



FUNCIÓN PÚBLICA

Plan de recuperación ante desastres tecnológicos

VERSIÓN 1.1

NOVIEMBRE 2020

Versión	Fecha Versión	Observación
1	03 noviembre del 2020	Primera versión del DRP
1.1	12 de noviembre de 2020	Ajuste del documento para publicación d datos abiertos

Versión de datos abiertos

Contenido

Introducción	6
Objetivo	8
Alcance	8
Glosario	8
Lineamientos de operación	9
Escenarios de desastre tecnológico	10
Niveles de Contingencia	12
Descripción de la infraestructura actual de servicios TIC	12
Centro de datos	12
Sistemas de almacenamiento:	13
Servicios de conectividad y red:	13
Red local:	13
Red local inalámbrica	13
Servidores	14
Telefonía IP	15
Servicios de energía	15
Gestión de desastres	16
Preparación frente a desastres tecnológicos	16
Detección/Identificación de desastres	17
Activación del plan de recuperación ante desastres	17
Criterios para activar el DRP	17
Procedimiento de notificación del DRP	18
Árbol de llamadas	21
Medios de comunicación:	21
Principios de la comunicación	21
Activación de contingencias	22
Vuelta a la normalidad	27
Roles y responsabilidades	28
Equipo de gestión de emergencias tecnológicas	28
Estrategia de pruebas al DRP	35
Alcance de las pruebas al DRP	35
Actividades de notificación, evaluación y activación del DRP.	37
Anexo 1	41

Lista de Tablas

Tabla 1 Escenario de Desastre Tecnológico	10
Tabla 2 Tipos de Contingencia	12
Tabla 3 Responsables plan de contingencia sistema de información SIGEP	23
Tabla 4 Responsables plan de contingencia sistema de información FURAG	25
Tabla 5 Responsables plan de contingencia sistema de información SUIT	27
Tabla 6 Equipo Directivo	29
Tabla 7 Equipo Técnico de Recuperación ante Desastres	30
Tabla 8 Equipo de apoyo	31
Tabla 9 Equipo de Comunicaciones y Prensa	31
Tabla 10 Mesa de ayuda Externa y Interna	32
Tabla 11 Responsabilidad del Equipo Técnico del DRP	33
Tabla 12 Escenarios de Componentes Tecnológicos	36
Tabla 13 Actividades y Responsable	36
Tabla 14 Notificación, evaluación y activación del DRP	38

Lista de Figuras

Figura 1 Modelo Servidores.....	14
Figura 2 Fases para la activación del DRP.....	18
Figura 3 Procedimiento de notificación del DRP	19
Figura 4 Árbol de comunicaciones del PRD	21
Figura 5 Árbol de comunicaciones del plan de contingencia SIGEP	23
Figura 6 Árbol de comunicaciones del plan de contingencia SIGEP	25
Figura 7Árbol de comunicaciones del plan de contingencia SUIT.....	26

Versión de datos abiertos

Divulgación de la versión de datos abiertos del plan de recuperación ante desastres

Departamento Administrativo de la Función Pública.

El Departamento administrativo de la función Pública, en cumplimiento de los requisitos de la ley 1712 de 2014, "Transparencia y acceso a la información pública", Artículo 21. Divulgación parcial y otras reglas. Realiza la publicación de la versión de datos abiertos de su plan de recuperación ante desastres teniendo en cuenta que de acuerdo con el artículo 18 de la citada ley "Información exceptuada por daño de derechos a personas naturales o jurídicas", el acceso a la totalidad de la información contenida en el documento original puede causar un daño a las condiciones de seguridad de la información de la infraestructura tecnológica de la Entidad.

Introducción

Hoy en día la información es uno de los activos más importantes de cualquier organización, independientemente de que esta sea de naturaleza pública o privada, esto radica en el valor mismo de la información, puesto que es la herramienta fundamental para el desarrollo de los procesos que se adelantan al interior de las organizaciones y a que permite garantizar el funcionamiento, la continuidad y seguridad del negocio. Para la protección de la información se deben generar un sin número de medidas que permitan mitigar a niveles aceptables los riesgos y de esta forma prevenir alteraciones en el cumplimiento de los objetivos de la organización.

Actualmente incorporar las Tecnologías de la Información y las Comunicaciones (TIC) a los procesos de gestión de las organizaciones es un elemento clave para el cumplimiento de la eficiencia. Es decir, con un uso adecuado de las TIC las entidades públicas pueden optimizar sus servicios, permitiendo al mismo tiempo alcanzar las metas propuestas. Sin embargo, al hacer uso de estas tecnologías de la información, emergen amenazas que implican el uso de controles orientados a garantizar la prestación de servicios de manera oportuna y segura.

Los planes de contingencia se convierten en un aliado muy importante para las organizaciones, en los casos en que se presentan interrupciones en la continuidad del negocio. En la actualidad las entidades están implementando planes de recuperación de desastres (DRP por sus siglas en inglés), que son procesos de restablecimiento de sus servicios tecnológicos que cubren los datos, el hardware y el software crítico, de forma que la organización pueda reactivar operaciones en caso de un desastre natural, un acto terrorista, un error humano o la ocurrencia de eventos que alteren el normal funcionamiento de sus procesos de soporte tecnológico.

Dado que cada vez más, tanto las entidades públicas como privadas necesitan garantizar la continuidad en la prestación de sus servicios, se presenta la necesidad de diseñar un plan de recuperación ante desastres (DRP) para el Departamento Administrativo de la Función Pública, que permita proteger la información y recuperar su área de tecnología frente ante cualquier eventualidad. El DRP del DAFP estará basado en las mejores prácticas y tecnología de vanguardia con el fin de cubrir las necesidades de la entidad ofreciendo un valor agregado de confianza para el ciudadano, las entidades, servidores y contratistas que hacen uso de los servicios institucionales.

Objetivo

Diseñar el plan de recuperación ante desastres tecnológicos (DRP) del Departamento Administrativo de la Función Pública, en caso de la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente.

Responsable:

Líder: jefe de la Oficina de Tecnologías de la Información

Equipo de respuesta Oficina TIC

Alcance

Este documento cubre el desarrollo de las estrategias en la recuperación y continuidad de los sistemas de información contra posibles desastres de diversa naturaleza que afecten los procesos misionales de la entidad tanto externos como internos y así estar preparados para cualquier eventualidad y en el menor tiempo posible restablecer los servicios y disminuir la pérdida de los recursos.

Glosario

Activo de información: Se refiere al activo que contiene información o elementos relacionados con el manejo de la información (sistemas, soportes, edificios, personas...) y que se caracteriza por tener valor para la organización o entidad (ISO/IEC 27000).

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

Continuidad del negocio: Capacidad de la organización de continuar entregando productos y servicios a niveles aceptables predefinidos después de que ocurra un evento.

DRP: Sigla en inglés (Disaster Recovery Plan) Plan de Recuperación ante Desastres de Tecnología: Información documentada que define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

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.

Plan de continuidad de negocio: Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación debido una vez presentada / tras la interrupción.

Plan de contingencia: Define los procedimientos y medidas que se deben tomar para que las organizaciones puedan continuar operando en caso de una situación de desastre o emergencia.

Plataforma tecnológica crítica: Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son esenciales para soportar los procesos y servicios de la entidad.

RAS: Sigla en inglés (Response Alternative and Solutions): documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

RTO: Sigla en inglés (Recovery Time Objective): tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

RPO: Sigla en inglés (Recovery Point Objective): cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio cuando se presenta un evento alterador del normal funcionamiento.

Lineamientos de operación

El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos institucionales de direccionamiento, misionales y de apoyo.

La efectividad en el restablecimiento oportuno de los servicios tecnológicos institucionales se basa en los siguientes lineamientos:

- ✓ Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos.
- ✓ Los servidores y contratistas que ejecutan este plan, o sus suplentes, se encuentran disponibles y no ha sido afectados por el desastre.
- ✓ Solo el responsable del plan activará el DRP, para este caso, el jefe de la Oficina de las Tecnologías de Información y Comunicaciones.
- ✓ Se contará con un sitios alternos y operativos dispuestos para la recuperación de las operaciones, procesos y procesamiento de la información.
- ✓ Las entidades y organizaciones externas cooperarán en la recuperación de la entidad y estarán disponibles en cualquier momento de la recuperación.
- ✓ El suministro del servicio de energía eléctrica es normal en los sitios alternos.

- ✓ Se han realizado las pruebas de las estrategias y procedimientos al menos una vez al año y han funcionado.
- ✓ Los servidores y contratistas con responsabilidades asignadas en este plan han participado en las pruebas y capacitaciones realizadas.
- ✓ La realización de copias de respaldo de las bases de datos, información y sistemas de información se realiza de acuerdo con la política institucional de copias de respaldo.

Escenarios de desastre tecnológico

Existen muchas clases de desastres tecnológicos que pueden ocurrir dentro de la entidad a continuación se explica los escenarios más frecuentes su causa y su solución.

