entidad. Infraestructura de respaldo que también es vulnerable como por ejemplo las unidades de potencia ininterrumpida (UPS) y el sistema de refrigeración del Centro de Cómputo

Los sistemas de comunicaciones (hardware y software, sistema de cableado, canales de datos y medios de transmisión) también están constantemente expuestos a riesgos por latencias, caídas o hasta perdidas de paquetes, pudiendo ser la principal fuente de problemas. Entonces el Hardware y el Software asociado a esto, también están expuestos a diversos factores de riesgo lógico y Físico, aunque no se descartan incidentes o errores humanos.

Para la contingencia en este caso, se efectuarán los procedimientos relacionados solamente en este plan, que involucran respaldo inmediato del bien afectado para la continuidad de operaciones.

El plan de continuidad de operaciones es un plan de procedimientos alternativos a la forma acostumbrada de operar de la Entidad, constituye una herramienta que ayuda a que los procesos críticos de la Entidad, continúen funcionando en una situación de desastre, aun cuando, el desastre sea incontrolable en el entorno.

8. FASES PARA LA IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD

8.1 FASE I: ANÁLISIS DEL NEGOCIO

8.1.1 Responsables

Según el acuerdo 514 de 2012, la Entidad está conformada por el Despacho del Personero, asesorado directamente por la Oficina de Control Interno y la Oficina Asesora de Divulgación y Prensa; le acompañan tres Personerías Delegadas con sus correspondientes dependencias y un Eje de Apoyo.

8.1.2 Compromiso de la Alta dirección

La alta dirección debe comprometerse tanto para la planeación como para la implementación y pruebas del plan de continuidad, así como proveer los recursos que se requieran para su realización. De igual forma, atendiendo a las necesidades del plan en contraste con los diferentes perfiles del personal con el que cuentan, liderar la conformación de diferentes comités que faciliten el seguimiento y materialización del plan.

8.1.3 Comité Directivo Modelo Integrado de la Personería de Bogotá D.C., MIPER

Para direccionar los aspectos relacionados con la seguridad de la Información, de acuerdo con lo establecido en la Resolución 580 del 18 de agosto de 2017 el comité MIPER cuyos integrantes son los directivo de la Entidad y tiene entre otras funciones la revisión del Plan Estratégico de Tecnologías de la Información y Comunicaciones de la Entidad (PETI), aprueba las normas de acceso a los servicios informáticos entre otras funciones.

8.1.4 Conformación de grupos de desarrollo del plan

Se sugiere la estructuración del grupo técnico-profesional encargado del desarrollo, implantación y mantenimiento del plan de continuidad, quedando conformado así:

Coordinador del plan de continuidad:
El coordinador del Plan es el canal de comunicación entre el grupo de comité técnico operativo y el comité de seguridad, a través del cual se transmitirán las decisiones tomadas en torno a las acciones del Plan, los niveles de ejecución del Plan y el estado de los recursos informáticos que cubre el Plan. Debe encargarse de monitorear y asegurar el cumplimiento estricto del Plan y del mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo. Proveer los recursos necesarios y notificar las decisiones a los funcionarios(as) (as) delegados.

El Director de la Dirección de Tecnologías de la Información y Comunicación DTIC, coordinador del plan, junto con el oficial de la seguridad informática, elaborarán el plan de trabajo para el desarrollo e implantación del proyecto y conformarán subgrupos de trabajo para la ejecución de cualquier incidente.

Comité técnico operativo:
Conformado por el Director de la Dirección de Tecnologías de la Información y Comunicación DTIC, quien será el coordinador y los siguientes Integrantes: Ingenieros Documentador, soporte técnico, infraestructura, bases de datos, sistemas de información, redes y comunicaciones y el oficial de seguridad que debes ser un funcionario de la Dirección de Tecnologías de la Información y Comunicación DTIC.

Funciones Generales

- Coordinar el desarrollo, implantación y mantenimiento del plan para la recuperación del sistema de información o la utilización de sistemas alternos.

- Efectuar el seguimiento a los costos en que se incurre en el desarrollo e implementación del Plan.
- Aprobar y formular recomendaciones ante el comité de seguridad acerca del establecimiento de convenios, contratos o compras de elementos para el desarrollo del Plan.
- Manejar los convenios y/o contratos que se hayan firmado para el desarrollo del Plan.
- Recomendar acerca de la compra y/o mantenimiento de hardware, software o instalaciones, si se requieren.
- Efectuar las pruebas que garanticen la plena operatividad del Plan.
- Mantener operativo el Plan.
- Verificar que se estén realizando los backup internos y externos.
- Realizar simulacros periódicos, por lo menos una vez al año, con los sistemas alternos, con el fin de mantener activos a los miembros del equipo y vigente el Plan.
- Garantizar que existan personas que puedan reemplazar a los funcionarios(as)(as) claves en los procesos de recuperación.
- Verificar que la infraestructura de respaldo, siempre esté disponible y listo para atender la contingencia.

La conformación y funciones específicas de cada uno de los miembros del comité se detallan a continuación:

Ingeniero documentador:

- Se encargará de mantener la información actualizada y el Plan
- Elaborar el plan de trabajo para el desarrollo e implantación del Plan.
- Documentar el Plan para la recuperación del servicio.
- Resguardar la documentación de procesos y procedimientos informáticos, protocolos y guías necesarias para la ejecución de planes respectivos.
- Control periódico de los estándares, protocolos y procedimientos informáticos
- Disponer de acceso inmediato a los documentos en caso de una contingencia.

Ingeniero encargado soporte técnico:

- Se encargará de mantener los inventarios de los bienes informáticos actualizados.
- Garantizar la operatividad de los equipos de cómputo y en coordinación con las Redes mantenerlas operativos.
- Efectuar el monitoreo permanente de los componentes de Hardware.
- Coordinar la instalación de nuevos equipos.
- Garantizar mantenimiento preventivo y correctivo de los equipos y medios de transmisión.
- Proveer soporte técnico a los usuarios
- Instalar equipos de cómputo y los elementos de soporte eléctrico.

Ingeniero encargado de la Infraestructura:

- Se encargará de mantener los inventarios de su infraestructura actualizados.
- Actualizar bitácora correspondiente.
- Garantizar la operatividad de la Infraestructura (servidores y Servicios).
- Coordinar la instalación de nuevos equipos relacionados con el Comité Técnico Operativo.
- Elaborar Copias de Respaldo (backups)
- Disponer de acceso inmediato a los backups cuando se requieran.

Ingeniero encargado de bases de datos:

- Velar por que los procedimientos establecidos para proveer los backups se apliquen.
- Actualizar bitácora correspondiente.
- Mantener actualizados los manuales de procedimientos para backup.
- Garantizar que los backups disponibles para los sistemas alternos de respaldo estén actualizados.
- Atender a los usuarios y prestar la asesoría que le sea requerida.

Ingeniero encargado de Sistemas de Información:

- Revisar los procedimientos para la actualización de archivos y las bases de datos.
- Actualizar bitácora correspondiente.
- Revisar, implementar y actualizar los procedimientos de instalación de software operativo y aplicativo.
- Modificar procesos e instruir a los usuarios sobre el manejo de los sistemas.
- Garantizar la existencia de copias de respaldo del software Operativo, Aplicativo y utilitario.
- Coordinar las tareas que deben ejecutar los responsables de los aplicativos críticos en el momento de la contingencia.

Ingeniero encargado de Redes y Comunicaciones:

- Garantizar la operatividad de la infraestructura (Servicios y sistemas de información de la Personería de Bogotá D.C.), desde el punto de vista de las comunicaciones.
- Actualizar la bitácora correspondiente.
- Efectuar el monitoreo permanente de los componentes involucrados en la red de transmisión de datos.
- Adecuar el equipo de comunicación y reconfiguración de la red de transmisión de datos.
- Mantener contacto permanente con proveedor de internet.

Un funcionario de la Dirección de Tecnologías de la Información y Comunicación DTIC cumple las funciones de oficial de seguridad y vela constantemente por el cumplimiento de las políticas de seguridad institucionales, haciendo permanentemente recomendaciones para optimizar tanto su cumplimiento como la actualización permanente del presente plan. De igual forma, un Asesor con conocimiento en seguridad informática, es la mano derecha del Director de TIC y le brinda el apoyo suficiente como para saber qué estamento del Comité de Contingencia y Seguridad debe ser activado según la situación y apoya en la formulación de estrategias de mejoramiento permanente sobre las acciones ejecutadas por cada uno.

8.2 FASE II EVALUACIÓN DE RIESGOS E IMPACTO

Para realizar un análisis de los riegos, se procede a identificar los objetos que deben ser protegidos, los riesgos residuales, los potenciales riesgos secundarios, su impacto en la Entidad, y su importancia dentro del funcionamiento.

8.2.1 Identificación de Riesgos

A continuación se presenta la lista de los riesgos más comunes ocurridos en la Entidad, sobre los cuales se priorizará una acción de mitigación, que se debe plasmar en el “plan de prevención”

Datos / Información

- Errores de los usuarios
- Errores del administrador del sistema/ de la seguridad
- Alteración de la información
- Destrucción de la información
- Fugas de información
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Acceso no autorizado
- Modificación de la información
- Destrucción de la información
- Revelación de información

Servicios

- Errores de los usuarios
- Errores del administrador del sistema/ de la seguridad
- Alteración de la información
- Destrucción de la información
- Fugas de información
- Caída del sistemas por agotamiento de recursos
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Uso no previsto

- Acceso no autorizado
- Repudio (negación de actuaciones)
- Modificación de la información
- Destrucción de la información
- Revelación de información
- Denegación de servicio

Aplicaciones

- Avería de origen físico o lógico
- Errores de los usuarios
- Errores del administrador del sistema/ de la seguridad
- Difusión de software dañino
- Alteración de la información
- Destrucción de la información
- Fugas de información
- Vulnerabilidades de los programas (software)
- Errores de mantenimiento /actualización de programas
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Uso no previsto
- Acceso no autorizado
- Modificación de la información
- Destrucción de la información
- Revelación de información
- Manipulación de programas

Equipamiento Informático

- Fuego
- Daños por agua
- Desastres naturales
- Desastres industriales
- Avería de origen físico o lógico
- Corte del suministro eléctrico
- Errores de mantenimiento /actualización de equipos
- Caída del sistemas por agotamiento de recursos

