FUNCIÓN PÚBLICA

FUNCIÓN PÚBLICA

Plan de recuperación ante desastres tecnológicos

Proceso de Tecnologías de la Información

Oficina de Tecnologías de la Información y las Comunicaciones

VERSIÓN 01
OCTUBRE 2022

Versión	Fecha de versión (aaaa-mm-dd)	Descripción del cambio
01	03 noviembre del 2020	Primera versión del DRP
02	12 de noviembre de 2020	Ajuste del documento para publicación de datos abiertos
03	12 de noviembre de 2020	Revisión del documento para generación de la versión clasificada
04	26 de octubre de 2022	Inclusión del procedimiento de recuperación del sistema Kactus Actualización de los datos de las tablas 3,4 y 5, responsables plan de contingencia sistema de información SIGEP, FURAG Y SUIT respectivamente

Contenido

Introducción

Hoy en día la información es uno de los activos más importantes de cualquier organización, puesto que es la herramienta fundamental para el desarrollo de los procesos que se adelantan al interior de las organizaciones y que permite garantizar el funcionamiento, la continuidad y seguridad del negocio. Para la debida protección de la información se deben generar medidas adicionales 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 y de recuperación ante desastres DRP (Disaster Recovery plan), se convierten en aliados importantes para las organizaciones cuando se presentan interrupciones en la continuidad del negocio. Los DRP son procesos de restablecimiento de los 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 los procesos de soporte tecnológico.

Dado que cada vez más la entidad necesita garantizar la continuidad en la prestación de sus servicios, se requiere diseñar y actualizar periódicamente el plan de recuperación ante desastres de la entidad, de manera articulada al plan de continuidad del negocio de Función Púbica, de manera que permita proteger la información y recuperar su tecnología frente ante cualquier eventualidad. El DRP estará basado en las mejores prácticas y tecnología 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.

1. Objetivo

Diseñar y actualizar periódicamente el plan de recuperación ante desastres tecnológicos DRP de Función Pública, para actuar adecuadamente ante la ocurrencia de un evento de desastre, interrupción mayor o un evento contingente.

2. Roles y responsabilidades

Tabla 1. Roles y responsabilidades

Responsable	Rol	Actividad
Línea Estratégica	Alta dirección (director, subdirector), secretario general, jefe de OAP, jefe de OTIC) Comité Institucional de Gestión y desempeño Comité de emergencias director, subdirector, secretario general, jefe de OAP	Definir y comunicar los lineamientos generales para el establecimiento y reacción ante eventualidades que impidan la continuidad, a través del plan de continuidad y el plan de recuperación. Proveer recursos para atender las necesidades del plan de continuidad y el plan de recuperación. Tomar decisiones institucionales para la operación del plan de continuidad y del plan de recuperación ante desastres presentadas por los responsables. Citar a las personas que conformar el comité de emergencias y activar la contingencia o desastre tecnológico según la alerta.
Primera Línea	Jefe de la Oficina de las Tecnologías de la Información – Líder del proceso.	Asesorar a la alta dirección sobre eventos y controles de los riesgos de continuidad, conforme a los requerimientos técnicos y normativos vigentes. Atender con diligencia los lineamientos definidos para las diferentes etapas del plan de continuidad y el plan de recuperación ante desastres. Gestionar y ejecutar los recursos para adelantar las actividades requeridas para la activación del plan de continuidad y el plan de recuperación ante desastres.

	Equipo de trabajo delegado de la Oficina de Tecnologías de la Información	Coordinar la atención organizada y estandarizada de las actividades planificadas ante una eventualidad. Dirigir y comunicar oportunamente las situaciones de riesgo de continuidad, según los canales e instancias definidas.
Segunda Línea	Jefe de la Oficina de las Tecnologías de la Información – Líder del proceso	Asesorar a toda la entidad sobre las acciones a seguir ante un evento de riesgos de continuidad o perdida de la información ante desastres tecnológicos. Adelantar las acciones oportunas ante una eventualidad de continuidad o perdida de información ante desastres tecnológicos. Generar y activar controles para prevenir situaciones de riesgo. Documentar y conservar la trazabilidad de las acciones adelantadas.

3. Alcance

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

4. 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).