Tabla 1 Escenario de Desastre Tecnológico

ESCENARIO	CAUSAS POTENCIALES	SOLUCIONES OPERATIVAS
Ausencia del personal responsable del proceso	Pandemia Periodo de vacaciones no planificado Retiro inesperado Fallecimiento Enfermedad crónica Intoxicación	Definición de árboles de llamada Capacitación al personal de respaldo Tener documentados los procesos y procedimientos institucionales
No disponibilidad de los servicios tecnológicos	Falla Eléctrica Incendio Inundación Desastres naturales Fallas tecnológicas en: comunicaciones, hardware, software, bases de datos.	Estrategia DRP
Indisponibilidad de la información	Falla de la infraestructura de los servicios esenciales. Fallas tecnológicas en: Comunicaciones, hardware, software, bases de datos Robo o secuestro de datos Ciberterrorismo Error humano.	Respaldo de la información clave del proceso (Backup) Contar con proveedores de servicios alternos. Almacenamiento en la nube

ESCENARIO	CAUSAS POTENCIALES	SOLUCIONES OPERATIVAS
Problemas de los servicios esenciales	Incendio Terrorismo Fuga de gas Explosión Desastres naturales.	Teletrabajo o home office Contar con canales alternos de comunicaciones, en especial para los procesos administrativos.
Pérdida total o parcial de servicios TIC	Fallas en equipos esenciales: • Switch core • Fibras ópticas de conexión con centros de cableado • Router core • Switches de piso • Enlaces de comunicación con ISP • Firewall	Estrategia DRP
Pérdida total o parcial de información por fallas en infraestructura de bases de datos, almacenamiento y respaldo	• Corrupción de la base de datos • Borrado o pérdida de datos • Falla total o parcial de sistema de almacenamiento • Falla total o parcial del servidor de respaldo.	Respaldo de la información clave del proceso (Backup) Estrategia DRP
Pérdida total o parcial de servicios informáticos por fallas en los servidores	• Falla total o parcial del servidor de respaldo. • Violaciones de seguridad • Falta de actualización	SIGEP: Se activa en plan de contingencia establecido por la Entidad en el documento denominado "DOCUMENTO PLAN DE CONTINGENCIA PARA SISTEMA SIGEP". FURAG: Se activa en plan de contingencia establecido por la Entidad en el documento denominado "DOCUMENTO PLAN DE CONTINGENCIA PARA SISTEMA FURAG". -SUIT: Se activa en plan de contingencia establecido por la Entidad en el documento denominado "DOCUMENTO PLAN DE CONTINGENCIA PARA SISTEMA SUIT".

Niveles de Contingencia

Cada escenario de contingencia tiene una respuesta específica que determina los responsables de las diferentes componentes o sistemas de información. A continuación, se describen de manera general los tipos de contingencia que se cubrirán con el plan de recuperación ante desastres:

Tabla 2 Tipos de Contingencia

Estados de Alerta	Definición
Menor	Generada por eventos que afectan a uno o varias áreas por un tiempo superable al tiempo de caída a 2 horas
Mayor	Provocada por incidentes que afectan el acceso a los sistemas de información, interrumpiendo la operación normal de la entidad por un periodo mayor a 24 horas continuas.
Catastrófica	Interrupción total al máximo tolerable afectando los procesos misionales y actividades de la entidad por más de 24 horas.

Fuente: Elaboración propia

Es importante precisar, que cuando se presente una contingencia mayor o catastrófica, el jefe de la oficina de tecnologías de la información y comunicaciones es el responsable de recomendar al grupo de gestión de emergencias institucional la activación de manera inmediata el plan de recuperación ante desastres. Ver documento técnico de continuidad de negocio institucional.

Descripción de la infraestructura actual de servicios TIC

A continuación, se realiza una descripción de la infraestructura actual que soporta los sistemas de información del Departamento Administrativo de la Función Pública:

Centro de datos

Centro de datos de procesamiento propio. Donde se encuentra alojado la infraestructura el almacenamiento, las plataformas de procesamiento, el respaldo que soportan los ambientes de producción desarrollo y pruebas de disponibilidad del negocio. Cumple con las recomendaciones estándares y un correcto flujo de aire

acondicionado con control interno y extractor para garantizar la disminución de energía en los sistemas de aire y la extracción de calor de estos puntos críticos. Este centro de datos es administrado por los ingenieros de la OTIC.

Cuenta con políticas de administración, mantenimiento, soporte y acceso físico restringido mediante el instructivo de centro de datos, sus equipos servidores y controladores se encuentran conectados a una subestación de 400KVA y una UPS.

Su ubicación es en el quinto (5) piso en las Instalaciones de Función Pública y es administrado por los ingenieros de la OTIC.

En el centro de datos reposa los servidores que funcionan bajo el Sistemas Operativos Windows Server 2000, 2008, 2012, 2016 2019 y Linux. Se cuenta con 17 servidores físicos y 16 Servidores Virtuales Hiper V.

Sistemas de almacenamiento:

Se cuenta con una NAS que es un sistema de almacenamiento en red con capacidad para soportar 132 discos, actualmente están 119 discos instalados

Servicios de conectividad y red:

La red actual de Función Pública consta de un canal de Internet de 128 Mbps y canal de datos entre sedes del DAFP y el colocation de 64 MB. Los servicios son provistos por IFX

Red local:

Corresponde a una red de topología Ethernet de área local que presta servicios de conectividad a la plataforma de servidores, estaciones de trabajo y servicios de impresión.

El backbone de la red de área local, está compuesto por un doble enlace de fibra óptica que conecta a los switches de acceso de las diferentes áreas funcionales con los switches Core ubicados en el data center principal.

La plataforma de servidores está conectada a la red de área local a través de enlaces redundantes de cobre a una velocidad de 10 Gb/s, directamente a una VLAN exclusiva de los servidores en los switches Core localizados en el Data Center principal.

Las estaciones de trabajo y los servicios de impresión usan conexiones de cobre a una velocidad de 1 Gb/s y a 100 Mb/s.

Red local inalámbrica

La red wifi presta servicios de acceso a los dispositivos inalámbricos, tales como teléfonos inteligentes, tabletas y computadores portátiles.

La arquitectura de esta red está basada en controladores redundantes que proveen servicio de conectividad a los diferentes puntos de accesos ubicados estratégicamente en las diferentes dependencias.

Esta red esta segmentada en dos subredes que separan el tráfico y mejoran la seguridad y la protección de la información. Estas subredes son: La red Hermes, sólo

para personas de cierto nivel dentro de la organización, la red de funcionarios, donde se conectan la mayor cantidad de dispositivos con acceso a las diferentes aplicaciones corporativas y finalmente la red de invitados (guest) que sólo permite el acceso a Internet.

Esta red cuenta con esquemas de seguridad muy robustos que evitan las conexiones no permitidas de terceros o de posibles intrusos.

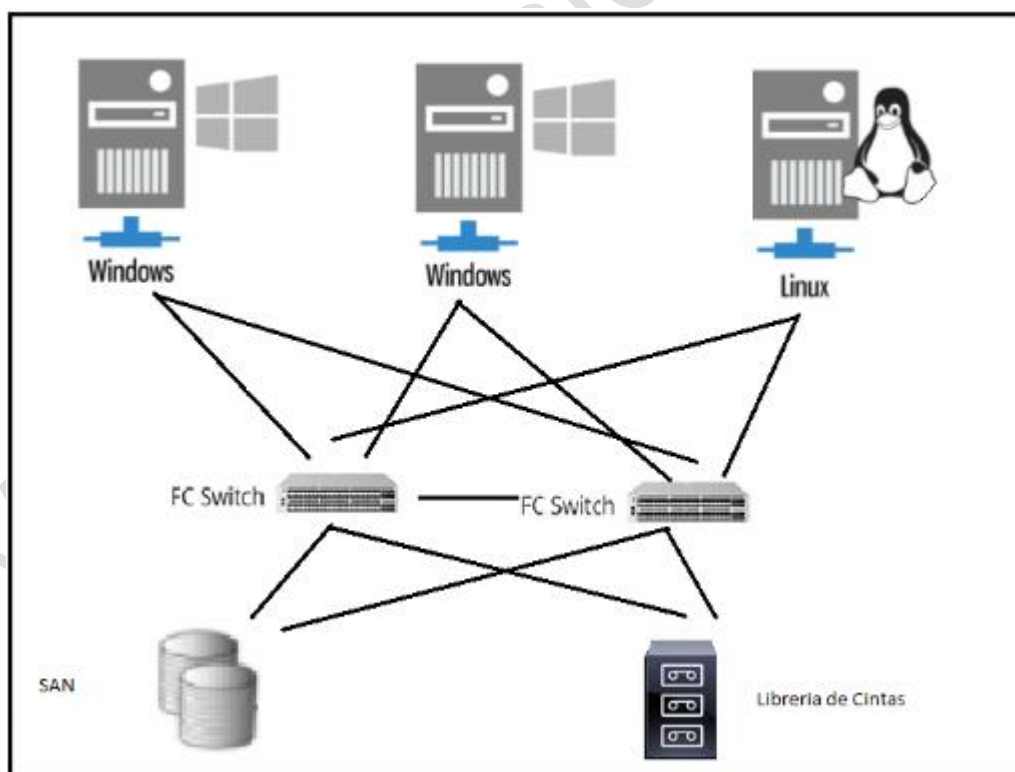
Servidores

La plataforma de Servidores funciona bajo los Sistemas Operativos Windows Server 2000, 2008, 2012, 2016 2019 y Linux. cuenta con 17 servidores físicos y 16 Servidores Virtuales Hiper V. Se encuentra ubicada en el centro de datos del quinto piso del Departamento Administrativo de la Función Pública única sede, administrado por los ingenieros de la OTIC.