- Perdida de equipos
- Abuso de privilegios de acceso
- Uso no previsto
- Acceso no autorizado
- Manipulación de hardware
- Denegación de servicio
- Robo de equipos
- Ataque destructivo

Redes de comunicaciones

- Fallo de servicio de comunicaciones
- Errores del administrador del sistema/ de la seguridad
- Errores de [re]encaminamiento
- Errores de secuencia
- Alteración de la información
- Fugas de información
- Caída del sistemas por agotamiento de recursos
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Uso no previsto
- [Re-]encaminamiento de mensajes
- Alteración de secuencia
- Acceso no autorizado
- Análisis de tráfico
- Interceptación de información (escucha)
- Modificación de la información
- Destrucción de la información
- Revelación de información
- Denegación de servicio
- Ataque destructivo

Equipamiento Auxiliar

- Desastres naturales
- Errores de mantenimiento / actualización de equipos (hardware)
- Uso no previsto

- Manipulación del hardware
- Ataque destructivo
- Acceso no autorizado
- Contaminación medioambiental
- Daños por agua
- Fuego

Instalaciones

- Fuego
- Daños por agua
- Desastres naturales
- Fuego
- Desastres industriales
- Contaminación electromagnética
- Suplantación de la identidad
- Abuso de privilegios de acceso
- Uso no previsto
- Acceso no autorizado
- Ataque destructivo

Personal

- Alteración de la información
- Destrucción de la información
- Fugas de información
- Indisponibilidad de la información
- Modificación de la información
- Revelación de información
- Indisponibilidad del personal
- Extorsión
- Ingeniería social
- Errores humanos
- Falta capacitación

8.2.2 Probabilidad de riesgo

Para que un riesgo sea considerado como amenaza al servicio, su probabilidad de ocurrencia debe ser superior a cero. De igual forma, la probabilidad de riesgo debe ser inferior al 100% pues en caso contrario correspondería a una certeza de ocurrencia de un evento. La probabilidad se puede entender también como la posibilidad de lograr un efecto, porque si la condición se produce, se supone que la posibilidad de que suceda será del 100%. Esta probabilidad la clasificaremos así:

Matriz de riesgo

MATRIZ DE RIESGOS		
PROBABILIDAD		
EFECTO	**VALORACIÓN**	**CRITERIO**
Raro	15%	Puede ocurrir excepcionalmente.
Posible	22%	Puede ocurrir en cualquier momento del futuro.
Probable	27%	Ocurre ocasionalmente
Casi cierto	36%	Ocurre en la mayoría de las circunstancias.

8.2.3 Impacto de riesgos

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la ocurrencia. Es una valoración aplicada al riesgo, para describir su impacto relacionado con la prestación del servicio normal. Cuanto mayor sea el número, mayor es el impacto.

Impacto del Riesgo

IMPACTO		
IMPACTO	**VALORACIÓN**	**CRITERIO**
Insignificante	1	Pérdida de control, operaciones, Información y/o equipamiento no sensibles.

Moderado	2	Pérdida de control, operaciones, Información y/o equipamiento medianamente sensibles.
Mayor	3	Pérdida de control, operaciones, información y/o equipamiento medianamente sensibles que pueden causar retraso o interrupción de servicios.
Catastrófico	4	Pérdida de control, operaciones, Información y/o equipamiento críticos que puede causar daño serio de infraestructura o destrozo patrimonial

8.2.4 Exposición a riesgos

La exposición al riesgo es el resultado de multiplicar la probabilidad por el impacto. En ocasiones, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin inconvenientes; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se podría pensar en ignorarlo, en cuyo caso habrá que considerar también la criticidad de dicho evento. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.

Exposición al riesgo

EXPOSICIÓN					
Probabilidad	15%	0,15	0,3	0,45	0,6
	22%	0,22	0,44	0,66	0,88
	27%	0,27	0,54	0,81	1,08
	36%	0,36	0,72	1,08	1,44
		1	2	3	4
		Impacto			

8.2.5 Ponderación del riesgo

PONDERACIÓN

Prioridad A	Riesgo Alto: Requiere medidas a tomar de manera urgente. (Igual o mayor a 1)
Prioridad B	Riesgo Moderado: Requiere medidas necesarias a tomar. (Entre 0,5 y 0,99)
Prioridad C	Riesgo Bajo: No requiere medias a tomar, aunque se tendrá en permanente vigilancia. (Entre 0 y 0,49)

8.2.6 Identificación de procesos

Identificación proceso de automatización		
Servicios	Sistemas de información y Aplicaciones móviles	SICAPITAL
		SICAPITAL Extranet (Hacienda)
		CORDIS u Orfeo
		SINPROC
		Sistema radar
	Servicios de red	Correo electrónico
		Acceso a internet
		Intranet
		Página web
		Directorio activo
		DNS, DHCP
Software base	Programas y sistemas específicos	Motores bases de batos
		Sistema Digiturno
		Control de visitantes
		Herramientas de desarrollo
		Apis - Monitoreos – Ejecutables
		ARGIS – sistema de mapa digital
		Herramientas de ofimática
		Antivirus
		Pcsecure
		Monitoreos

		Ejecutables de aplicaciones
		Backup de base de datos
		Backup de información sensible
		Backup de plataforma de aplicaciones (sistemas)
		Backup de website
		Backup configuración servidores
		Backup configuración switches

Identificación proceso de soporte		
Infraestructura operacional	Infraestructura de respaldo	Sistemas operacionales
		Sistemas de aire acondicionado
		Sistema inint.de potec. Ups´s
		Planta eléctrica
		Equipos de primeros auxilios
		Sistema de control de incendios
	Infraestructura de redes y comunicaciones	Switch core
		Switches de borde
		Appliance de seguridad
		Routers inalámbricos
		Cableado estructurado
		Cuartos de telecomunicaciones
		Backbone de voz y datos
	Infraestructura de servicios	Servidores de red
		Estaciones de trabajo
		Impresoras
		Scanners
		Planta telefónica
		Teléfonos
		Portátiles
		Celulares

		Tabletas

8.2.7 Registros

8.2.7.1 Sistemas de información

De acuerdo con la prioridad de los riesgos y el impacto generado, como resultado la siguiente relación de procesos críticos, con prioridad alta, media y baja, procesos que deben estar disponibles 99.9%.

Sistemas de Información

SISTEMA INTEGRADO DE PROCESOS SINPROC	
Objetivo: Sistema para el registro, consulta y modificación de procesos Misionales	
RESPONSABLES	COMPONENTES CRÍTICOS
Encargado del sistemas de información Ingeniero de área Ingeniero Junior – Ingenieros Desarrolladores	Antecedentes disciplinarios
	Firma Digital de antecedentes (Hilopas)
	Módulo Quejas por internet Q.R.S.D

SISTEMA INTEGRADO DE PROCESOS SINPROC	
RESPONSABLES	COMPONENTES CRÍTICOS
Encargado del sistemas de información Ingeniero de área Ingeniero Junior Ingenieros desarrolladores	Módulo procesos disciplinarios
	Módulo de requerimiento ciudadano (Personal y escrito)
	Módulo de fallos
	Módulo de querellas
	Módulo centros comerciales
	Módulo de tutelas
	Módulo de ministerio público (Familia)
	Módulo grupo PAS
	Módulo de Conciliaciones

BASE DE DATOS	Weboido , Siafi2
DEPENDENCIAS DEL SERVICIO	Servidor de aplicaciones App, “Ficha Técnica Servidores” Servidor de Base de datos BDPerso Servicio DNS´s, EXTERNO Servicio de Internet Red LAN, “Diagrama de Red Interna y Externa”
Uso: 7X24	
Usuarios: Delegadas Disciplinarios I, II, III, IV. Policivo, C.A.C., Oficina Jurídica, Ministerios Públicos, Finanzas, Asuntos de Gobierno, Línea 143, Grupo Requerimiento Ciudadano, Oficina de Conciliaciones, Grupo PAS, Derechos Humanos Operadores: Asesores y Secretarias	

SISTEMA PERNO	
Objetivo: Sistema para el registro, consulta y modificación de Novedades de la Nómina de la Entidad	
RESPONSABLES	COMPONENTES CRÍTICOS
Encargado del sistemas de información Ingeniero de área Ingeniero Junior Grupo - Subdirección De Gestión De Talento Humano	Hojas de Vida Liquidación Consultas de Nómina Novedades
BASE DE DATOS	SICAPITAL
DEPENDENCIAS DEL SERVICIO	Servidor de Aplicaciones App03,

	Servidor de Base de datos BDPERSO Servicios DNS´s Servidor Persobogota1 Servicio de Internet Red LAN
Uso: 5X8 Usuarios: Todos los funcionarios(as)(as) de Planta de la Personería de Bogotá D.C. Operadores: Grupo de Subdirección de Gestión de Talento Humano	

SISTEMA CORDIS	
Objetivo: Sistema para el registro y consulta de la Correspondencia Interna y Externa de la Entidad	
RESPONSABLES	COMPONENTES CRÍTICOS
Encargado del sistema de información Ingeniero Junior Ingeniero de área Grupo - Secretaria General Correspondencia	Registro de correspondencia Interna y Ext. Seguimiento documental Etiquetas para el envío y recepción
BASE DE DATOS	Siafi2
DEPENDENCIAS DEL SERVICIO	Servidor de Aplicaciones App02, “Ficha técnica Servidores de Respaldo y Contingencia” Servidor de Base de datos DBCONTI, Servicios DNS´s Servidor Persobogota1 Servicio de Internet Red LAN
Uso: 5X8 **Usuarios**: Todas las dependencias de la Personería de Bogotá D.C.	