BIA - Análisis del impacto al negocio Business Impact Analysis 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 Objetive): tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

RPO: sigla en inglés (Recovery Point Objetive): 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.

5. 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 las siguientes premisas:

- 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 han 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 sitio 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.
- Se realiza copias de respaldo de las bases de datos, información y sistemas de información de acuerdo con la política institucional de copias de respaldo.

6. Escenarios de desastre tecnológico

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

Tabla 2. 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

Problemas de los servicios esenciales	Incendio Terrorismo Fuga de gas Explosión Desastres naturales.	Establecer el Teletrabajo, home office (trabajo en casa) o trabajo remoto (ley 2121 de 3 de agosto de 2021) 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".*** **KACTUS:** Se activa en plan de contingencia establecido por la Entidad en el documento denominado ***"DOCUMENTO PLAN DE CONTINGENCIA PARA SISTEMA KACTUS***

7. 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 3.Tipos de Contingencia

Estados de Alerta	Definición	Respuestas afirmativas
Menor	Generada por eventos que afectan a uno o varias áreas por un tiempo superable al tiempo de caída a 2 horas	1 a 2
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.	3 a 7
Catastrófica	Interrupción total al máximo tolerable afectando los procesos misionales y actividades de la entidad por más de 24 horas.	8 a 9

Fuente: Oficina Asesora de Planeación

Tabla 4. Medición Impacto Desastre Tecnológico

No.	Pregunta: ¿Si el riesgo de corrupción se materializa podría…?	Respuesta	
		Si	No
1	¿Afecta al responsable funcional y técnico de los sistemas de información impactados?		
2	¿Afecta el cumplimiento de metas y objetivos de la dependencia?		
3	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
4	¿Generar pérdida de recursos económicos?		
5	¿Afectar la generación de los productos o la prestación de servicios misionales?		
6	¿Generar pérdida de información de la entidad de algunas de las bases de datos misionales?		
7	¿Generar pérdida de imagen y credibilidad del sector?		
8	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
9	¿Afectar el cumplimiento de misión de la entidad por más de 24 horas?		

Fuente: Oficina Asesora de Planeación

Para medir el estado de alerta sobre la contingencia o desastre tecnológico ocurrido, deberá responder el cuestionario con el fin de determinar el impacto. Por otro lado, es importante precisar, que cuando se determine que la contingencia es 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 a través del siguiente enlace: https://www.funcionpublica.gov.co/documents/418537/0/2021-11-09_Documento_tecnico_plan_continuidad_v5+%285%29.pdf/9f53ae98-3996-6c4e-be8e-2d4155920cb6?t=1646686112334

8. 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 con el switch Core para el acceso de las diferentes áreas funcionales con los switches Core ubicados en el datacenter 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 un Internet limitado al ciudadano, la cual está totalmente aislada de la red corporativa de la entidad. Estas redes inalámbricas cuentan 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.