La protección de la infraestructura del centro de datos existe una solución de seguridad perimetral, con el objetivo de garantizar la confiabilidad e integridad de la información.

El esquema de seguridad provee los servicios de IPS, antispyware, y balanceador de carga.

Figura 1 Modelo Servidores.



Fuente Departamento Administrativo de la Función Pública 2020

Telefonía IP

El Departamento Administrativo de la Función Pública cuenta con una solución de telefonía IP de su propiedad soportada en un servidor en alta disponibilidad Asterisk

Tiene un canal de 60 líneas funcionando con teléfonos Yealink y las extensiones son SIP

Servicios de energía

Actualmente Función Pública no cuenta con planta eléctrica.

Sistemas de baterías y UPS:

UPS APC modelo Symmetra PX 80kW con Serial PD0804160048 y configurada a 80KVA, con servicio de mantenimiento preventivo y correctivo.

Características de salida La UPS cuenta con las siguientes características de salida:

- ✓ Capacidad de potencia de salida 80kw / 80kva.
- ✓ Máxima potencia configurable 80kw / 80 kva.
- ✓ Tensión de salida nominal 120V,208V,208V3PH.
- ✓ Distorsión de tensión de salida menor al 3%.
- ✓ Frecuencia de salida (sincronizada a 57 - 63 HZ para 60 Hz nominal red eléctrica principal).
- ✓ Factor de cresta ilimitado.
- ✓ Topología Doble conversión en línea.
- ✓ Tipo de forma de onda de seno.
- ✓ Conexiones de salida (1) Hard Wire 5-wire (3PH + N + G) (1) Bornes de Tornillo.
- ✓ Derivación built-in bypass estático.

Características de entrada La UPS cuenta con las siguientes características de entrada:

- ✓ Entrada de voltaje 208V 3PH
- ✓ Frecuencia de entrada 50/60 Hz +/- 5 Hz (detección automática)
- ✓ Conexiones de Entrada Alambre duro de 5 hilos (3PH + N + G)
- ✓ Rango de tensión de entrada para operaciones principales 177 – 240
- ✓ Máxima Resistencia de cortocircuito (Icw) 30 kA.

Características de las baterías

- ✓ Tipo de batería: sólo batería exterior
- ✓ Vida útil de las baterías: 3-5 años
- ✓ Baterías reemplazables en caliente SI
- ✓ 4. Batería de 12V 7,2 Ah, marca CBS, libre de mantenimiento para módulo SYBT4 de UPS marca APC modelo Symmetra PX de 80KVA/80KW
- ✓ Las baterías se encuentran provistas en sus respectivos módulos SYBT4.
- ✓ Dimensiones: Altura total hasta el borde de la pestaña terminal 98,6 mm, altura batería 94,3mm, largo batería 151,0mm, ancho superior 64,8mm, ancho de la base 64,0mm, distancia entre punto medio de terminales 45.0mm, peso 2,4Kg, resistencia interna 23mΩ.

Características ambientales:

- ✓ Ambiente operativo 0 - 40 °C
- ✓ Humedad relativa de operación 0 - 95%
- ✓ Altitud de funcionamiento 0-3000 metros
- ✓ Temperatura de almacenamiento -15 - 40 °C
- ✓ Humedad relativa de almacenamiento 0 - 95%
- ✓ Elevación de almacenamiento 0-15000 metros
- ✓ Ruido audible a 1 metro de la superficie de la unidad 7 1.00 dBA
- ✓ Disipación térmica en línea 22744.00 BTU/hr
- ✓ Clase de protección NEMA 1.

Gestión de desastres

Preparación frente a desastres tecnológicos

Consiste en planificar y organizar las acciones, así como establecer la estrategia para hacer frente a posibles situaciones de emergencia y desastres. Para el caso del Departamento Administrativo de la Función Pública se debe considerar los siguientes preparativos:

- Generar reportes sobre eventos o emergencias que se hayan presentado en la Entidad con su respectivo análisis de riesgos.
- Establecer planes de ayuda conjunta a nivel nacional, regional, local e institucional.
- Realizar capacitaciones a todos los funcionarios y contratistas.

En el denominado Escenario 3: Desastre tecnológico del documento técnico de continuidad de negocio institucional se identifican las alertas de los sistemas de información, servicios informáticos y la infraestructura de servicio y los servicios que se deben monitorear constantemente son:

Subsistemas de telecomunicaciones

- Router de acceso a Internet
- Canal de acceso a servicios de Internet
- Switches de Core y switches de piso
- Equipos de seguridad perimetral como firewall y concentrador de VPN

Servicios de mensajería electrónica y sistema colaborativo Office 365

Servidores virtuales y físicos que soportan sistemas de información institucionales

- Sitio web institucional
- Intranet institucional
- Sistema de gestión documental Orfeo
- Sistema de almacenamiento compartido de archivos Orfeo
- Sistema de información SIGEP
- Sistema de información SUIIT
- Sistema de información FURAG

- Sistema CRM
- Sistema de información estratégica SIE
- Sistema Integrado de Planeación y Gestión
- Sistema de gestión institucional
- Sistema de gestión de mesa de ayuda Proactiva Net
- Canales virtuales de comunicación EVA
- Portales de divulgación de información: sirvo a mi país, banco de éxitos, banco de gerentes, reporte de conflicto de interés, declaración de bienes y rentas, gestor normativo, rendición de cuentas.

Sistemas de almacenamiento masivo SAN

Sistema de virtualización de servidores

Subsistemas de aire acondicionado

Sistema de energía eléctrica, sistema de UPS, bancos de baterías

Detección/Identificación de desastres

De igual manera, una adecuada detección e identificación frente a desastres tecnológicos debe mínimo contemplar lo siguiente:

- ✓ Identificar las áreas de alto riesgo en la Entidad.
- ✓ Determinar la situación actual para la respectiva planificación en lo que y coordinación para emergencias tecnológicas
- ✓ Identificar los roles y definir sus responsabilidades.
- ✓ Determinar cuál es la capacidad de reacción de los equipos de respuesta existentes en cada área.
- ✓ Definir estrategias de emergencias ante una eventualidad.
- ✓ Establecer los mecanismos de alerta y alarma, así como los canales de comunicación a utilizar, lo anterior con el fin de comunicar a toda la entidad se debe realizar en caso de un evento.
- ✓ Fortalecer la coordinación interinstitucional para la respuesta ante desastres tecnológicos.

Activación del plan de recuperación ante desastres

Criterios para activar el DRP

Como parte de las estrategias inmediatas ante una posible crisis, se contemplan las tareas que deben efectuarse lo más rápido posible, después de que se presente el incidente, para reducir posibles impactos.