SISTEMAS EMERGENTES

Objetivo: Sistema para el registro de información relacionada con el requerimiento ciudadano en LINEA 143	
RESPONSABLES	COMPONENTES CRÍTICOS
Ingeniero encargado del sistema de información	 Sistema Radar
BASE DE DATOS	Weboido
DEPENDENCIAS DEL SERVICIO	Servidor de Aplicaciones App Servidor de Base de datos BDPERSO Servicios DNS´s Servidor Persobogota1 Servicio de internet Red LAN
Uso: 7X24 Usuarios: usuarios externos Operadores: Línea 143	
SISTEMAS DIGITURNO	
Objetivo: Sistema para el llamado de turnos en el Centro de Atención a la Ciudadanía y Delegada para Protección de Víctimas del Conflicto Armado	
RESPONSABLES	COMPONENTES CRÍTICOS
Encargado del sistema Ingeniero Junior	Módulos de atención Módulos virtuales de selección Módulo de tableros de llamados
BASE DE DATOS	DIGITURNO 4.5
DEPENDENCIAS DEL SERVICIO	Servidor Digiturno-pc, Servicio de Canal de datos Sedes externas, “Interconexión sedes externas” Red LAN Impresora EPSON Monitores de turnos
Uso: 5X8 Usuarios: Ciudadano que visita la Entidad para la solución de temas relacionados con:	

Servicios Públicos, Atención Prioritaria en Salud, Consultas de Tutelas, Consultas por Servicios Públicos, Derecho al Trabajo, Derecho Consumidor, Impugnación y Desacatos, Orientación Jurídica, Otros Servicios, Pensiones, Salud, Tutelas, Restitución de tierras, Víctimas del conflicto armado, Operadores: Funcionarios(as)(as) Asesores del centro de Atención y de Delegada de victimas

Operadores: Secretarias de dependencias

SISTEMA ADMINISTRATIVO Y FINANCIERO EXTRANET	
Objetivo: Es una herramienta informática creada por la Secretaría Distrital de Hacienda (SDH) para satisfacer las necesidades de administración de la información en Entidades del sector público, de los niveles nacional, territorial y distrital. Está integrada por componentes administrativos, financieros, tributarios y pensionales.	
RESPONSABLES	COMPONENTES CRÍTICOS
Ingeniero de Soporte Técnico encargado Funcionarios (as)(as) de Secretaria de Hacienda ETB	Presupuesto (Módulo Predis)
	Cronograma de presupuesto (Módulo Opget)
	Planillas de Pagos (Módulo Opget)
	Plan de cuentas (Módulo PAC)
DEPENDENCIAS DEL SERVICIO	Enrutador de Hacienda Red LAN Configuración especial del HOST de las estaciones “Instructivo para instalar un cliente Secretaria de Hacienda o Planeación”
BASE DE DATOS	10.168.13.7
Uso: 7X24 Usuarios: Dirección administrativa y Financiera Dirección de Talento Humano	

Sub Dirección Administrativa y Financiera Operadores:

Prioridad C - Sistemas de Información

SISTEMA DE CONTROL DE VISITANTES	
Objetivo: Es una herramienta encargada de administrar, ordenar, dirigir o regular el control de acceso a la Entidad de agentes externos o visitantes	
RESPONSABLES	COMPONENTES CRÍTICOS
Subdirección de Gestión Documental y Recursos Físicos - Admón. Edificio	Software Base de datos
	Módulo de captura
DEPENDENCIAS DEL SERVICIO	Red LAN
BASE DE DATOS	VISITANTES.BMP
Uso: 5X8 Usuarios: Sub Dirección Administrativa y Financiera Operadores:	

Prioridad A – Servicios

CORREO ELECTRÓNICO	
Consideración	**Observación**
Nivel de importancia de la aplicación en la Entidad	Alto
Impacto operativo, financiero o contable	4
Oportunidad de servicio	Trabajo colaborativo otorgado por la Alcaldía de Bogotá
Programas críticos	Agenda
	Herramientas colaborativas
	Drive
	Chat
	Listas de distribución
Usos críticos	Comunicación interna y externa de los funcionarios(as)(as) de la Entidad, envío y recepción de

	información y archivos de carácter urgente Notificaciones a los investigados, etc. Dispositivos Móviles. Compartición de documentos y trajo simultáneo desde cualquier lugar. Comunicación en tiempo real y realización de video conferencias, entre equipos de trabajo. Creación Sitios web.
Comunicaciones: Entrada y salida de datos	Ingreso de información archivos y temas
	Envío de información archivos y temas
	Backup de correos y archivos
	Mensajería Instantánea
	Compartición de Archivos
Dependencias del Servicio	Servicio de Internet Canal de Datos Red LAN Convenio Interadministrativo anual.

INTRANET	
Consideración	**Observación**
Nivel de importancia de la aplicación en la Entidad	Medio
Impacto operativo, financiero o contable	2
Oportunidad de servicio	Trabajo colaborativo que día tras día se convierte en la herramienta primordial de acceso a operaciones y procesos críticos
Programas críticos	Portal de Oracle
	Java Run time
	WorkFlow
	Digifile
Usos críticos	Acceso a los servicios en línea Acceso a los procedimientos de la Entidad Acceso a los formularios

	Acceso a temas de interés de los funcionarios(as)(as)
Comunicaciones: entrada y salida de datos	Documentos
	Servicios
	Normativas
	Información de interés general interno
Dependencia	DNS Interno, Servidor Persobogota1 Base de datos INTRANET Red de datos LAN Servidor App Servidor INTRANET.SRV,
PAGINA WEB	
Consideración	**Observación**
Nivel de importancia de la aplicación en la Entidad	Alto
Impacto operativo, financiero o contable	4
Consideración	Observación
Oportunidad de servicio	Imagen corporativa; servicios al ciudadano, antecedentes disciplinarios en línea
Programas críticos	JOOMLA
	Java
	PHP
	MYsQL
	Servicios Intranet
	Indagar
Usos críticos	Portal de acceso a la información para el ciudadano
	Expedición de antecedentes Disciplinarios WEB
	Quejas por internet
Comunicaciones: entrada y salida de datos	Correos en línea

	Chat
	Foros
Dependencia	DNS Interno y Externo
	Servicio de Internet
	Base de datos DBPERSONERÍA DE BOGOTÁ D.C.
	Red de datos LAN
	Servidor WEB,
ACCESO A INTERNET	
Consideración	**Observación**
Nivel de importancia de la aplicación en la Entidad	Alta
Impacto operativo, financiero o contable	3
Oportunidad de servicio	Contacto con Proveedores, otros agentes de ministerio público, acceso a los portales de Gestión, Renovación Tecnológica, Investigación
Programas críticos	Portal de contratación Sivicof
	Acceso a ACUEDUCTO
	Indagar
Consideración	Observación
Usos críticos	Normativa
	Noticias relacionadas con la misión de la Entidad
	Teleconferencias
	Capacitación
Comunicaciones: entrada y salida de datos	Descargas de documentos, archivos e información
	Consulta de información, etc. Indagar
Dependencia	Canal de datos de Internet ETB, Contrato 450/13
	Firewall de acceso Perimetral
	DNS Interno y Externo
	Red LAN

DIRECTORIO ACTIVO	
Consideración	**Observación**
Nivel de importancia de la aplicación en la Entidad	Medio
Impacto operativo, financiero o contable	3
Oportunidad de servicio	Software libre mantenido con contrato de soporte a LINUX
Programas críticos	Samba 4
	DNS
	Indagar
Usos críticos	Acceso de los usuarios a los Computadores de la red
	Políticas de directivas de grupo
	Compartición CONTROLADA de archivos LAN
	Papel tapiz
	Instalación de programas
Comunicaciones: entrada y salida de datos	N/A
Dependencia	Red LAN Servidor PERSOBOGOTA1 y todos sus servicios,

Bases de Datos

Consideración	**Observación**
Nivel de importancia de la aplicación en la Entidad	Alto
Impacto operativo, financiero o contable	4
Oportunidad de servicio	El motor de base de datos es muy estable y maneja seguridades de acuerdo a su afinamiento y administración
Productos críticos	ASM

	Enterprise manager
	LISTENER
	SQL/PLUS
	Indagar
Usos críticos	Instancia ORCL
	Instancia de WEBOIDO (Sistema SINPROC)
	Instancia de Siafi2 (Correspondencia)
	Instancia de SICAPITAL (siprueba)
	Instancia INTRANET
Comunicaciones: entrada y salida de datos	Información misional
	Información critica
Dependencia	Red LAN, DNS interno y externo Canal de datos de Internet ETB Firewall de acceso perimetral Servidor BDPERSO

Antivirus

Prioridad A – Antivirus

Consideración	Observación
Nivel de importancia de la aplicación en la Entidad	Alto
Impacto operativo, financiero o contable	3
Oportunidad de servicio	Todos los días hay nuevas amenazas, el antivirus es una herramienta que mediante consola automatiza toda actualización y no necesita instalarse si desplegar un agente liviano

Consideración	Observación
Productos críticos	Consola ePO
	Agente McAfee
	Motor 8.8 última versión ePA
	SQL/PLUS

	DLP (para dispositivos)
	Indagar
Usos críticos	Escaneo automático
	Impide la instalación de programas
	Limpia y elimina virus
	Impide ingreso de código malicioso
Comunicaciones: entrada y salida de datos	N/A
Dependencia	Red LAN Directorio Activo, Servidor Persobogota1 Servidor CONSOLAEPO,

Prioridades:

La estimación de los daños en los bienes y su impacto, establece la prioridad en relación al tiempo estimado y los recursos necesarios para la recuperación de los servicios afectados con el incidente.

Por lo tanto los activos valorados como prioridad A o más alta, serán los tenidos en cuenta en el proceso de restablecimiento ante un evento.

Fuentes de daño:

- Accesos no autorizados
- Código malicioso (Virus, sabotaje).
- Mala operación o malas intenciones.
- Desastres Naturales
- Fallas en la infraestructura de soporte (UPS´s, Sistema de aire acondicionado)
- Fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo por arte de la Entidad.
- Fallas de las comunicaciones.
- Abandono de sus puestos de trabajo.
- Otros imponderables.

- Fallas de Hardware

8.3 FASE III: PLAN DE RESPUESTA Y RECUPERACIÓN

8.3.1 Medidas preventivas

Control de Accesos: El control de acceso reside en la autorización, autenticación, autorización de acceso y auditoría, donde se definen medidas efectivas para controlar el ingreso a los activos computacionales:

- Acceso físico de personas no autorizadas.
- Acceso a la Red de PC's y Servidores.
- Acceso restringido a las librerías, programas, y datos.

Respaldos: Resguardo adecuado de los dispositivos críticos. Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, entre los cuales se cuenta:

- UPS de respaldo de actual Centro de Computo
- Centro de datos alterno

Seguridad Física del Personal: Tomando las medidas adecuadas que permitan mejorar los niveles de seguridad, capacitando apropiadamente al personal, soportando personal de respaldo en funciones o reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones, permisos, calamidades o enfermedad.