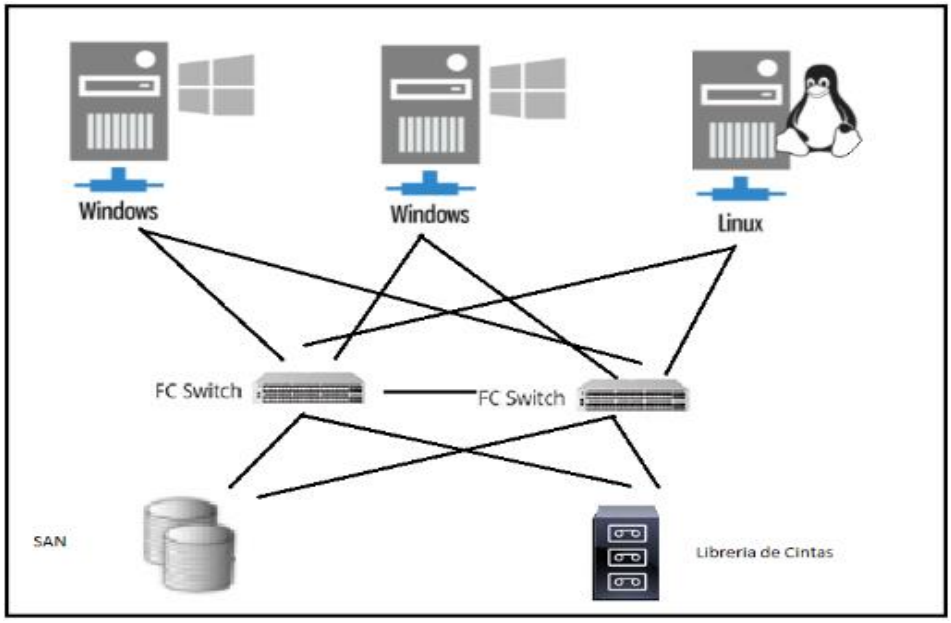

Ilustración 1. Modelo Servidores.
Fuente Función pública 2020

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 cuenta con planta eléctrica instalada desde diciembre del 2022 por el grupo de gestión administrativa, la cual soporta las dos UPS (Uninterruptable Power Suppl – Sistema de alimentación ininterrumpida) marca APC de 40KVA por 20 minutos adicionales para el sostenimiento de energía de la infraestructura de los sistemas de información que se incluyen en este plan de recuperación de desastres tecnológicos. Igualmente se cuenta con servicio de infraestructura en la nube que cubre todo el sistema energético de los servidores y dispositivos que integra infraestructura de los sistemas de información SIGEP, FURAG, SUIT y KACTUS.

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. 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.

De igual manera, 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.

9. Gestión de desastres

9.1. 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 de 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, identificado en el documento técnico de continuidad de negocio institucional, en la cual 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 SUIT
- Sistema de información FURAG
- Sistema CRM
- Sistema de información de nómina KACTUS
- 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

Este sistema soporta toda la infraestructura de almacenamiento de archivos, bases de datos recogidos a través de los diferentes sistemas de información institucional entre otra información importante para el funcionamiento de los diferentes servicios tecnológicos de la entidad.

Sistema de virtualización de servidores
Subsistemas de aire acondicionado
Sistema de energía eléctrica, sistema de UPS, bancos de baterías

9.2. 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 qué se debe realizar en caso de un evento.
- Fortalecer la coordinación interinstitucional para la respuesta ante desastres tecnológicos.

Los anteriores ítems mínimos, se especifican en detalle en la estrategia institucional de gestión de la continuidad para el escenario "desastre tecnológico", definido en el Documento Técnico del Plan de Continuidad del Negocio desde la pagina 35 a la 37, en las cuales se referencia la fase 1: Detección.

9.3. 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. Dichas tareas se encuentran definidas en el Documento Técnico del Plan de Continuidad del Negocio en la página 38, en la cual se referencia la fase 2: Activación.