A continuación, se enumeran las fases que se deben considerar para la activación del DRP:

Figura 2 Fases para la activación del DRP



Fuente: Elaboración propia

Así mismo se listan algunas actividades anexas a las fases definidas anteriormente:

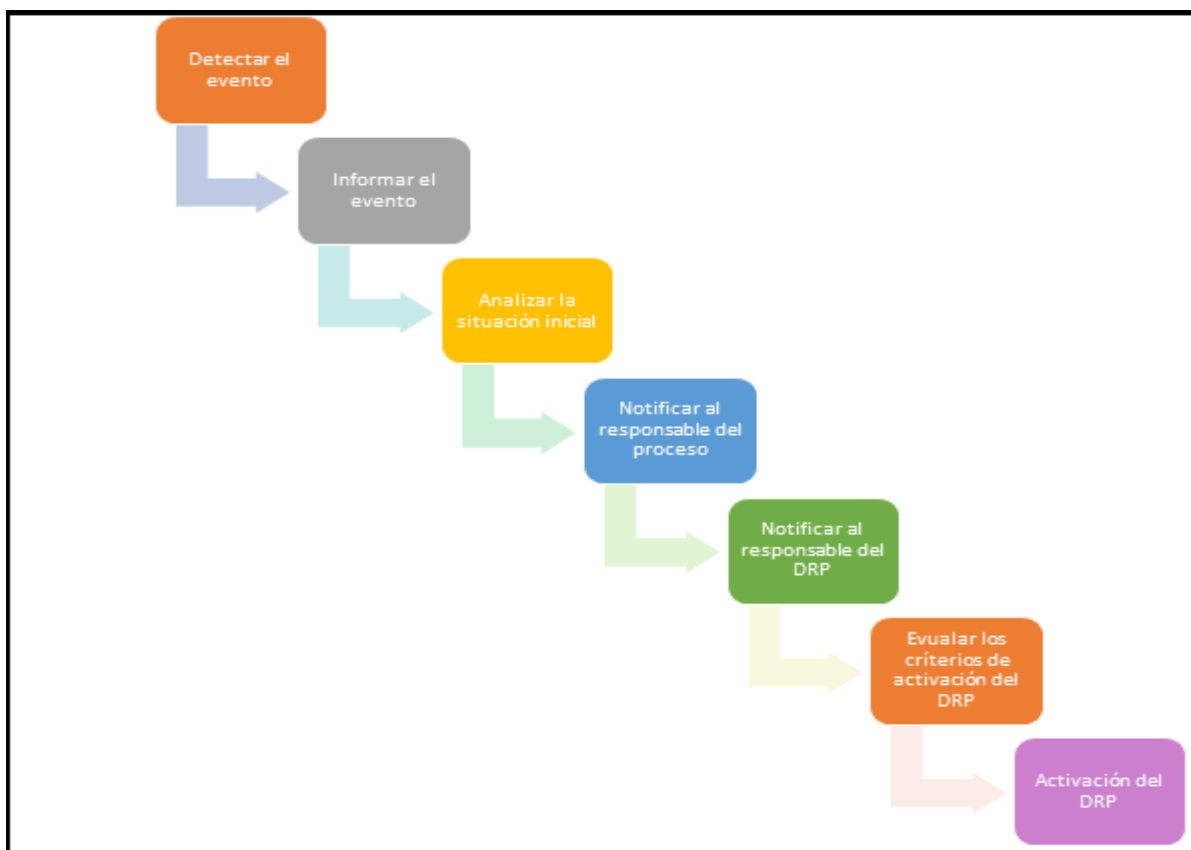
1. Registro de Incidentes
2. Evaluación inicial del alcance del incidente y fallos
3. Validar la criticidad de la falla (Contingencia menor, mayor o catastrófica)
4. Comunicar al equipo de gestión de emergencias institucional (Dirección, Subdirección, Secretaría general, Oficina de tecnologías de información y comunicaciones, Oficina asesora de comunicaciones)
5. Activar Alertas definidas en el plan de evacuación de emergencias si es necesario
6. Activar el plan de evacuación y emergencias
7. Activación del plan de recuperación de desastres
8. Ejecución procedimientos de contingencia por dependencias
9. Notificar el inicio de las actividades de contingencia
10. Monitoreo y seguimiento en el periodo de contingencia
11. Comunicación continua interna/externa a los grupos de valor
12. Activación de plan de retorno de contingencia
14. Regreso a modo normal de operación
15. Notificación formal de fin de contingencia
16. Actualización del plan de recuperación de desastres
17. Documentación de lecciones aprendidas
18. Actualización de planes de prueba
19. Fin de la ejecución de las acciones de contingencia

Procedimiento de notificación del DRP

Cuando se presenta una emergencia, se debe tener en cuenta que se debe gestionar la notificación de esta con el fin de iniciar con el proceso de activación del Plan de

Recuperación de Desastres (DRP). Teniendo en cuenta lo anterior, el procedimiento para gestionar la notificación es el siguiente:

Figura 3 Procedimiento de notificación del DRP



Fuente: Elaboración propia.

La notificación de la indisponibilidad de los sistemas de información se puede generar por diferentes causas, dependiendo de la naturaleza del evento, del momento en el cual ocurra y de la posible causa. Es importante tener en cuenta que el procedimiento de notificación y activación debe estar ligado a los procedimientos a todos procedimientos establecidos en el Departamento Administrativo de la Función Pública.

Se debe asegurar la comunicación permanente con los directivos del Departamento Administrativo de la Función Pública en cada momento (antes, durante y después) por la naturaleza de las decisiones que se deban tomar cuando se presente una emergencia.

Reconocimiento del evento e informar

La identificación o reconocimiento del evento ocurre cuando se ha presentado un incidente y es evidente que causará una interrupción en los sistemas tecnológicos o sistemas de información del Departamento Administrativo de la Función Pública.

Es el punto en el tiempo en que la implementación de las respuestas y acciones de recuperación, incluyendo la notificación y la activación del DRP son inminentes

Analizar la situación inicial

La evaluación de daños es la actividad inicial que debe efectuarse inmediatamente después de un incidente. Esta actividad es realizada por el responsable del DRP, quien tiene la responsabilidad de investigar y evaluar el incidente, así como comunicarse con otras áreas de soporte, para llevar a cabo una evaluación inicial y una valoración de daños.

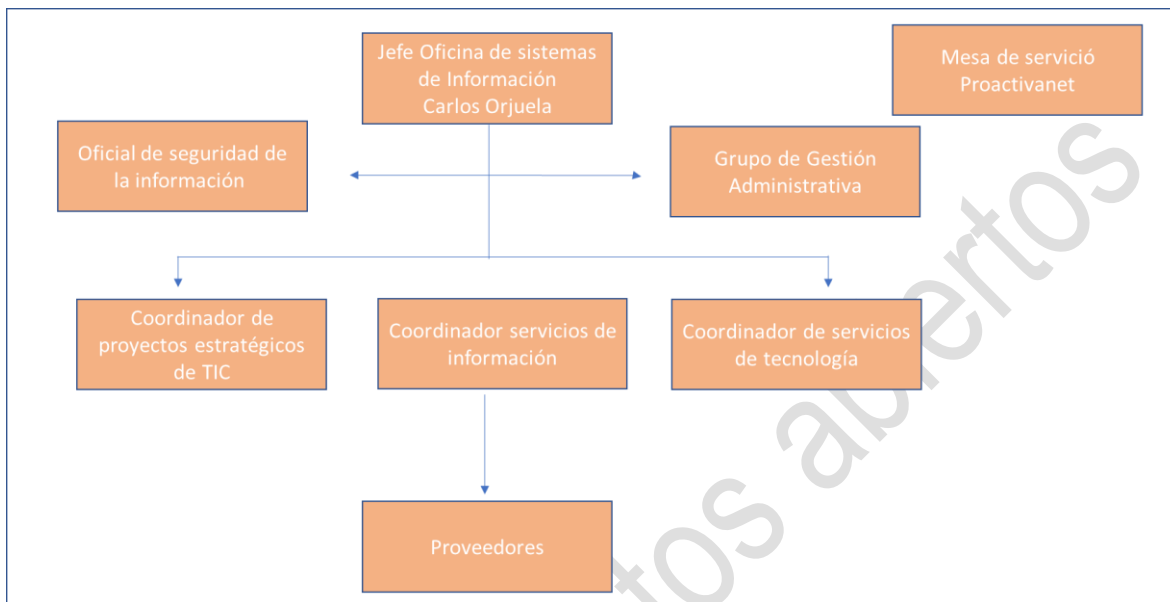
Dependiendo de la magnitud del desastre, el responsable del DRP podrá recurrir a proveedores o grupos involucrados a efecto de elaborar el documento de evaluación del desastre, por lo que deberán hacer lo siguiente:

- a. Poner en estado de alerta los procesos críticos que impactan a la Entidad.
- b. Obtener información pertinente con respecto al incidente.
- c. Descripción del incidente
- d. Daño estimado
- e. Informar a las áreas afectadas

Árbol de llamadas

Cuando se presente un desastre, interrupción o evento, se debe seguir el siguiente esquema de llamadas:

Figura 4 Árbol de comunicaciones del PRD



Fuente: Elaboración propia

Medios de comunicación:

- **Personalmente:** Este medio permite ser más explícito y detallar lo sucedido con el evento. La comunicación depende de factores socio ambientales y/o factores de riesgo (catástrofes) que afecten este tipo de comunicación.
- **Vía telefónica:** La comunicación telefónica es un medio facilitador para acortar distancias y tener una conversación interpersonal. Con él se puede al igual que en la comunicación persona a persona ser más explícito y tomar alguna decisión dentro de la comunicación cuando ocurra una emergencia.
- **Vía correo electrónico:** El correo electrónico se ha establecido como un medio efectivo para comunicarse a cualquier distancia y en el menor tiempo.
- **Grupos de mensajería instantánea:** La mensajería instantánea como un tipo de correo permite interactuar más rápida y efectivamente entre una o varias personas.