Seguridad de la Información: La información y programas de los Sistemas de Información que se encuentran en el Servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado.

Plan de mitigación y respaldo: El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación y/o restablecimiento. Todos nuevos diseños de Sistemas, o proyecto realizado deben tener

un plan de respaldo. Se deben tener presentes las bitácoras como documentación de eventos que sirven de apoyo para restablecer un servicio con ocurrencia repetida.

Respaldo de datos Vitales: Identificar las áreas para realizar respaldos:

- Sistemas de Información.
- Configuraciones e instalaciones
- Sistemas de Red.
- Sistemas de backup
- Nube

8.3.2 Reacción Inicial

El responsable de la seguridad informática quien declara la emergencia debe:

- Determinar qué clase de siniestro o incidente se ha presentado.
- Dar aviso al administrador de edificio en caso necesario.
- Notificar a los miembros del equipo de recuperación que se consideren necesarios, de acuerdo con el tipo de suceso presentado.
- Mantener actualizados a los funcionarios(as)(as) sobre la evolución de la emergencia.
- Nombrar otros miembros del equipo cuando así lo exijan las circunstancias.
- Definir los servicios que se deban trasladar de la nube publica al Data Center de la Entidad o viceversa, en caso de que el siniestro así lo requiera.
- Analizar las alternativas de procesamiento de acuerdo con la evaluación del daño.
- Establecer los controles que considere necesarios para llevar a cabo las actividades del plan, en forma confiable.
- Determinar, con los otros miembros y con el proveedor del equipo, la magnitud del daño generado por el siniestro y establecer si se requiere poner en marcha el Plan.
- Poner en marcha el Plan.

Plan para traslado al respaldo

- Efectuar una reunión inicial del equipo humano de recuperación para distribuir las tareas y responsabilidades asignadas de acuerdo al Plan de recuperación.

- Coordinar los recursos de comunicación para la activación de los procesos de restauración, grabación y puesta en marcha en la Nube pública.
- Obtener los medios de los Backups en su versión más actualizada en caso de pérdida de información.
- Nombrar otros miembros del equipo cuando así lo exijan las circunstancias.
- Ordenar, junto con los otros miembros del equipo, el traslado a los Sistemas Alternos de los recursos adicionales que se requieran.

Tareas en sitio alterno de respaldo

- Verificar que se estén efectuando adecuadamente los procedimientos de recuperación.
- Coordinar el flujo de los documentos e información entre la Personería de Bogotá D.C., y los sistemas alternos.
- Coordinar que se provean los recursos para la ejecución normal de las labores en la Nube Pública o viceversa según la contingencia.
- Verificar los informes de funcionamiento de las aplicaciones críticas, con el fin de asegurar su adecuada operación.
- Autorizar la operación de las aplicaciones críticas.
- Revisar los informes obtenidos en la ejecución de las aplicaciones críticas.
- Verificar y analizar que la información producida sea confiable, con base en los controles definidos.

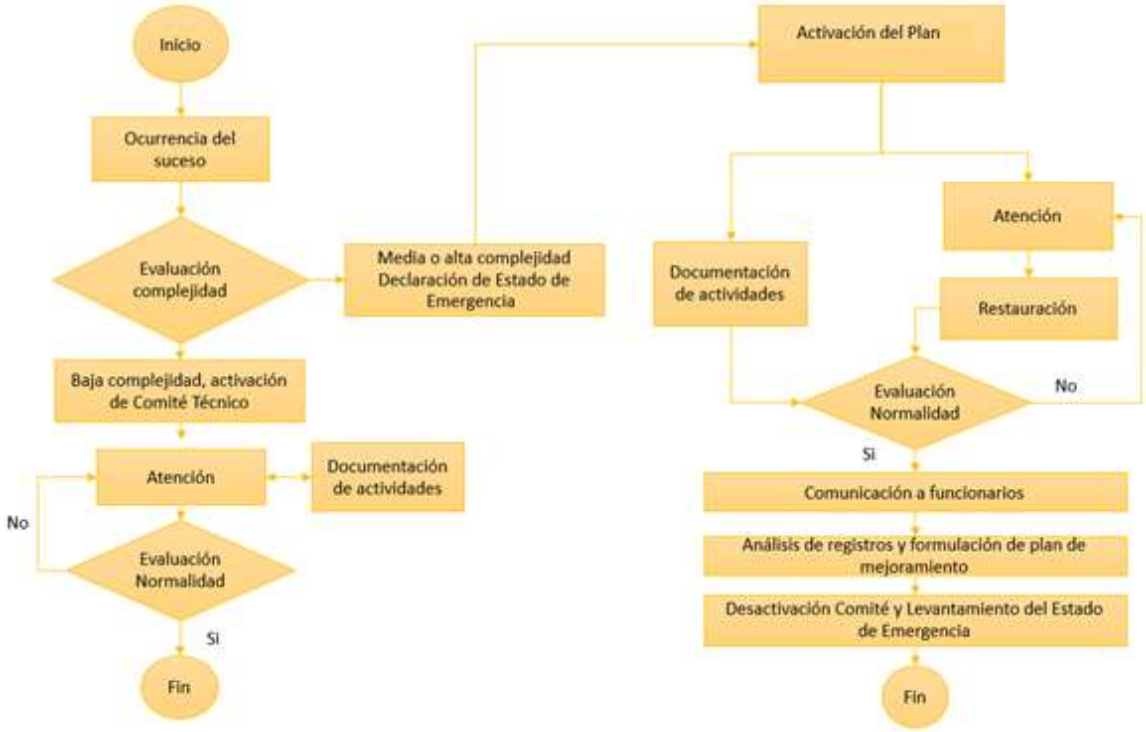
Retorno a la normal operación

- Coordinar el regreso a una situación normal de operación.
- Iniciar las tareas conducentes a restablecer la normalidad de la operación en el menor tiempo posible.
- Coordinar la adecuada instalación del hardware.
- Coordinar la adecuada instalación del software aplicativo, operativo y utilitario.
- Coordinar la instalación de las comunicaciones.
- Verificar que la operación de las aplicaciones críticas se realice en forma satisfactoria mediante pruebas iniciales y análisis de controles.
- Coordinar el traslado de las operaciones al centro de cómputo de la Entidad comité técnico operativo de la Personería de Bogotá D.C.

- Autorizar la operación de las aplicaciones.
- Revisar los informes obtenidos de la ejecución de las aplicaciones.
- Verificar y analizar que la información producida sea confiable, con base en los controles definidos previamente.
- Liberar al Sistemas Alternos de los recursos innecesarios que se hayan requerido durante la contingencia.
- Dar por concluida la situación de emergencia, en compañía de los otros miembros del equipo.
- Informar al Comité Directivo sobre el restablecimiento normal de las operaciones.

El siguiente flujo muestra en detalle las fases y etapas por las que la Personería de Bogotá D.C., atravesará una vez producido el evento que conlleve a aplicar el Plan de Continuidad.

8.3.3 Flujo para la Activación Plan de Continuidad



8.3.4 Recuperación de operaciones

Parte de la premisa de que ha ocurrido un evento de gran magnitud o un desastre originado por daño, error o incidente no controlable, pero que puede dejar operativos los sistemas temporalmente o reemplazarlos y vueltos a la normalidad durante el transcurso de 5 días como mínimo.

Contempla las gestiones necesarias durante la materialización de un incidente no controlable. Su finalidad es operar temporalmente como plan de continuidad de negocio de servicios tecnológicos y restaurar los procesos a la normalidad a partir de procedimientos definidos para tal fin. El objetivo es restablecer las operaciones de los recursos en el menor tiempo posible.

El nivel de este evento es considerado crítico cuando según la matriz se ve afectada la integridad de la Entidad y se puede perder la gestión que conlleva a la pérdida de

credibilidad y confianza en la misión de la Entidad. Los riesgos secundarios tienen una alta severidad y derivados de un riesgo residual con alta severidad.

Cada uno de estos procesos debe llevarse de la manera más detallada posible, ya que las prioridades de continuidad se consigan como resultado. Se permite el uso de sistemas manuales mientras es gestionada.

Se pretende restablecer en el menor tiempo posible el nivel de operación normal del centro de datos, basándose en los planes de emergencia y de respaldo a los niveles del Comité Técnico Operativos y de los demás niveles.

La responsabilidad sobre el plan de recuperación es de la administración, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

El plan de recuperación contempla los siguientes objetivos:

- Determinar las políticas y procedimientos para respaldar las aplicaciones y los datos.
- Planificar la reactivación dentro de las 12 horas de producido un desastre, el sistema de procesamiento y las funciones asociadas.
- Supervisar los sistemas y aplicaciones.
- Establecer las acciones a realizar para garantizar una oportuna respuesta frente a un desastre.

8.3.5 Activación del Plan

Queda a juicio del Director de emergencias determinar la activación del Plan, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste.

Los Directores de cada área determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

Se aplicará el procedimiento siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres de operaciones).

Parte de la pregunta ¿Qué eventos activan la Contingencia? A fin de establecer los mecanismos de mitigación más importantes en las incidencias más críticas de alto impacto.

Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente alertada. Su finalidad es mitigar los efectos adversos de la posible y probable amenaza.

Tiene como objetivo mantener operativo los equipos para el correcto funcionamiento de la red y procesos más críticos en la Personería de Bogotá D.C.

Cada documento, debe guiar el paso a paso de reinstalación y configuración del servicio afectado y puede ser retroalimentado por cada uno de los ingenieros que participen en el proceso de restauración del servicio, de acuerdo con la responsabilidad de gestión de mitigación

8.3.6 Prioridades del plan de Continuidad de Negocio de Servicios Tecnológicos

Eventos a tener en cuenta como señales de prevención

- Alarma del centro de cómputo.
- Alarma del (los) servidor(es).
- Alarmas del (los) equipo(s) de comunicación.
- Reporte de falla de aplicaciones (falta de acceso, lentitud, perdida de información, latencias, errores de código).
- Reporte de falla de servicios (falta de acceso, lentitud, perdida de gestión, latencias, errores de ejecución).
- Reportes de pérdida de conexión a la base de datos
- Reporte de inasistencia del personal: administrador de la red, administrador de las bases de datos, administrador de soporte técnico.
- Mensajes de error durante la ejecución de programas.
- Falla general en las estaciones de trabajo.
- Falla de comunicación de estaciones de trabajo
- Fallo de comunicación telefónica.
- Anuncio de virus informático.