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

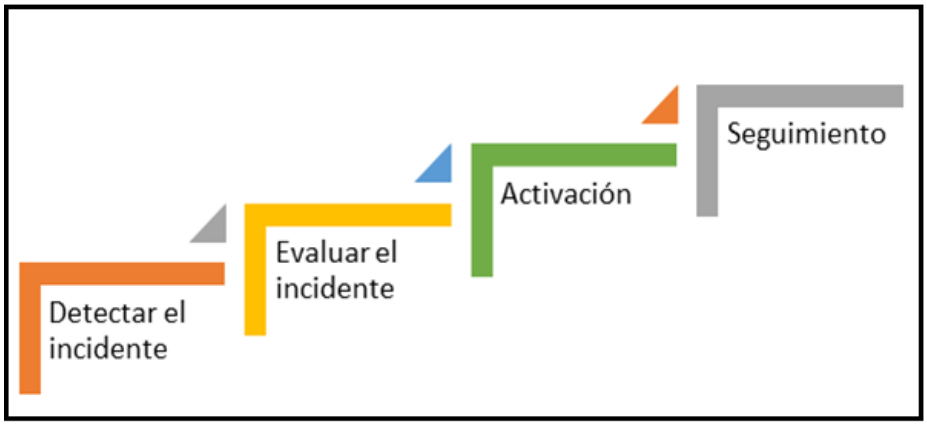

Ilustración 2.Fases para la activación del DRP
Fuente: Elaboración propia

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

- Registrar el incidente a través del formato de registro de incidentes que se encuentra publicado en el vínculo de formatos del Proceso de Tecnologías de Información
- Evaluación inicial del alcance del incidente y fallos que se realizan en la detección
- Validar la criticidad de la falla (Contingencia menor, mayor o catastrófica)
- Comunicar al equipo de gestión de emergencias institucional (Dirección, Subdirección, Secretaría general, Oficina de tecnologías de información y comunicaciones, Oficina asesora de comunicaciones)
- Activar Alertas definidas en el plan de evacuación de emergencias si es necesario salir de las instalaciones de la entidad
- Activar el plan de evacuación y emergencias
- Activación del plan de recuperación de desastres para los casos en que el desastre tecnológico presentado sea el impacto de escenarios de emergencia social y escenarios de desastre natural y colapso de la infraestructura
- Ejecución procedimientos de contingencia por dependencias
- Notificar el inicio de las actividades de contingencia, las cuales hace referencia a las fases 3 y 4 que corresponden al plan de operación alterno y la fase de resolución del incidente que se describe en la página 39 y 40 del Documento Técnico del Plan de Continuidad del Negocio
- Monitoreo y seguimiento en el periodo de contingencia
- Comunicación continúa interna/externa a los grupos de valor
- Activación de plan de retorno de contingencia
- Regreso a modo normal de operación

- Notificación formal de fin de contingencia
- Actualización del plan de recuperación de desastres
- Documentación de lecciones aprendidas
- Actualización de planes de prueba
- 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:

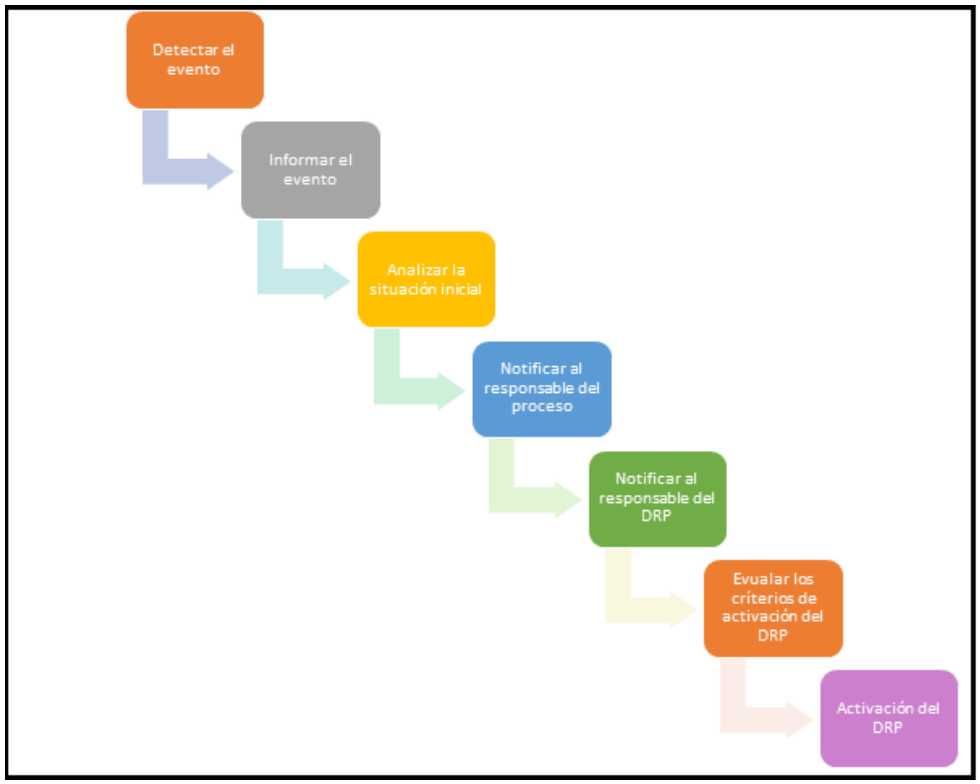

Ilustración 3. Procedimiento de notificación del DRP
Fuente: Elaboración propia.

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 todos procedimientos establecidos en Función Pública en el Documento Técnico del Plan de Continuidad del Negocio fase 1 y 2 del escenario desastre tecnológico.

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.