Principios de la comunicación

La comunicación de la emergencia deberá considerar los siguientes principios:

1. **Informar de manera oportuna y periódica:** Ante una situación de emergencia de alto impacto, la entidad debe establecerse como fuente primaria de

información y comunicar la evolución de la intención del incidente. Estos elementos le permitirán generar confianza y credibilidad con los funcionarios, contratistas y demás actores de la Entidad.

2. **Emitir reportes lo más exactos posible:** Una vez validada la información, debe ser publicada siguiendo el protocolo definido por el equipo de gestión de emergencias institucional (Dirección, Subdirección, Secretaría general, Oficina TIC, Oficina asesora de planeación) y tener disponible para evitar suposiciones o especular.
3. **Hablar con la verdad:** Transmitir la información que sea necesaria para generar confianza y tranquilidad al interior de la entidad. No obstante, puede existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a las partes interesadas.

Activación de contingencias

En esta etapa se relaciona los procedimientos de recuperación de cada sistema de información:

SIGEP Sistema de Información y Gestión del Empleo Público

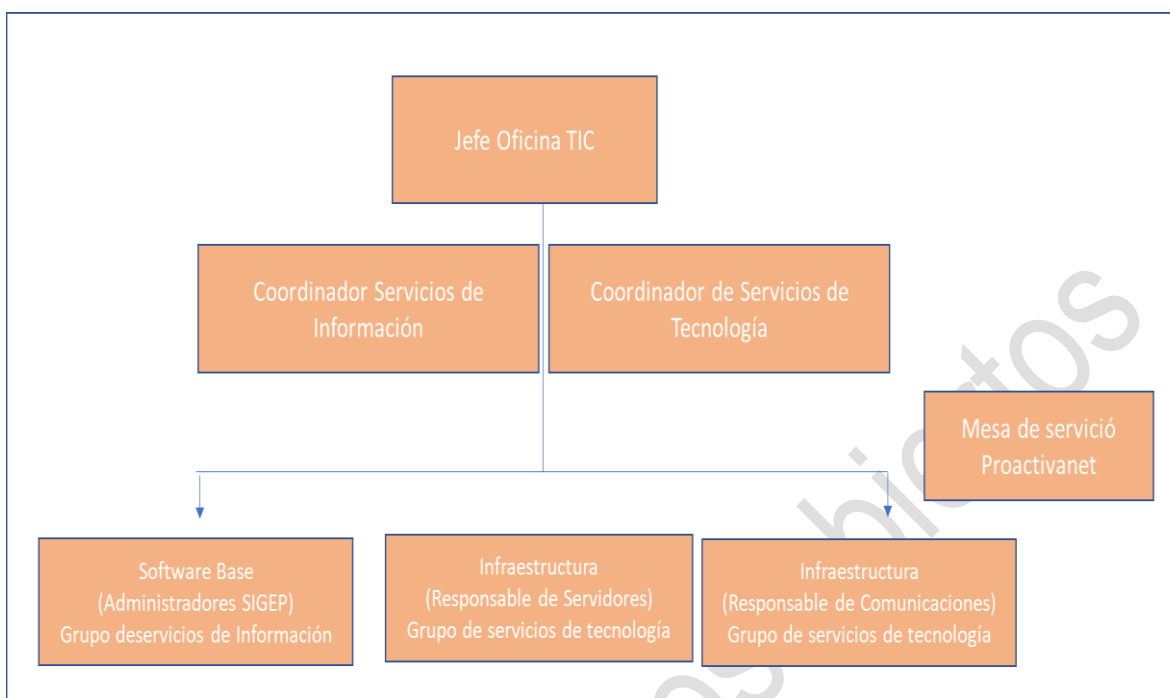
Descripción de la activación de este plan

El plan de contingencia se activa a partir de una falla de la base de datos y del servidor de aplicaciones del ambiente de producción del sistema de información SIGEP.

El primer paso después de la activación del Plan de contingencia es la notificación a los usuarios afectados:

- ✓ Clientes internos: Dirección de empleo público, Grupo de gestión humana, Oficina de comunicaciones, Grupo del servicio al ciudadano - SIGEP.
- ✓ Clientes externos: Entidades públicas, con sus servidores públicos y contratistas.
- ✓ Publicación de banner de notificación de indisponibilidad del sistema de información, esto toma un tiempo aproximado de dos horas, esta actividad se desarrolla en paralelo a las actividades descritas en el Documento *El Plan de Contingencia para Sistema SIGEP*

Figura 5 Árbol de comunicaciones del plan de contingencia SIGEP



Fuente Documento plan de contingencia para sistema SIGEP

Para asegurar la acertada implementación y gestión de la continuidad del servicio tecnológico se deben establecer roles y responsabilidades que involucren las áreas de gestión en el departamento de Tecnologías de la información que se muestra a continuación en la siguiente tabla.

Tabla 3 responsables plan de contingencia sistema de información SIGEP

Rol	Ubicación	Teléfono-ext.	Responsable	Celular
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508 504	Edwin Vargas Evelio Lopez	información no disponible en la versión de datos abiertos de este documento
Administradores de redes y Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Leonardo Calderón	información no disponible en la versión de datos abiertos de este documento
Administrador SIGEP	Departamento Administrativo de la Función Pública – Piso 5	505 200 517 503	Lina Escobar G Francisco Urbina Rafael Rodríguez Oiris Olmos Sosa	información no disponible en la versión de datos abiertos de este documento
Proveedor* Soporte Básico META4	META4		Gerente Soporte y Base Instalada	información no disponible en la versión de datos abiertos de este documento

Rol	Ubicación	Teléfono-ext.	Responsable	Celular
Proveedor* Soporte Extendido- HEINSONH	Departamento Administrativo de la Función Pública – Piso 5 Gerente proyecto HEINSONH	505	Desarrollador en Sitio Olga Tapias	información no disponible en la versión de datos abiertos de este documento
Administrador DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez	información no disponible en la versión de datos abiertos de este documento

Fuente Documento plan de contingencia para sistema SIGEP

El procedimiento completo de la activación y el restablecimiento del servicio, se encuentra en el documento denominado “*Documento Plan de Contingencia para Sistema Sigep*”.

FURAG Formulario Único Reporte de Avances de la Gestión

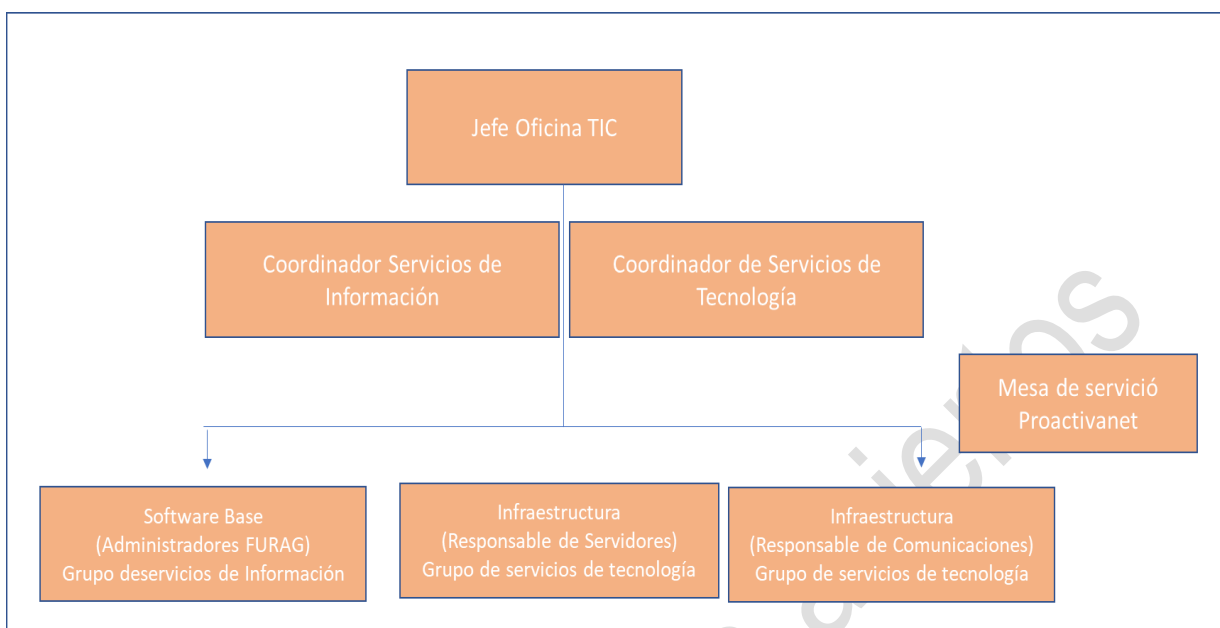
Descripción de la activación de este plan

El plan de contingencia se activa a partir de una falla de la base de datos y del servidor de aplicaciones del ambiente de producción del sistema de información FURAG.