¿Qué hacer cuando ocurre una alarma?

La gestión de mitigación contempla los siguientes procedimientos:

- Notificación de la incidencia mediante correo electrónico ***admin@personeriabogota.gov.co*** o telefónicamente al área de soporte a la extensión 333
- Aviso de notificación al Director de la Dirección de Tecnologías de la Información y Comunicación DTIC.
- Transferencia de caso al grupo Técnico operativo que corresponda, (el ingeniero designado por el Director de Tecnologías encargado de cada una de las áreas de DTIC) para gestionar mitigación.
- Identificación de los equipos con alta disponibilidad con que se cuenta en el momento, relacionados con su correspondiente respaldo (potencia regulada, equipos de comunicaciones y seguridad perimetral). Aplicación del procedimiento relacionado según el caso por parte del Ingeniero de cada área o en su delegación al Ingeniero Junior.
- Registro en la Bitácora de eventos

8.3.7 Elementos necesarios para continuidad de operaciones

Formatos de captura de procesos: Se trata de un formulario para “tramite usuario y tramite respuesta” elaborado en hoja de cálculo, el cual sirve para la captura de los procesos misionales entre ellos, procesos disciplinarios, requerimiento ciudadano, PQRs, trámite respuesta, veedurías, ministerios públicos, antecedentes disciplinarios etc. y que puede ser migrado fácilmente en el momento de poner en producción el sistema SINPROC.

Servicio cloud: Se debe tener en cuenta que centró en operación el servicio de la Nube que permite tener 99.9% de disponibilidad de los servicios más críticos de la Entidad y que contempla la replicación de estos servicios de manera geográficamente distante de manera automática, con copia de respaldo incluida y en caso de que alguno de los servicios falle en esta plataforma se utilizaría los copia de los servers en el Data Center de la Entidad, donde cada uno de los servidores de alta criticidad está en producción y los del centro de cómputo tienen copia. En este caso se puede aplicar contingencias de manera trasversal

Copias de respaldo (Backups): Importante recurso para restauración inmediata y que se activa como la contingencia más efectiva para la recuperación de los datos, tan pronto ocurrido el siniestro.

Infraestructura de respaldo:

Centro de datos espejo: Este un requerimiento importante para la continuidad de operación de los servicios tecnológicos, dado que allí es donde se debe instalar y configurar un centro de datos alterno que entrará en operación inmediatamente suceda un siniestro y que permita la continuidad de las operaciones de la infraestructura, para lo cual se requieren los siguientes componentes:

Switches de respaldo: Se requiere contar con equipos de respaldo para las comunicaciones hacia los servicios más críticos en el momento de pérdida de

comunicación del CORE (equipo principal de red que controla los dispositivos de comunicaciones). Estos equipos deben estar dispuestos en un centro de comunicaciones alterno.

Servidores: Se requieren equipamiento espejo del centro de datos en operación Donde se alojaran las bases de datos, aplicaciones que soportan los procesos misiones de la Entidad.

Sub estación eléctrica: se sugiere disponer de una estación eléctrica alterna ubicada en un sitio estratégico fuera de la zona, que en un evento crítico permita subsanar el incidente eléctrico

Ups: Se trata de un equipo operativo que reemplace la UPS que están en el centro de datos principal y que se puede disponer en el momento de daños de interrupción de la UPS que alimenta el parque computacional de la Entidad.

Canales de comunicaciones: Se debe tener en cuenta con los proveedores de los enlaces la disponibilidad de los enlaces alternos, para re direccionar las comunicaciones al centro de datos alterno.

Nube privada: Se sugiere contratar una nube privada para que en caso de siniestro, opere como centro de datos alterno y garantizar la continuidad de operaciones en cuento a infraestructura tecnológica de datos y aplicaciones. Es de anotar que para que opere correctamente, se requiere un canal de comunicaciones que permita a los usuarios finales llegar a este. (switch alterno y canal de comunicaciones alterno) de lo contario no es funcional esta alternativa.

8.3.8 Recursos afectados

Centro de datos redes y comunicaciones

- Apagado total del Centro de datos
- Pérdida de operaciones de los servicios en la Nube
- Pérdida de operaciones de los servicios del Centro de datos
- Daños físicos de Infraestructura

Descripción del problema: Se encuentra que es imposible el uso de Centro de Cómputo en su totalidad, ya que hubo un incidente catalogado como no controlable, fallo de energía o una falla humana de operación catastrófica para los sistemas.

Tiempo de Tolerancia: 5 días - Capacidad en tiempo de soportar sin perjuicios para el restablecimiento de los servicios más críticos, pasada la recuperación, se esperan 20 días para recuperar totalmente la operación de los sistemas en la nube pública.

Procedimiento a seguir:

- Dentro de las 6 horas siguientes al desastre se debe:
  - ✓ Notificar a los usuarios la interrupción del servicio.
  - ✓ Notificar al Director de Tecnologías y al ingeniero designado por el Director de Tecnologías encargado de las áreas.
  - ✓ Activar el procesamiento manual de las aplicaciones (si es necesario), cuya responsabilidad es del Comité Técnico de Operación.
  - ✓ Efectuar una evaluación de daños e identificar equipos reusables para transferirlo al Centro de datos temporal.
  - ✓ Notificar al Proveedor las configuraciones de hardware y alistar los requerimientos.
  - ✓ Notificar a todos los funcionarios(as)(as) de la Dirección de Tecnologías, que están involucrados en el Plan.
  - ✓ Seleccionar y catalogar las oficinas de servicio para el procesamiento de los reportes de respaldo.
  - ✓ Inicializar las preparaciones ambientales en el Centro de Cómputo temporal. (voz, datos red eléctrica).
  - ✓ Ordenar los servicios para comunicación de datos en la nube pública, si es necesario.

- Dentro de las 24 horas siguientes al desastre debe:
  - ✓ Contactar con el proveedor y ordenar el soporte tanto de hardware como de software
  - ✓ Iniciar y coordinar los procedimientos de preparación del lugar para el Centro de Cómputo Temporal.

- ✓ Iniciar el ensamblaje de la documentación y medios magnéticos en el lugar de almacenamiento externo (Cinto-teca de la Dirección de Tecnologías).
- ✓ Confirmar el soporte dado por el proveedor.
- ✓ Complementar el procesamiento de los reportes seleccionados en el Centro de datos alterno.

- Dentro de los 2 días siguientes al desastre debe:
  - ✓ Catalogar el despacho de suministros
  - ✓ Trasladar el personal necesario y/o requerimientos al Centro de Cómputo Temporal
  - ✓ Completar el ensamblaje de la documentación y los medios magnéticos en el Centro de Cómputo Temporal, coordinando la prestación de los servicios desde el Centro de Cómputo Temporal.

- Dentro de los 3 días siguientes al desastre:
  - ✓ El Centro de Cómputo Temporal debe estar totalmente preparado para operar
  - ✓ Llevar el inventario de los medios magnéticos, los listados y otra documentación en el Centro de Cómputo Temporal.
  - ✓ Recibir en el Centro de Cómputo Temporal suficientes suministros, muebles y equipo relacionado.
  - ✓ Determinar el punto inicial de aplicaciones críticas.
  - ✓ Establecer un catálogo de procesamiento de las aplicaciones críticas.
  - ✓ Evaluar las líneas de comunicación de datos catalogados para una restauración inicial.

- Dentro de los 4 días siguientes al desastre debe:
  - ✓ Completar la preparación ambiental del Centro de Cómputo Temporal
  - ✓ Recibir la documentación y el medio magnético de los lugares de almacenamiento en el Centro de Cómputo Temporal.
  - ✓ Asegurar el ambiente físico en el Centro de Cómputo Temporal y establecer la seguridad de los datos.
  - ✓ Restablecer los backups de datos de producción de las cintas de backups.
  - ✓ Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
  - ✓ Evaluar los sistemas operacionales

- ✓ Notificar a los usuarios el estado de la recuperación y validar operaciones en las estaciones de trabajo.

- Dentro de los cinco días siguientes al desastre:
  - ✓ Asegurar la operación total de los sistemas críticos.
  - ✓ Migrar datos de los sistemas manuales al sistema en producción.
  - ✓ Continuar la implantación por fases de la red de comunicación de datos

- Dentro de los 20 días siguientes al desastre:

Restauración completa de la red de comunicación de datos y de las Operaciones.

Amenazas asociadas (Centro de datos redes y comunicaciones)

Amenazas	Riesgo	Recomendación
Desastre físico	B	En el caso de incidente no controlable (ya descrito en identificación de riesgos) en el Centro de Cómputo, deben ejecutarse inmediatamente los procedimientos de emergencia implementados por el grupo de Salud Ocupacional previa notificación a uno de sus integrantes.
Mala operación (falla humana)	M	Determinar el punto de quiebre mediante diagnóstico, notificar a la Dirección del Plan, gestionar restauración y documentar
Daño del fluido eléctrico	M	Solicitar la activación de la UPS alterna para reiniciar los servicios
Daño del aire acondicionado	B	En caso de evidencia de daño, se activaría el interruptor de la condensadora que se encuentra en la parta posterior del Centro de Cómputo, marcado como “CONDENSADORA”, en el segundo tablero de izquierda a derecha.

Pérdida de operaciones de los servicios en la Nube Pública

Descripción del problema: Uno o varios servicios se encuentran inoperantes con caídas de las comunicaciones o daño total de los equipos virtualizados, ya que hubo un incidente

catalogado como no controlable, fallo de energía o una falla de operación por error humano o caída del canal de internet.

Tiempo de tolerancia: 5 días - capacidad en tiempo de soportar sin perjuicios, algún imprevisto

Procedimiento a seguir:

- Solicitar al documentador técnico acceso al archivo para la activación de servidores de contingencia.
- Solicitar al administrador de bases de datos backups de la información
- Solicitar la “guía de instalación de servidores y aplicaciones en caso de ser necesario.
- Verificar que la causa del problema y restaure la última actualización del aplicativo; si los datos han sufrido daños restaure desde el último Backup

Amenazas asociadas

Pérdida de operaciones de los servicios en la Nube Pública

Amenazas	**Riesgo**	**Recomendación**
Borrado o modificación de alguno de sus componentes	M	Restauración de copias de respaldo (backups) Identificación del componente faltante
Aparición de virus informático	B	Mantener software antivirus actualizado. Mantener software Guardián y vacunar todo tipo de información que penetre al servidor
Interrupción del fluido eléctrico	A	Mantener en buen estado el sistema de UPS y contrato de mantenimiento al día
Sabotaje	M	Creación de políticas de control para el acceso al Centro de Computo y en especial a los servidores y/o equipos de cómputo

Daños físicos de Infraestructura

Daño físico Servidores en el Centro de Cómputo de la Entidad.