9.4. 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

9.5. 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:

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

9.6. Definir y activar árbol de llamadas

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

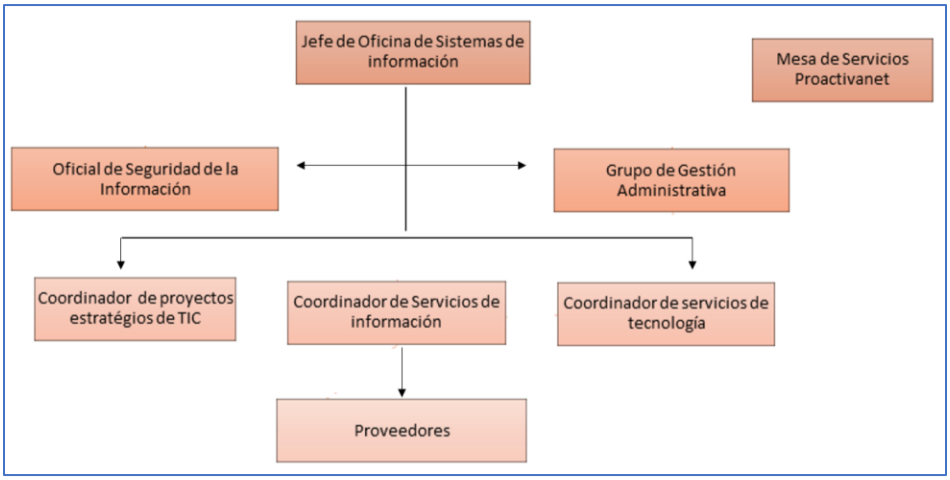

Ilustración 4. Árbol de comunicaciones del PRD
Fuente: Elaboración propia

9.7. Medios de comunicación durante el evento

Se pueden utilizar los múltiples medios de comunicación existentes en la entidad para comunicar lo ocurrido durante el incidente del desastre tecnológico, sin embargo, es responsabilidad del Jefe de la Oficina de Tecnología de la Información y las Comunicaciones, brindar la información oportuna y clara en los medios de comunicación apropiados existente en el Departamento Administrativo de la Función Pública sobre los estados de solución e impactos del incidente; principalmente al personal que tiene responsabilidades funcionales y operativas de los sistemas de información o activos de información afectados. Los múltiples medios de comunicación pueden ser:

- **Personalmente:** esté 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.
- **Mesa de ayuda: e**ste es el sistema de ayuda de servicios tecnológicos implementados internos en la Entidad que permite llevar el seguimiento desde la identificación del incidente hasta la resolución del mismo.

9.8. Principios de la comunicación durante el evento

La comunicación de la emergencia deberá considerar los siguientes principios:

- **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.
- **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.
- **Hablar con la verdad:** trasmitir 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.

10. Procedimientos de recuperación de cada sistema

10.1. 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 institucional- 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 una hora, esta actividad se desarrolla en paralelo a las actividades descritas en el Documento El Plan de Contingencia para Sistema SIGEP

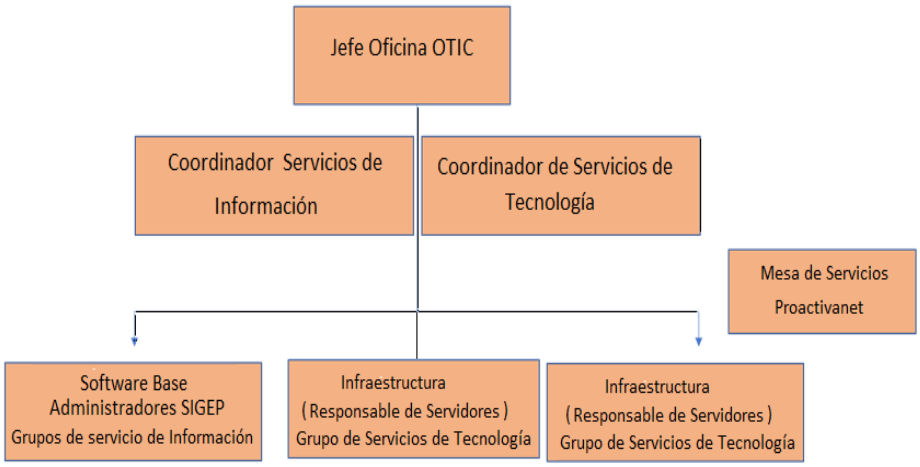

Ilustración 5. Árbol de comunicaciones del plan de contingencia SIGEP
Fuente Documento plan de contingencia para sistema SIGEP

Para asegurar la acertada implementación y gestión de la continuidad del servicio tecnológico se deben establecer roles y responsabilidades que involucren los grupos de gestión en la oficina de tecnologías de la información y las comunicaciones que se muestra a continuación en la siguiente tabla.