El primer paso después de la activación del Plan de contingencia es la notificación a los usuarios afectados:

- ✓ Clientes internos: Dirección de Gestión y Desempeño Institucional, Oficina de comunicaciones, Grupo del servicio al ciudadano - FURAG.
- ✓ Clientes externos: Entidades públicas, con sus servidores públicos y contratistas.
- ✓ Publicación de banner de notificación de indisponibilidad del sistema de información, esto toma un tiempo aproximado de dos horas, esta actividad se desarrolla en paralelo a las actividades descritas en el Documento Plan de Contingencia para Sistema FURAG

Figura 6 Árbol de comunicaciones del plan de contingencia FURAG



Fuente Documento plan de contingencia para sistema FURAG

Para asegurar la acertada implementación y gestión de la continuidad del servicio tecnológico se deben establecer roles y responsabilidades que involucren las áreas de gestión en el departamento de Tecnologías de la información que se muestra a continuación en la siguiente tabla

Tabla 4 responsables plan de contingencia sistema de información FURAG

Responsable	Ubicación	Teléfono-ext.	Nombre	Celular
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508	Edwin Vargas	información no disponible en la versión de datos abiertos de este documento
		504	Evelio López	
Administradores de Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Leonardo Calderón	información no disponible en la versión de datos abiertos de este documento
Administrador FURAG	Departamento Administrativo de la Función Pública – Piso 2 y 5	207	Víctor Hugo Jáuregui	información no disponible en la versión de datos abiertos de este documento
		503	Oiris Olmos Sosa	
		200	Francisco Urbina	
Ingeniero Desarrollo	Departamento Administrativo de la Función Pública – Piso 2	207	Víctor Hugo Jáuregui	información no disponible en la versión de datos abiertos de este documento
DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez	información no disponible en la versión de datos abiertos de este documento

Fuente Documento plan de contingencia para sistema FURAG

El procedimiento completo de la activación y el restablecimiento del servicio, se encuentra en el documento denominado “Documento Plan de Contingencia para Sistema Furag”.

SUIT SISTEMA ÚNICO DE INFORMACIÓN DE TRAMITES

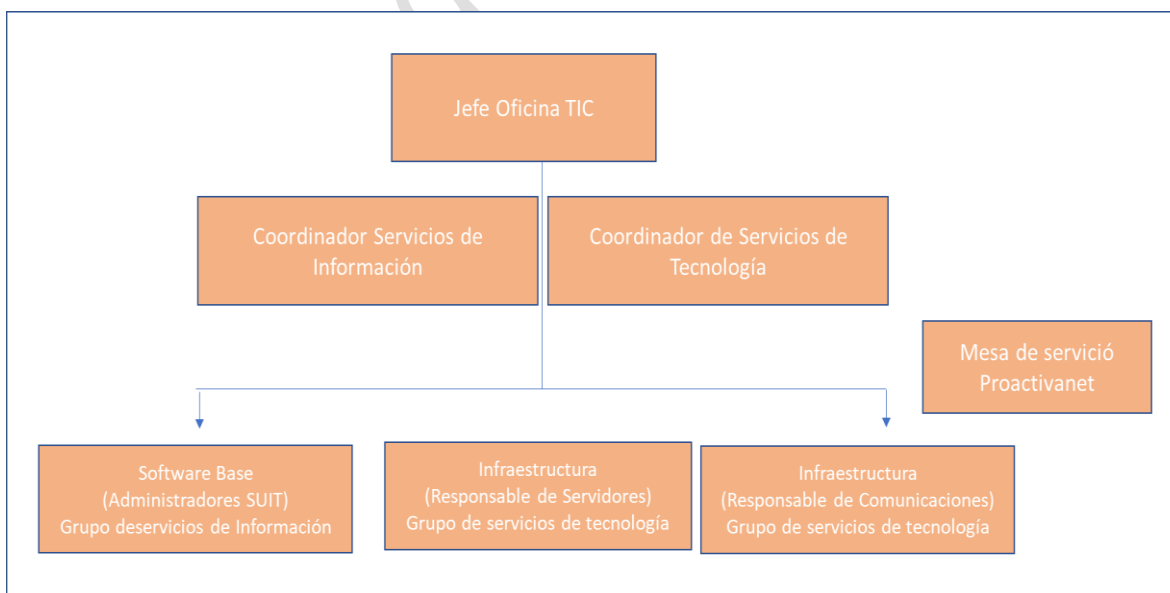
Descripción de la activación de este plan

El plan de contingencia se activa a partir de una falla de la base de datos y del servidor de aplicaciones del ambiente de producción del sistema de información SUIT.

El primer paso después de la activación del Plan de contingencia es la notificación a los usuarios afectados:

- ✓ Clientes internos: Dirección de participación, transparencia y servicio al ciudadano, Oficina de comunicaciones y Grupo del servicio al ciudadano – SUIT.
- ✓ Clientes externos: Entidades públicas.
- ✓ Publicación de banner de notificación de indisponibilidad del sistema de información, esto toma un tiempo aproximado de dos horas, esta actividad se desarrolla en paralelo a las actividades descritas en el Documento *Plan de Contingencia para Sistema SUIT*

Figura 7Árbol de comunicaciones del plan de contingencia SUIT



Fuente Documento plan de contingencia para sistema SUIT

Para asegurar la acertada implementación y gestión de la continuidad del servicio tecnológico se deben establecer roles y responsabilidades que involucren las áreas de gestión en el departamento de Tecnologías de la información que se muestra a continuación en la siguiente tabla.

Tabla 5 responsables plan de contingencia sistema de información SUIT

Rol	Ubicación	Teléfono-ext.	Responsable	Celular
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508 504	Edwin Vargas Evelio Lopez	información no disponible en la versión de datos abiertos de este documento
Administradores de Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Leonardo Calderón	información no disponible en la versión de datos abiertos de este documento
Administrador SUIT	Departamento Administrativo de la Función Pública – Piso 5	201 207 200	Jose Torres Víctor Jauregui Francisco Urbina	información no disponible en la versión de datos abiertos de este documento
Administrador DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez	información no disponible en la versión de datos abiertos de este documento

Fuente Documento plan de contingencia para sistema SUIT

El procedimiento completo de la activación y el restablecimiento del servicio, se encuentra en el documento denominado “DOCUMENTO PLAN DE CONTINGENCIA PARA SISTEMA SUIT “

Vuelta a la normalidad

Para definir la vuelta a la normalidad, se deben considerar los siguientes aspectos:

- ✓ Fecha del retorno a la operación normal.
- ✓ Consideraciones especiales para aplicar en el proceso de vuelta a la normalidad.
- ✓ Consideraciones especiales con respecto a la recuperación de la información y mantener la integridad de los datos, cuando aplique.

- ✓ El jefe de sistemas de Información junto con los coordinadores de la oficina de la OTIC y el Jefe Grupo de Gestión Administrativa, definen el retorno a la normalidad, para ello deben definir los siguientes aspectos:
1. Creación de la incidencia por el aplicativo Proactivanet “lo puede crear cualquier integrante del grupo OTIC”.
 2. Día fecha y hora de la activación de los sistemas de información.
 3. Realización de una valoración donde explique específicamente si hubo daños y afectaciones a los equipos físicos y virtuales. (ver Anexo 1).
 4. Sincronización de: Subsistemas de telecomunicaciones, Servicios de mensajería electrónica, sistema colaborativo Office 365, Servidores virtuales físicos que soportan sistemas de información institucionales y físicos, Sistemas de almacenamiento masivo SAN, Sistema de virtualización de servidores, Subsistemas de aire acondicionado, Sistema de energía eléctrica, sistema de UPS, bancos de baterías.
 5. Los coordinadores de la OTIC, el Jefe Grupo de Gestión Administrativa y el Apoyo de seguridad de la información, documentaran el incidente e identificando las posibles mejoras para un nuevo evento verificando la guía Documento Técnico del Plan de Continuidad del Negocio de Función Pública.
 6. Actualizar la matriz de materialización del riesgo en gestión de incidentes.
 7. Cierre por proactivanet de la incidencia

Roles y responsabilidades

Los roles y responsabilidades definidos en este plan deberán ser ejercidos por el personal seleccionado, de forma tal que se minimice el impacto y se actúe de forma adecuada. Para este caso, se definió un equipo de gestión de emergencias tecnológicas, el cual se describe a continuación:

Equipo de gestión de emergencias tecnológicas

Este equipo tiene como objetivo actuar con gran rapidez cuando ocurre una emergencia grave o un desastre. Tiene como función principal la toma de decisiones en caso de que ocurra un desastre que cause la interrupción en los procesos críticos y los sistemas de información del Departamento Administrativo de la Función Pública.

Entre las funciones principales se definen las siguientes:

- ✓ Analizar la situación para actuar oportunamente cuando ocurra una emergencia o desastre.
- ✓ Tomar la decisión de activar o no el DRP.