Descripción del problema: El servidor no puede responder a los requerimientos de los clientes. Los recursos de red no pueden ser accedidos o el servidor no responde y no permite ingresar desde consola.

Tiempo de Tolerancia: 6 horas.

Procedimiento a seguir

- Llamada de servicio con carácter urgente y comunicar al encargado del Centro de datos.
- Esperar el diagnostico; si excede el tiempo de tolerancia para su recuperación, aplicar procedimiento de contingencia en la nube o el servidor alterno.
- Restaurar el soporte del disco(s) en espacio temporal y llamar al servicio de soporte con carácter urgente.
- Llamada de servicio con carácter urgente y comunicar al encargado del Centro de datos.
- Llamar al Proveedor.
- Llamar al servicio de soporte con carácter urgente.

Amenazas asociadas

Daño en alguno de los equipos (disco, memoria, procesador, main board) que afecte la función de multitarea, bloqueos continuos y caídas del sistema. No se deja “accesar” y por tanto no reinicia el sistema.

Daños físicos de Infraestructura

Amenazas	Riesgo	Recomendación
Se queme el disco duro	B	Mantener regulada la energía eléctrica. En caso de incendio extinguir, en primer lugar, el fuego de la CPU (En la CPU se encuentra toda la información del servidor).

		Mantener extintores.
Posibilidad de que se moje	B	No debe estar cerca a los ductos de agua. No debe estar cerca de la ventana Mantener cubierto el sistema con forros plásticos
El disco duro se des configure	B	Realizar mantenimientos preventivos al servidor. Mantener controles para el acceso al servidor (tanto físico como lógico)
Desconfiguración del Setup	B	Mantener las características de setup disponibles para configurarlo de nuevo. Realizar mantenimiento correctivo
Aparición de virus informático	B	Mantener software antivirus actualizado. Mantener software Guardián y vacunar todo tipo de información que penetre al servidor
Sabotaje	M	Creación de políticas de control para el acceso al Centro de Computo y en especial a los servidores y/o equipos de cómputo
Posibilidad de que se queme la main board	B	Mantener regulada la energía eléctrica. En caso de incendio extinguir, en primer lugar, el fuego de la CPU (En la CPU se encuentra toda la información del servidor). Mantener condiciones de temperatura controlada
Posibilidad de que se moje la main Board	B	No debe estar cerca a los ductos de agua. No debe estar cerca a la ventana
La main Board se des configura	B	Realizar mantenimientos preventivos al servidor. Mantener controles para el acceso al servidor (tanto físico como lógico)
Desconfiguración del Setup	B	Mantener las características de setup disponibles para configurarlo de nuevo. Realizar mantenimiento correctivo. Tener una hoja de vida del sistema de hardware

Conexión a red.

Descripción del problema: El dispositivo de comunicaciones no puede responder a los requerimientos de los clientes. Los servicios no pueden ser accedidos, no responden y no se dejan acceder desde consola. Se pierde comunicación con las estaciones de trabajo. Falla en la RED de acceso soportada por la ETB (Canales de datos y ADSL), se pierde el enlace de la Personería de Bogotá D.C., con las Personerías Locales. Tiempo de Tolerancia: 6 horas.

Procedimiento a seguir:

- Se deben definir los procedimientos para que las estaciones trabajen en la modalidad fuera de línea (off line).
- Atender el mantenimiento correctivo con el área de redes y comunicaciones.
- Revisar los procedimientos con que cuente el proveedor.
- Determinación y notificación del daño.
- Registro en la Bitácora de servicios.

Sistema operativo

Descripción del problema: Falla del equipo al intentar arrancarlo y/o al intentar entrar a los aplicativos. Se encuentra imposible inicializar el sistema operacional instalado o sale error o irreparable (PANIC por el kernel o Pantalla Azul).

Tiempo de tolerancia: 6 horas.

Procedimiento a seguir:

- Diagnosticar y encontrar punto de quiebre.
- Notificar al encargado del centro de cómputo para la correspondiente activación de la contingencia, quien identificará el servicio afectado y:
  - ✓ Encenderá el servidor de respaldo correspondiente.
  - ✓ Restaurará la información más reciente mediante procedimiento.
- Reinstalación de sistema y servicio

- ✓ Solicitará al documentador técnico la guía de instalación de servicios y servidores.
- ✓ Solicitará al El ingeniero designado por el Director de Tecnologías de la Información y Comunicación DTIC encargado del soporte de los medios de instalación.
- ✓ Instalará de acuerdo con la guía.
- ✓ Sacará de la copia más actualizada posible para la restauración.
- ✓ Registrará en la bitácora de servicios.

Bases de datos

Descripción del problema: Falla del motor de bases de datos descrito así:

- Un registro de transacciones o de la base de datos que los sistemas de información usan se ha quedado sin espacio en disco.
- La base de datos de los sistemas de información entra en un estado de incoherencia o se daña.
- El servicio de SQL Server u Oracle Databases Enterprise no se está ejecutando o no está configurado correctamente.

Tiempo de tolerancia: 6 horas.

Procedimiento a seguir:

- Comprobar que se esté ejecutando el servicio de database asociado, con las herramientas administrativas.
- Consultar los datos desde las herramientas de desarrollo.
- Diagnosticar y encontrar punto de quiebre.
- Notificar al administrador de las bases de datos para la correspondiente activación de la contingencia, quien identificará el servicio afectado y:
  - ✓ Solicitará el encendido del servidor de respaldo correspondiente.
  - ✓ Restaurará la información más reciente mediante procedimiento.
- Reinstalación del servicio
  - ✓ Solicitará al documentador técnico la guía de instalación de servicios y servidores.
  - ✓ Solicitará al El ingeniero designado por el Director de Tecnologías encargado de Soporte los medios de instalación.

- ✓ Instalará de acuerdo con la guía.
- ✓ Sacará de la cinto teca el backup más actualizado posible para la

8.3.9 Recuperación y Respaldo

Son los procedimientos que se utilizan en las tareas para recobrar la información lo más actualizada posible, con el único propósito de restablecer la normalidad de esta área en la organización.

Establecer con claridad, los procesos a seguir para mantener respaldada la información de la Entidad, clasificada como valiosa o importante.

Determinar, en el menor tiempo posible, cuál, dónde, cómo y qué información se debe recuperar en cada contingencia de acuerdo con el nivel de riesgo.

Determinación de la importancia, periodicidad y/o rotación de los archivos y dispositivos de almacenamiento temporal.

Determinación de dispositivos de respaldo adecuados para su almacenamiento temporal.

Determinación del lugar y el establecimiento de convenios con Entidades especializadas en almacenamiento externo.

Determinación del lugar y el establecimiento de convenios con Entidades especializadas en prestar el servicio de respaldo de equipos de cómputo.

Secuencia de eventos de recuperación

- Clasificar cada una de las secuencias dadas en eventos no deseables, con el fin de lograr la normalidad de las actividades en un tiempo adecuado.
- Determinar el proceso de recuperación y reinicio de operaciones.
- Establecer las pautas que garanticen la eliminación de errores e inconsistencias en el instante de la restauración de copias de seguridad.

Estatus para la recuperación

- Establecer los elementos para la copia de respaldo de la información, definiendo claramente quién, cómo y cuándo se hace este procedimiento. Además, teniendo en cuenta aspectos técnicos como dispositivos, almacenamiento, rotación y seguridad de la información de respaldo.

- Entrar en acción cuando ocurre una contingencia. Para ello se deben determinar la gravedad de la situación, las acciones a ejecutar y la documentación del incidente (dónde, cómo, cuándo, quiénes, así como las acciones tomadas para resolver la contingencia en cuanto al tiempo de solución del percance).

Acciones

- Evaluación preliminar del evento y su impacto.
- Reacción de grupos activos de recuperación de contingencias.
- Informe técnico elaborado de acuerdo con el Plan de Contingencias.

Acción I: Evaluación preliminar del evento y su impacto

- Procedimientos:

  - ✓ Notificación de la eventualidad. Este aspecto implica la oportuna y confiable comunicación de los usuarios con los administradores de los sistemas. Se debe dar a entender al usuario la importancia de reportar las eventualidades y no tratar de solucionar el problema sin estar capacitado. Puede ser contraproducente, en la medida que por acciones equivocadas, puede complicar la situación.
  - ✓ Recopilar la información del evento presentado. Se deben tener en cuenta aspectos como hora de la eventualidad, estado de la aplicación, cifras de control, logs del sistema y registro de otros datos relevantes.
  - ✓ Redactar un informe técnico del estado del problema.

- Tiempo estimado: Lo más rápido posible de acuerdo con la situación presentada. Intervalo de 15 minutos a 6 horas.

- Responsables: El ingeniero designado por el Director de Tecnologías encargado es, equipo de Ingenieros Junior y de soporte de las aplicaciones.

Acción II: Reacción del grupo de continuidad

- Tiempo Estimado: Entre una (1) y seis (6) horas.

- Responsables: El ingeniero designado por el Director de Tecnologías encargado es quien verificara las siguientes acciones:

  - ✓ Ubicación y solicitud de las copias de seguridad, de acuerdo con la última actualización reportada en el informe técnico.
  - ✓ Solicitar a los usuarios abstenerse de utilizar el sistema durante el tiempo que dure la eventualidad.
  - ✓ Realizar el proceso de restauración de los archivos y actualizar la configuración, de ser necesario.
  - ✓ Evaluar la necesidad de actualizar manualmente los registros que, por desfase de tiempo, no hayan quedado en el sistema.
  - ✓ Aplicar los procesos de verificación del sistema de retorno, para la operación correcta de las aplicaciones.
  - ✓ "Dar luz verde" para que los usuarios reinicien sus actividades

Acción III: Informe técnico

- Tiempo de duración: Tres (3) días.