Tabla 5. Responsables plan de contingencia sistema de información SIGEP

Rol	Ubicación	Teléfono-ext.	Responsable
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508 504	Edwin Vargas Evelio López
Administradores de redes y Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Santiago Molina
Administrador SIGEP	Departamento Administrativo de la Función Pública – Piso 5	505 200 517 503	Lina Escobar G Francisco Urbina Rafael Rodríguez Oiris Olmos Sosa Jorge Gómez
Proveedor* Soporte Básico HEISOHN	Empresa ADA	6739744	Gerente de proyectos Edwin Mejía
Proveedor* Soporte Extendido-HEINSONH	Departamento Administrativo de la Función Pública – Piso 5 Gerente proyecto HEINSOHN	505 6337070 / 9512	Desarrollador en Sitio Olga Tapias
Administrador DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez

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".

10.2. 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 una hora, esta actividad se desarrolla en paralelo a las actividades descritas en el Documento Plan de Contingencia para Sistema FURAG

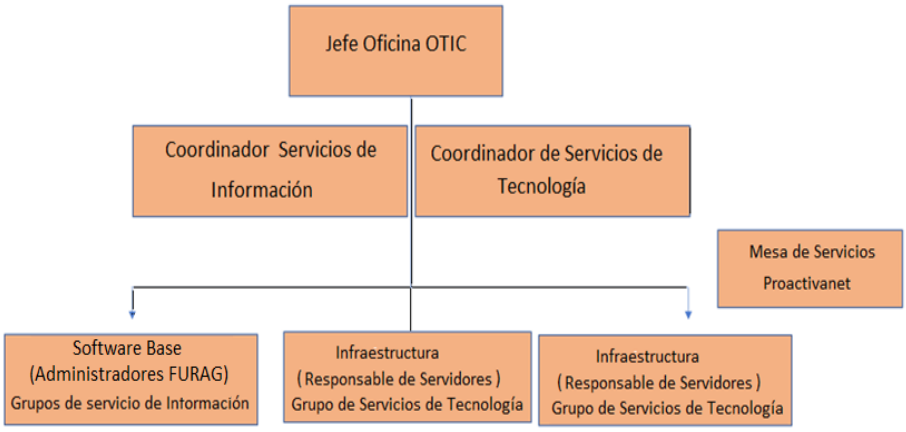

Ilustración 6. Árbol de comunicaciones del plan de contingencia FURAG
Fuente Documento plan de contingencia para sistema FURAG

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 6. Responsables plan de contingencia sistema de información FURAG

Responsable	Ubicación	Teléfono-ext.	Nombre
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508	Edwin Vargas
		504	Evelio López William Aguirre
Administradores de Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Santiago Molina
Administrador FURAG		207	Víctor Hugo Jáuregui

	Departamento Administrativo de la Función Pública – Piso 2 y 5	503	Oiris Olmos Sosa
		200	Francisco Urbina
Ingeniero Desarrollo	Departamento Administrativo de la Función Pública – Piso 2	207	Víctor Hugo Jáuregui
DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez Juan Manuel Velázquez (contratista)

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".