- ✓ Iniciar el proceso de notificación a los funcionarios y contratistas por medio de los diferentes responsables y roles definidos.
- ✓ Definir un presupuesto estimado para gastos que genere el desastre o crisis.
- ✓ Realizar el seguimiento del proceso de recuperación ante desastre teniendo en cuenta los tiempos estimados de recuperación.
- ✓ Tomar decisiones ante situaciones o imprevistos durante la recuperación de los procesos críticos y sistemas de información. Comunicar a los diferentes equipos de la organización sobre las decisiones que se tomen en el proceso de recuperación ante desastres.

Para este caso, el equipo de emergencias tecnologías del Departamento Administrativo de la Función Pública está conformado por los siguientes equipos:

- **Equipo Directivo:** Avala la decisión tomada por el equipo técnico para la activación del DRP. De igual manera monitorea la emergencia o evento desde su inicio, su estabilización y retorno a la normalidad.

El equipo gestión de emergencias está integrado por:

Director del Departamento administrativo de la función pública

Subdirectora del Departamento administrativo de la función pública

Secretaria General

Jefe de la Oficina de tecnologías de información y las comunicaciones

Jefe de la Oficina asesora de planeación

Tabla 6 Equipo Directivo

Equipo Directivo			
Nombre	Rol	Celular	teléfono
Fernando Antonio Grillo Rubiano	Director	información no disponible en la versión de datos abiertos de este documento	(1)739 5656 Ext.901
Claudia Patricia Hernández León	Subdirectora	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.911
Juliana Valencia Andrade	Secretaria General	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.801
Hugo Armando Pérez Ballesteros	Director de Desarrollo Organizacional	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.821
Francisco Camargo Salas	Director de Empleo Público	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.701
Fernando Augusto Segura Restrepo	Director de Participación, Transparencia y Servicio al Ciudadano	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.631

Equipo Directivo			
Nombre	Rol	Celular	teléfono
Armando López Cortés	Director Jurídico	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.741
María Magdalena Forero Moreno	Directora de Gestión del Conocimiento	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.920
María del Pilar García González	Directora de Gestión y Desempeño Institucional	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.521
Carlos Andrés Guzmán Rodríguez	Jefe de la Oficina Asesora de Planeación	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.850
Diana María Bohórquez Losada	Jefe de Oficina Asesora de Comunicaciones	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.511
Luz Stella Patiño Jurado	Jefe de Oficina de Control Interno	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.601
Carlos Eduardo Orjuela Oliveros	Jefe de Tecnologías de la Información y las Comunicaciones	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.500

Fuente: Elaboración propia

- **Equipo Técnico de Recuperación ante Desastres:** Verifica el incidente, analiza las consecuencias e impactos potenciales, decide la activación o no del DRP y notifica al Equipo Directivo. Este equipo estará liderado por la Oficina de Tecnologías de la Información y las Comunicaciones.

Tabla 7Equipo Técnico de Recuperación ante Desastres

Equipo Técnico de Recuperación ante Desastres			
Nombre	Rol	Celular	Teléfono
Carlos Eduardo Orjuela Oliveros	Jefe de Tecnologías de la Información y las Comunicaciones	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext. 500
Eduar Alfonso Gaviria Vera	Coordinador Grupo de Proyectos Estratégicos de TI	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext. 512
Francisco Jose Urbina Suarez	Coordinador Grupo de Servicios de Información	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.200
Hilda Constanza Sanchez Castillo	Coordinador Grupo de Servicios de Tecnología	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext. 513
Juan Carlos Alarcon Suescun	Apoyo de Seguridad	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656.

Equipo Técnico de Recuperación ante Desastres			
Nombre	Rol	Celular	Teléfono
Diana María Bohórquez Losada	Jefe de Oficina Asesora de Comunicaciones	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.521

Elaboración propia

- **Equipo de Apoyo:** Son las personas que soportar la ejecución del DRP, cuando se les requiere. El equipo de apoyo estará conformado por el grupo de servicios de información.

Tabla 8 Equipo de apoyo

Equipo de apoyo			
Nombre	Rol	Celular	Teléfono
Francisco Jose Urbina Suarez	Coordinador Grupo de Servicios de Información	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.200
Hilda Constanza Sanchez Castillo	Coordinador Grupo de Servicios de Tecnología	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext. 513
Edwin Vargas	Administrador de Servidores	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.508
Evelio Lopez	Administrador de correo	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.504
Leonardo Calderón	Administradores de Infraestructura	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.507
Administrador DBA	Rafael Rodríguez	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.517

Fuente: Elaboración Propia

- **Equipo de Comunicaciones y Prensa de la Entidad:** Responsable del manejo de las comunicaciones con todas funcionarios, contratistas y partes interesadas de la Entidad. Para este caso, este equipo estará en cabeza de la Oficina Asesora de Comunicaciones.

Tabla 9 Equipo de Comunicaciones y Prensa

Equipo de Comunicaciones y Prensa			
Nombre	Rol	Celular	Teléfono
Diana María Bohórquez Losada	Jefe de Oficina Asesora de Comunicaciones	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.521
Cesar Augusto Arciniegas Beltrán	Profesional Especializado	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.523
Nury Esperanza Rojas Patiño	Profesional Especializado	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.525
Gabriela Rosalia Osorio Valderrama	Profesional Especializado	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.521

Equipo de Mesa de Ayuda

Tabla 10 Mesa de ayuda Externa e Interna

Mesa de ayuda Externa			
Nombre	Rol	Celular	Teléfono
Jaime Humberto Jimenez Vergel	Jefe Grupo de Servicio al Ciudadano Institucional	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.300
Armando Rubilo Cuaspa Huertas	Técnico Administrativo	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.306
Ada Hayde González García	Contratista	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext. 308
Erika Gissele Acosta Guerrero	Contratista	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.313
Fabiola Camacho Jimenez	Técnico Administrativo	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.307
Laura Camila Gerena Vargas	Contratista	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.301
Mateo Eduardo Alarcón Pinzón	Técnico Administrativo	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.303
Yenny Stella Chacon Santamaria	Contratista	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.302
Mesa de ayuda Interna			
Nombre	Rol	Celular	Teléfono
Julian Mauricio Martínez	Jefe Grupo de Gestión Administrativa	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.400
Edwin Sanchez Roza	Supervisor Mesa de Servicio TI Primer Nivel	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.404
Claudia Liliana Borda Espitia	Mesa Ayuda	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.404
Jonathan Archila Alonso	Mesa Ayuda	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.404
Rafael Norberto Coronado Blanco	Mesa Ayuda	información no disponible en la versión de datos abiertos de este documento	(1) 739 5656 Ext.404

Fuente: Elaboración propia

Equipo técnico de recuperación ante desastres

Tiene como objetivo establecer las distintas responsabilidades para conseguir recuperación exitosa ante una emergencia, teniendo en cuenta el DRP establecido.

A continuación, se definen los siguientes roles del equipo de DRP:

Responsable del DRP: jefe de la Oficina de Tecnologías de la Información

Apoyo y coordinación: Apoyo a la Seguridad de la Información

Apoyo y coordinación: Responsable de la Mesa de ayuda

Apoyo y coordinación: Coordinador del Grupo de Gestión Administrativa

El Equipo de DRP tiene las siguientes responsabilidades:

- Garantizar la operatividad del DRP.
- Establecer, probar, ajustar y actualizar el DRP.
- Coordinar la recuperación de los servicios en el menor tiempo posible y dentro de los tiempos establecidos.
- Realizar un informe acerca de las causas del desastre y en caso de ser necesario modificar los controles y el DRP si así se requiere.
- Brindar servicios de calidad en los tiempos esperados (RPO y RTO) y garantizar la continuidad del proceso.

Así mismo, las responsabilidades para cada uno de los roles son las siguientes:

Tabla 11 Responsabilidad del Equipo Técnico del DRP

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
Responsable del DRP	Velar por la actualización, y pruebas del DRP. Así mismo, los recursos requeridos del DRP.	Activar el DRP, las estrategias de recuperación y planes de contingencia establecidos.	Garantizar la actualización del DRP conforme con las oportunidades de mejora generadas durante el evento de interrupción.
Jefe de la Oficina de Tecnologías de la Información	Gestionar los recursos necesarios para el DRP. Establecer comunicación con las personas encargadas o responsables sobre la situación de contingencia.	Comunicar a los Directivos el desastre, interrupción o evento contingente. Informar y liderar el estado de la operación de contingencia. -Liderar el retorno a la normalidad.	Informar a los Directivos, personal y contratistas que sobre el retorno a la normalidad del servicio.
Responsable de la Mesa de ayuda	Informar las y requerimientos que se deban ajustar.	Evaluar el desastre, interrupción o evento. Comunicar el evento o interrupción al responsable del DRP. Verificar disponibilidad y	

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
	Participar en la ejecución de las pruebas al DRP.	notificar al personal requerido para atender el evento. Comunicar a los proveedores la activación del DRP. Ejecutar los planes de contingencia y recuperación. Realizar el seguimiento de la solución al evento. Mantener informado al responsable del DRP	Documentar los inconvenientes y oportunidades de mejora del DRP.
Apoyo a la Seguridad de la Información	Coordinar actividades de capacitaciones, documentación y actualización del DRP. Coordinar las actividades de pruebas del DRP. Identificar los recursos necesarios para la operación del DRP.	-Proveer soporte a los profesionales especializados. - Verificar, revisar y evaluar la continuidad de la seguridad de la información. Integrar los requisitos de la seguridad de la información en la gestión de continuidad del negocio. -Gestionar los recursos necesarios para dar solución al evento presentado. Mantener informado al responsable del DRP	Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados.