- Responsables: Comité de recuperación, personal capacitado que participe durante la contingencia.

  - ✓ Explicación del estado de la situación actual del sistema.
  - ✓ Áreas afectadas por la eventualidad.
  - ✓ Metodología y aspectos aplicados en la determinación de la evaluación preliminar.
  - ✓ Personal contactado (interno o externo) durante el tiempo de ejecución del plan.

- ✓ Procedimientos aplicados en la recuperación.
- ✓ Estado final y explicación del procedimiento garantizando la fiabilidad de la recuperación.
- ✓ Incluir personal del grupo de contingencias y recuperación que participaron.
- ✓ Tiempo de duración de la eventualidad.
- ✓ Consignación de esta información para futuras fallas.

En general, el Plan de Continuidad saldrá adelante, siempre y cuando cuente la colaboración de todos, respetando y acatando las recomendaciones hechas y los procesos a seguir.

8.4 FASE IV: PLAN DE REVISIÓN PROCEDIMENTAL, PRUEBAS Y MANTENIMIENTO

Para la puesta en marcha y el funcionamiento de los proyectos, es imprescindible la creación de mecanismos de divulgación de los procesos a nivel de la dirección del comité y a cada integrante de los diferentes comités de continuidad y recuperación, verificando que los documentos y procedimientos, objeto de este trabajo, estén completos, cumplan con los estándares y sean los adecuados para el desarrollo del plan.

En este punto podemos suponer que se tiene toda la infraestructura necesaria para la ejecución del plan, pero si no hay preparación de los procedimientos, el equipo directivo y operativo estará abocado a fracasar.

Una vez establecidas responsabilidades y tareas, el documentador técnico es el encargado de facilitar los archivos requeridos y los procedimientos necesarios para la activación del Plan.

Objetivos

- Establecer cuál es el control que se tiene para la guarda y custodia de los procedimientos y documentos requeridos.
- Establecer cuál es la ubicación de estos archivos, con el fin de identificar los pasos a seguir en caso de la aplicación de algunas de las fases del Plan de Continuidad por la presentación de algún incidente

8.4.1 Procedimiento

Nombrar los responsables para la verificación.
Solicitar la documentación.
Revisar cada uno de los documentos relacionados.
Clasificar, regular y reglamentar los contenidos, remitiendo información a la oficina de control interno para su correspondiente proceso.

8.4.2 Plan de Capacitación

Se deben crear mecanismos para la publicación y ejecución del Plan de continuidad y la divulgación de todos los procesos asignados a cada integrante de los comités de recuperación.

En este sentido si no hay preparación del equipo directivo y operativo no sirve de nada el establecimiento del Plan.

Objetivos

- Establecer cuál es el personal que debe conocer los procedimientos, con el fin de capacitarlos sobre cada una de las fases del Plan de continuidad
- Garantizar el pleno cubrimiento de todas las fases de Plan de continuidad por parte de las personas involucradas.
- Establecer responsables de la inducción y re-inducción para la continuidad del plan de capacitación.
- Elaborar por cada fase procedimientos de entrenamiento simulado.
- Generar factores de evaluación que cualifiquen el nivel de entrenamiento.
- Determinar el contenido a tratar para cada líder.
- Dotar de herramientas de capacitación a cada líder.

Procedimiento

- Nombrar y hacer responsable de cada fase a un líder.
- Dotar de elementos para la capacitación y el entrenamiento a cada uno de los líderes involucrados.

- Obtener un esquema general, el cual conduzca a determinar cada una de las actividades a tratar en la capacitación.
- Elaborar por cada fase procedimientos de entrenamiento simulado.
- Generar factores de evaluación que cualifiquen el nivel de entrenamiento.

8.4.3 Manual de procedimientos

Las normas y procedimientos del manual son de obligatorio cumplimiento, siempre y cuando se quiera que todo salga bien; el manual es de carácter confidencial, ya que este documento presenta las debilidades y fortalezas de la Personería de Bogotá D.C.

Es responsabilidad del Director de la Dirección de Tecnologías de la Información y Comunicación DTIC, dar a conocer el contenido del manual al personal que desempeña las funciones relativas a las normas y procedimientos en él descritos.

El contenido de los manuales será permanentemente actualizado por el ingeniero designado por el Director de la Dirección de Tecnologías de la Información y Comunicación encargado de la documentación técnica, que pertenece al comité técnico operativo, mediante el sistema de hojas intercambiables.

8.4.4 Procedimiento operativo y administrativo

Objetivos

- Establecer pautas operativas y administrativas que conduzcan a definir políticas de atención.
- Fortalecer el ámbito cultural del procedimiento de capacitación del Plan de Contingencias.

Procedimientos

- Establecer fechas, tiempo de duración y objetivos del plan de recuperación, al igual que los elementos de evaluación.

- Involucrar directamente a la alta gerencia para que se dote de los recursos necesarios y cada proceso de capacitación.

8.4.4.1 Planes de emergencia

Objetivos

- Proveer de elementos o pautas que normalicen la reacción ante la posibilidad de materialización de eventualidades.
- Fortalecer el personal operativo y directivo con los elementos de decisión propios de la situación de emergencia.

Procedimientos

- Establecer fechas en las cuales se deben realizar simulacros que evidencien la capacidad de reacción en cada caso de emergencia.
- Establecer políticas de evaluación y ajuste del plan.

- Evaluar los procedimientos de respaldo y recuperación, para efectuar los respectivos ajustes.

8.4.5 Plan de Pruebas

El desarrollo de un plan experimental de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o, en caso contrario, se le deben efectuar ajustes para su funcionalidad.

El mayor énfasis será ejercido sobre las pruebas o simulacros, y sobre los eventos posteriores a la emergencia relacionados con el reinicio de las operaciones normales de la Entidad.

En este ejercicios se deben tener en cuenta los siguientes aspectos:

- Validar la habilidad de los funcionarios(as)(as) y la consistencia de los procedimientos en eventos de recuperación de siniestros.

- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar y corregir fallas en el plan.
- Divulgar y retroalimentar el entrenamiento en los procedimientos y guías de recuperación
- Comprometerse con plan y la seguridad para su efectiva aplicación en caso de presentarse emergencias.
- Estar preparado para corregir aspectos de pólizas y seguros y reducir al máximo los costos en compras de nuevos equipos.

La metodología para pruebas, consiste en la realización de simulacros y ensayos en los eventos donde se puede presentar la contingencia, en los cuales se evidencia el grado y prioridad de cada proceso para establecer los ajustes y mejoras a que haya lugar.

Objetivos

- Validar la habilidad de los funcionarios(as)(as) y la consistencia de los procedimientos en eventos de recuperación en caso de desastres.
- Probar la factibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar, supervisar y corregir fallas en el plan.
- Facilitar la divulgación y el entrenamiento en los procedimientos y guías de recuperación.
- Establecer un compromiso con la alta Gerencia de la Entidad para que a través de él, se ejerza la aplicación del plan y se fomente la cultura de la seguridad y prevención en la administración.
- Estar preparado para evaluar las necesidades de seguridad y reducir al máximo los costos en primas de aseguramiento.
- Motivar a los funcionarios(as)(as) involucrados en el diseño y desarrollo del plan a mantener actualizados los procedimientos.

Normas

El Comité Directivo del MIPER, deberá evaluar y fijar las responsabilidades del plan de pruebas, como se sugiere a continuación:

- Personal de Administración: Grado de participación y compromiso, niveles de jerarquía de aprobación, asignación de recursos constantes y temporales.
- Personal de la Dirección de Tecnologías: programación, operación y soporte técnico.
- Grupo de usuarios por área operativa.
- Personal externo: Proveedores, asesores, compañías de mantenimiento y/o garantía, grupos de apoyo internos o externos, centro de recuperación contratados o comprometidos.

Procedimientos

- Como mínimo se debe garantizar que los segmentos de respaldo para instalaciones, datos y documentación, sean probados.
- Una falla en la recuperación en estas tres áreas esenciales puede significar una demora más allá de un período tolerable.
- La Dirección de Tecnología, apoyadas en la oficina de Control interno, identificarán y documentarán los diferentes niveles de prueba del plan. Esos pueden ser: por segmento, por áreas relacionadas o a gran escala.

Pasos para conducir la prueba:

El Comité técnico operativo del plan indicará el esquema de las pruebas teniendo en cuenta:

- Selección del objeto de la prueba, para identificar los aspectos o capítulos del plan que está siendo evaluados.
- Descripción de los objetivos de la prueba y mecanismos de medición del alcance del éxito de los objetivos.
- Reunión con los entes directivos y operativos para explicar la prueba y sus objetivos y obtener como resultado su acuerdo y soporte.
- Comunicación formal de una prueba anunciada, los factores críticos a considerar y el tiempo estimado de la prueba.
- Consolidar los resultados de la prueba al final de esta.
- Evaluación de resultados: progresos, inconvenientes y logros.

- Determinación de las implicaciones de los resultados de la prueba. Se debe analizar si el resultado de un caso simple (segmento), puede tomarse como referencia para la realización satisfactoria de todos los capítulos del plan a gran escala.
- Generación de recomendaciones para cambios o ajustes.
- Definición del tiempo límite para respuesta y gestión.
- Cambios en documentación o manuales, si es aplicable.

Áreas específicas del plan que debe ser aprobados:

La Dirección de Tecnología, conocerán y recomendarán las partes específicas del plan que deben ser probadas, enfatizando en las siguientes:

- Recuperación del sistema operativo en el equipo central y en cada una de las estaciones necesarias en el plan de pruebas, utilizando archivos y documentación almacenada en el sitio externo.
- Habilidad para procesar en modo “Degradado” o limitado. Como consecuencia del estado de disponibilidad de los recursos físicos para su utilización.
- Recarga de los discos del sistema y de los procedimientos de cargue y arranque utilizando archivos y documentación almacenada en el sitio externo.
- En sitios de procesamiento alterno, solución de diferencias en la configuración de equipos.
- Disponibilidad de equipos periféricos de procesamiento
- Disponibilidad de equipos de soporte; aire acondicionado, unidades de potencia no interrumpida de corriente eléctrica.
- Disponibilidad de soporte logístico, provisiones y suministros, transporte y comunicaciones.
- Evacuación del equipo central desde el Centro de Computo Operativo de la Entidad, en respuesta a eventos tales como, incendio, inundación o sabotaje.
- Habilidad de la administración y del Comité Asesor de Sistemas para determinar su prioridad cuando se procesan recursos computacionales limitados.
- Capacidad para recuperar y procesar en forma satisfactoria sin personal clave, asumiendo la pérdida de personal de turnos primarios.
- Destreza para adaptar el plan a desastres menores.