10.3. SUIT Sistema único de información de trámites

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

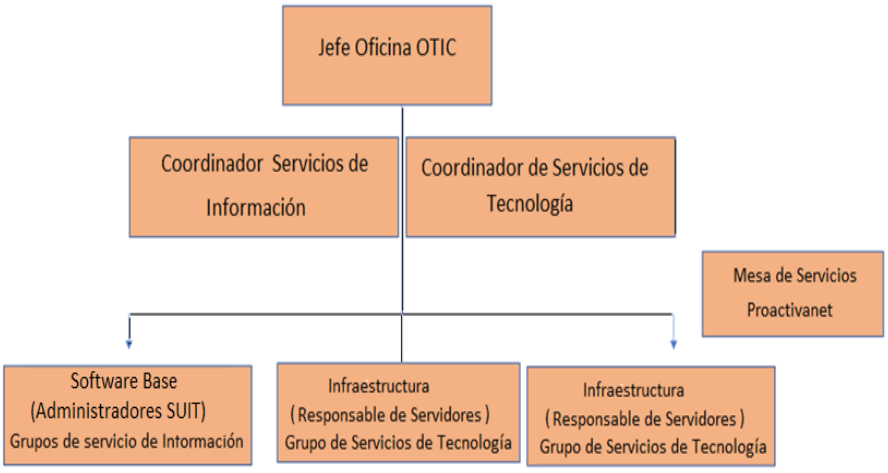

Ilustración 7. Árbol de comunicaciones del plan de contingencia SUIT
Fuente Documento plan de contingencia para sistema SUIT

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 la oficina de tecnologías de la información que se muestra a continuación en la siguiente tabla.

Tabla 7. Responsables plan de contingencia sistema de información SUIT

Rol	Ubicación	Teléfono-ext.	Responsable
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508 504	Edwin Vargas Evelio López
Administradores de Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Santiago Molina
Administrador SUIT	Departamento Administrativo de la Función Pública – Piso 5	201 207 200	Edisson Bonilla (Contratista) Víctor Jauregui Francisco Urbina
Administrador DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez

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".

10.4. De Nómina – KACTUS

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

- **Clientes internos administración:** grupo de gestión humana, secretaría general, grupo de gestión financiera, dirección de empleo público, entre otros.
- **Clientes internos funcionales:** todos los servidores públicos de Función Pública.
- **Informar** a todos los servidores públicos sobre la indisponibilidad del servicio a través de los canales de comunicación interna.

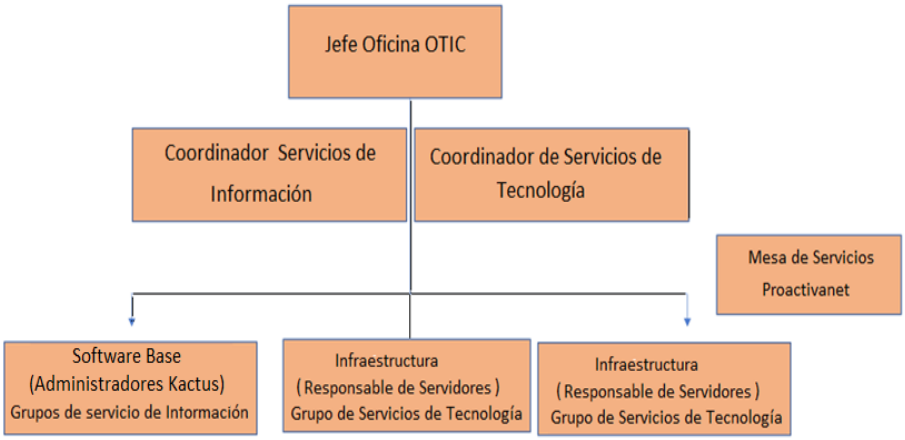

Ilustración 8. Árbol de comunicaciones del plan de contingencia
Fuente Documento plan de contingencia para sistema KACTUS

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 8. Responsables plan de recuperación del servicio de KACTUS

Rol	Ubicación	Teléfono-ext.	Responsable
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508 504	Edwin Vargas Evelio López
Administradores de redes y Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Santiago Molina
Administrador Kactus	Departamento Administrativo de la Función Pública – Piso 5	511	Luis Alejandro Bejarano Novoa
Proveedor* Soporte	Digital Ware		Asesor encargado para la contingencia en el momento
Administrador DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez

Fuente Documento plan de recuperación del servicio de KACTUS

El procedimiento completo de la activación y el restablecimiento del servicio se encuentra en el documento denominado "Documento plan de recuperación del servicio de KACTUS".