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
Coordinador del Grupo de Gestión Administrativa	Participar en la ejecución de las pruebas al DRP	Apoyar a los responsables del DRP, en actividades administrativas y logísticas ante una contingencia, entre otras. Suministro de información de los proveedores y contratos de mantenimientos. Coordinar la logística de desplazamiento, en caso de que se requiera.	- Reportar los inconvenientes y oportunidades de mejora del DRP

Fuente: Elaboración propia

Estrategia de pruebas al DRP

La programación y metodología para utilizar en la realización de pruebas al DRP están relacionadas en el Procedimiento de Gestión al Plan de Recuperación ante Desastres. Aquí se hace importante poner en practicar los procedimientos ante un incidente o desastre, identificar las áreas que necesitan mejorar y permitir al DRP permanecer activo, actualizado, entendible y usable.

Alcance de las pruebas al DRP

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

- ✓ Verificar la totalidad y precisión del plan.
- ✓ Evaluar el desempeño del personal involucrado.
- ✓ Evaluar la coordinación entre los miembros del equipo de emergencia, técnico, proveedores y terceros. Identificar la capacidad de recuperar registros e información vital.
- ✓ Medir el desempeño de los sistemas de información.

- ✓ Identificar los posibles brechas o falencias que puedan tener el plan

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

A continuación, se indican los escenarios del plan de pruebas:

Tabla 12 Escenarios de Componentes Tecnológicos

Escenarios de Componentes Tecnológicos	Causa	Efecto
Infraestructura técnica (servidores)	Procesos críticos de la Entidad	Indisponibilidad de la infraestructura por fallas
Infraestructura de bases de datos, almacenamiento y respaldo	Corrupción de la base de datos, pérdida de datos, falla total en almacenamiento o el en servidor de respaldo	Indisponibilidad de datos e información.
Infraestructura de comunicaciones	Switch Core, fibra óptica, enlaces de comunicación con ISP, firewall.	Indisponibilidad de los servicios de comunicaciones por fallas.
Centro de computo	Atentado, incendio, inundación, daño sistema aire acondicionado, daño suministro eléctrico.	Indisponibilidad de los servicios de comunicaciones de la Entidad.
Falla generalizada de toda la infraestructura tecnológica	Falla total de la infraestructura, daño suministro eléctrico, incendio, entre otros.	Indisponibilidad de los servicios y sistemas que soporta la infraestructura tecnológica.
Prueba para falla de cadena de servicios	Falla parcial de la cadena de servicios, daño suministro eléctrico, incendio, entre otros.	Indisponibilidad en la prestación de un servicio o proceso crítico.

La preparación de las pruebas debería contemplar las siguientes actividades:

Tabla 13 Actividades y Responsable

Actividad	Responsable
Establecer el líder para las pruebas.	Responsable del DRP
Informar e involucrar a los participantes en las pruebas.	Líder de las pruebas del DRP
Identificar a los líderes de los otros grupos que participarán en las pruebas.	
Gestionar reuniones con los equipos involucrados en las pruebas, con el fin de determinar / comunicar los siguientes elementos: • Objetivos a alcanzar como resultado de la prueba. • Alcance/escenario (parcial, total, aplicaciones, procesos, áreas de soporte, servicios a probar, etc.) • Tipo de prueba (escritorio, simulacro, programada, etc.) • Resultados esperados de las pruebas. • Problemas esperados de las pruebas y estrategias para mitigarlos.	
Definir el cronograma y el tiempo en las que se ejecutarán las pruebas.	
Definir con el equipo de recuperación ante desastres y el equipo de apoyo administrativo la disponibilidad de los recursos requeridos en las fechas definidas.	
Garantizar la asistencia de las personas involucradas en la ejecución de la prueba.	
Disponer de las instalaciones donde se ejecutará la prueba.	
Tener acceso a las copias de respaldo, registros vitales, infraestructura de hardware, etc. requeridos para la prueba.	
Disponibilidad de las áreas de soporte, proveedores y demás entes involucrados en la ejecución de la prueba.	

Una vez se finalicen el proceso de pruebas, se deben presentar los resultados al equipo de emergencias del DRP.

Actividades de notificación, evaluación y activación del DRP.

Los usuarios deben reportar el incidente a la mesa de ayuda cuando:

- No se pueden utilizar los sistemas de información del DAFP

- No hay red de comunicaciones.
- No hay acceso a los archivos electrónicos centralizados.
- Cualquier otro evento de tecnología que afecte la prestación del servicio.

La mesa de ayuda debe atender el incidente de acuerdo con lo establecido en sus procedimientos si:

- El incidente afecta la disponibilidad de los sistemas, a nivel general.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso al correo electrónico.
- Ningún usuario puede acceder a sus archivos electrónicos centralizados.

En cualquiera de los casos, debe escalarlo a las personas responsables. La persona a cargo del sistema de información afectado debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

- Naturaleza e impacto del incidente.
- Estrategias definidas en el DRP aplicables u otras soluciones potenciales.
- Tiempo estimado de solución del incidente.

Finalmente, comunicarse con el responsable del DRP, en este caso, el jefe de la OTIC para informar los resultados del diagnóstico.

A continuación, se describe el responsable y las actividades para la notificación, evaluación y activación del DRP:

Tabla 14 Notificación, evaluación y activación del DRP

Responsable	Actividad	Acción
Usuarios	Deben reportar el incidente o interrupción a la mesa de ayuda en los casos en que: - No puedan utilizar los sistemas de información - O cuando se presente cualquier evento de tecnología que afecte la prestación del servicio.	Reportar

Personal administrativo	Deben reportar el incidente o interrupción a la mesa de ayuda en los casos en que: - Cualquier evento que afecte o pueda afectar los servicios esenciales.	Reportar
Mesa de ayuda	Debe atender el incidente o interrupción de acuerdo con lo establecido en su procedimiento y en todos los casos se debe escalar a la persona responsable.	Reportar
Equipo Técnico de Recuperación ante Desastres	Debe realizar un diagnóstico sobre el incidente o interrupción presentada teniendo en cuenta: - Naturaleza, causa e impacto del incidente. - Estrategias definidas en el DRP que apliquen en el caso. - Tiempo estimado de solución del incidente. - Comunicarse con el responsable del DRP para informar los resultados del diagnóstico.	Evaluar
Responsable del DRP	Define si activa o no el DRP teniendo en cuentas los siguientes aspectos: - Si la solución dura más de 24 horas. - No disponibilidad de los servicios tecnológicos. - Si el incidente afecto considerablemente los servicios TIC.	Definir
Equipo de apoyo	- Fecha y hora a partir de la activación del DRP. - Responsables que estarían en el proceso de activación, en caso de que	Comunicar

	se requiera algún trámite con otra área de la Entidad.	
--	--	--

Así mismo, se debe realizar algunas actividades en paralelo como lo son:

- a. Si es un evento que afectó las comunicaciones, se debe configurar firewall y switch de contingencia y comunicarse con proveedor de comunicaciones, en caso de una falla de conexión.
- b. Si es un evento que afectó los servidores, se debe configurar y activar el servidor de contingencia.
- c. Si es un evento que afectó las bases de datos y almacenamiento, se deben iniciar la recuperación de información y bases de datos desde los respaldos, configurar el servidor de contingencia y usar los discos de contingencia (en los casos que aplique).

Versión de datos abiertos

Anexo 1

LISTA DE CHEQUEO DE PLAN DE RECUPERACION DE DESATRES DAFP

Con esta lista de chequeo se quiere realizar una valoración donde se explique específicamente si hubo daños y afectaciones a los equipos físicos y virtuales e infraestructura.

Fallas de recurso tecnológico: Favor describir el estado actual de cada uno de los servicios

Servicio	Funciona Correctamente		Observaciones
	SI	NO	
Sistemas de almacenamiento			
Servicios de conectividad y red			
Red local			
Red local inalámbrica			
Servidores Físicos			
Servidores Virtuales			
Telefonía IP			
Servicios de energía UPS			
Aplicativos (Software)			
Bases de Datos			
Almacenamiento de bases de datos			



Función
Pública

Soporte físico en el Centro de Computo: Fluido eléctrico, Aire acondicionado, Extintores			
--	--	--	--

tos abiertos

Version de C