- Efectividad de alternativas manuales para aquellos sistemas que confían en esa opción.
- Habilidad de entrada de datos para alimentar sistemas críticos utilizando las instalaciones del área de soporte externo.
- Habilidad de los usuarios para continuar con las operaciones normales de la Entidad para los sistemas identificados como no críticos.
- Ingenio para establecer contacto, en un período definido por emergencia y de manera organizada, con el personal clave o sus funcionarios(as)(as) alternos.
- Nivel de cumplimiento de los estándares normativos aprobados por la Entidad.
- Identificación de los recursos utilizados durante la emergencia que son cubierto por la póliza de seguros.
- Disponibilidad de formas y cantidad mínima de papelería.
- Adherencia nula, parcial o total a medidas de seguridad durante el período de emergencia.
- Habilidad para ejecutar tareas de evaluación y tratamiento de primeros auxilios.
- Mecanismos para recuperación de información perdida en caso de sistemas en línea.
- Análisis de tiempos y procedimientos durante la prueba

8.4.6 Plan de prevención

Contempla las contramedidas necesarias antes de la materialización de una amenaza. Su finalidad es prevenir los efectos adversos de la posible y probable amenaza.

Su objetivo es mantener operativos los procesos para el correcto funcionamiento de los servicios más críticos en la Personería de Bogotá D.C.

El nivel de este evento es considerado evitable cuando de acuerdo al análisis de riesgo así se considere. Aquí se tiene en cuenta el nivel de criticidad sin asumir su probabilidad; en este caso se aplicará la acción de prevención de acuerdo con las mencionadas “condiciones de prevención de riesgo”.

Cada uno de los protocolos nos guiará a la aplicación de la gestión correspondiente y en ocasiones se requiere de la clave de acceso a las maquinas, en cuyo caso existe un documento base de todas las contraseñas llamado “Información de seguridad”, que se maneja a nivel de protocolo de seguridad informática, y está en poder del Director de Tecnologías.

Condiciones de prevención de riesgo

Tomar las siguientes acciones preventivas que están implementadas por la Dirección de Tecnologías, para adelantar la prevención de riesgos (Contramedidas), con los documentos que se mencionan y se anexan para tal fin.

- Gestión de Protocolos y Guías
- Des-habilitación de los puertos de comunicación y habilitación de los puertos seguros (administración de servidores y servicios)
- Filtrado y control de contenidos
- Contar con equipos de respaldo ante posibles fallas de los equipos de producción, para su reemplazo provisional hasta su desinfección y habilitación.
- Gestión de backups referidos a aplicaciones, configuraciones y datos.
- Contar con garantía, bolsa de repuestos y/o Bolsas de soporte y mantenimiento preventivo con el respectivo protocolo de soporte, para la infraestructura.
- Contar con servicios de soporte vigentes para la infraestructura.
- Gestión de Monitoreo de servidores, servicios y dispositivos de comunicación según protocolo.

Costos de continuidad

RELACIÓN COSTO ELEMENTOS DE CONTINUIDAD DE NEGOCIO			
TIPO DE ELEMENTO	**CANTIDAD**	**CALIDAD**	**COSTO COP$**

Centro de datos alterno (Nube publica) Virtualización de Infraestructura	1	Suscripción anual Microsoft Azure	$ 100.000.000
Servicio Express Route	1	Suscripción anual Microsoft	$ 20.000.000
Servicio Security Acount	1	Suscripción anual Microsoft	$ 10.000.000
Canal de datos- enlace dedicado	1	Suscripción anual proveedor directo del servicio	$ 20.000.000

Contramedidas

- Guía de configuración de los puestos de trabajo: Es primordial tener en claro que dentro del procedimiento de continuidad cada estación de trabajo de proceso crítico tenga comunicación con el nuevo centro de datos alterno o infraestructura tecnología alterna para la continuidad de operaciones.
- Documento “Estado general de la infraestructura: Documento clave para identificar, cuantificar y determinar la configuración de todos los recursos con los que cuenta la Entidad en materia de infraestructura y su estado actual, necesario para: tener claro cómo deberían estar configurados todos los equipos, las redes, las conexiones y sus respectivos servicios, para prevenir el riesgo de Ausencia o inasistencia del personal calificado y para que cualquier persona con conocimientos tecnológicos pueda administrar en caso de requerirse con urgencia.
- Documento “Protocolo de copias de respaldo: Identifica el proceso de copias de respaldo, necesario para asegurar la información de las bases de datos, configuraciones, servicios y aplicaciones, y su aplicación en el plan de ejecución.
- Documento “Manual de políticas de seguridad informática”: En estas políticas se encuentra lo necesario para identificar los diferentes lineamientos de los servicios, seguridad de la información, copias de respaldo, controles de acceso, y su aplicación en el plan de prevención contra ataques y vulnerabilidades.
  Documento “Procedimiento de redes y comunicaciones: Muestra el estado actual de la infraestructura relacionada con las comunicaciones internas y externas y su procedimiento de atención al usuario final, para aplicar la contramedida de prevención de des-configuración y/o daño de las redes.

- "Ficha técnica servidores de respaldo y contingencia": Identifica los servidores con los que se cuenta para la restauración de los procesos más críticos como aplicaciones misionales y críticas, página web, bases de datos, y el estado de la virtualización, lo que permite tener claro que hacer en caso de necesitar activar esta contingencia.
- Informe "Conexión de equipos del centro de cómputo con fuente de poder redundante: Muestra cómo están conectados en el momento los servidores y equipos del centro de cómputo con fuente de poder redundante, necesario para mitigar cualquier caída de la red regulada de este espacio de la Dirección de Tecnologías de la Información y Comunicación DTIC.
- Contratos: Lo siguientes contratos son importantes para asegurar el soporte técnico para evitar daños por operación constante de los equipos y servicios más críticos.
- Convenio ETB
- Mantenimiento preventivo y correctivo de UPS
- Mantenimiento y actualización de Linux
- Garantía de aire acondicionado
- Monitoreo: Con este monitoreo se está revisando constantemente la operación normal de la red, los servidores y las aplicaciones y cuando se muestra un estado de alerta es cuando se aplicaría la contingencia de ejecución. También permite analizar que está operando mal.
- Gestión de Switches "syslog" Herramientas IMC "documento de gestión"
- Gestión de Browser session "TOAD"
- "Bitácora de eventos servicios y equipos-1"
- Allí se registran los incidentes más importantes y permite volver a aplicar la gestión en caso de reincidencia de los problemas presentados o los más comunes y como fueron corregidos.
- Relación de pólizas Dirección Administrativa y Financiera
- Estas pólizas demuestran la protección de bienes informáticos en caso de robo, pérdida o daño.
- Mapa de gestión de riesgos por proceso.
- Este documento demuestra que la Entidad está preparada para cualquier eventualidad crítica en materia de conmoción interna por causa de un siniestro.

9 RECOMENDACIONES

Las Condiciones generales que se deben dar para que el plan de continuidad tenga éxito y el manual sea práctico son:

- Conciencia de los directivos y funcionarios(as) de la Personería de Bogotá D.C., sobre la necesidad del plan.
- Verificación periódica de las copias de respaldo.
- Realizar los simulacros periódicos del plan, en toda la Personería de Bogotá D.C.
- Mantenimiento o actualización de la documentación de las aplicaciones críticas.
- Que los miembros del equipo humano de recuperación o contingencia conozcan sus funciones y responsabilidades.
- Mantenimiento de copias de las copias de respaldo en lugares exteriores a la Entidad.
- Que se haya definido donde mantener o guardar los equipos de soporte.
- Que se tengan suficientes existencias de medios magnéticos, formas continuas, tinta para impresoras y demás suministros.
- Que las hojas de vida de los equipos de soporte se encuentren actualizadas.
- Que el Plan este actualizado.
- Verificación y actualización del plan cada seis meses.
- Que las gestiones dadas en el análisis de riesgos, se hayan tenido en cuenta.
- Que se cuente con todos los equipos requeridos para la contingencia.

10 PUNTOS DE CONTROL

TAREAS	DESCRIPCIÓN DEL RIESGO	ACCIONES DE CONTROL	FRECUENCIA	RESPONSABLE	REGISTRO
Seguimiento a copias de respaldo	Perdida de información por no aplicar los procedimientos establecidos en las políticas de copias de respaldo.	Seguimiento a las políticas y procedimientos de backups	Mensual	Director DTIC, ingenieros responsables de aplicaciones y bases de datos e infraestructura	Actas, informes y seguimiento
Definición y ejecución de pruebas	Traumatismo en la ejecución del plan al no contar con estrategias y equipos de contingencias.	Realizar pruebas simulacros	Anual	Director DTIC, ingenieros de tecnología y líderes de procesos	Actas, informes de seguimiento
Capacitación y comunicación del plan	Deficiencia en la ejecución del plan de comunicación por falta de seguimiento.	Seguimiento al plan de comunicación y capacitación	Anual	Director DTIC, ingenieros responsables de aplicaciones y bases de datos e infraestructura y líderes de procesos	Actas, informes de seguimiento
Seguimiento al mantenimiento y documentación de aplicaciones criticas	Ineficacia en la ejecución del plan por falta de revisión de la documentación	Revisión de la documentación de las aplicaciones	Anual	Director DTIC, ingenieros responsables de aplicaciones y bases de datos e infraestructura	Actas, informes de seguimiento

Seguimiento a los protocolos de alertas	Incumplimiento en los tiempos de la ejecución del plan por falta de seguimiento.	Seguimiento a la aplicación de los protocolos establecidos en el plan de continuidad.	Anual	Director DTIC, ingenieros responsables de aplicaciones y bases de datos e infraestructura y líderes de procesos	Actas, informes de seguimiento
Seguimiento al plan de recuperación	Deficiencia en la valoración del impacto de los incidentes por falta de pruebas a los planes de recuperación.	Pruebas a los planes de recuperación establecidos	Anual	Director DTIC, ingenieros responsables de aplicaciones y bases de datos e infraestructura	Actas, informes de seguimiento