11. 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 la Oficina de tecnologías de la información y las comunicaciones junto con los coordinadores de la oficina de la OTIC y el coordinador grupo de gestión administrativa, definen el retorno a la normalidad, para ello deben definir los siguientes aspectos:

- Creación de la incidencia por el aplicativo Proactiva Net (lo puede crear cualquier integrante del grupo OTIC).
- Día fecha y hora de la activación de los sistemas de información afectados.
- Realización de una valoración donde explique específicamente si hubo daños y afectaciones a los equipos físicos. Utilizar el formato de registro de incidente de seguridad de la información.
- 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.
- Los coordinadores de la OTIC, grupo de gestión administrativa y el apoyo de seguridad de la información, documentarán el incidente e identificando las posibles mejoras para un nuevo evento verificando la guía que proporciona el Documento Técnico del Plan de continuidad del Negocio de Función Pública.
- Actualizar la matriz de materialización del riesgo en gestión de incidentes.
- Cierre por Proactiva Net de la incidencia

12. Identificación de los equipos de trabajo

La responsabilidad del plan debe ser ejercida por el personal seleccionado, de forma tal que se minimice el impacto y se actúe de forma adecuada. Para este caso, se definido 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 por el comité de emergencia de la entidad.

Para este caso, el equipo de emergencias tecnológicas de la entidad está conformado por los siguientes equipos:

Tabla 9. Equipo Directivo y Equipo Técnico de Recuperación Ante Desastres

Equipo 1	Integrantes		Funciones
Equipo directivo	Director, subdirector, secretario general, jefe de la oficina de tecnologías de la información y las comunicaciones, jefe de la oficina asesora de planeación.		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 hasta su retorno a la normalidad.
Nombre	**Rol**	**Correo**	**Teléfono**
César Augusto Manrique Soacha	Director	dgeneral@funcionpublica.gov.co	(1)739 5656 Ext.901
Jesús Hernando Amado Abril	Subdirector	jamado@funcionpublica.gov.co	(1) 739 5656 Ext.911
Lidoska Julia Dolores Peralta Prieto	Secretaria General	lperalta@funcionpublica.gov.co	(1) 739 5656 Ext.801
Hugo Armando Pérez Ballesteros	Director de Desarrollo Organizacional	hperez@funcionpublica.gov.co	(1) 739 5656 Ext.821
Francisco Camargo Salas	Director de Empleo Público	fcamargo@funcionpublica.gov.co	(1) 739 5656 Ext.701
Armando López Cortés	Director (E) de Participación, Transparencia y Servicio al Ciudadano	alopez@funcionpublica.gov.co	(1) 739 5656 Ext 631
Armando López Cortés	Director Jurídico	alopez@funcionpublica.gov.co	(1) 739 5656 Ext.741

Jesús Hernando Amado Abril	Director (E) de Gestión del Conocimiento	jamado@funcionpublica.gov.co	(1) 739 5656 Ext.920
Hugo Armando Pérez Ballesteros	Director (E) de Gestión y Desempeño Institucional	hperez@funcionpublica.gov.co	(1) 739 5656 Ext.521
Henry Humberto Villamarín Serrano	Jefe de la Oficina Asesora de Planeación	hvillamarin@funcionpublica.gov.co	(1) 739 5656 Ext.850
Daniel Canal Franco	Jefe de Oficina Asesora de Comunicaciones	dcanal@funcionpublica.gov.co	(1) 739 5656 Ext.511
Luz Stella Patiño Jurado	Jefe de Oficina de Control Interno	lpatino@funcionpublica.gov.co	(1) 739 5656 Ext.601
Hilda Constanza Sanchez Castillo	Jefe (E) de Oficina de Tecnologías de la Información y las Comunicaciones	hsanchez@funcionpublica.gov.co	(1) 739 5656 Ext.500
Equipo 2	**Integrantes**		**Funciones**
Equipo técnico de recuperación antes desastres	Integrantes de la Oficina de Tecnologías de la Información y las Comunicaciones.		Verifica el incidente, analiza las consecuencias e impactos potenciales, decide la activación o no del DRP y notifica al Equipo Directivo
Equipo Técnico de Recuperación ante Desastres			
Nombre	**Rol**	**Correo**	**Teléfono**
Hilda Constanza Sanchez Castillo	Jefe (E) de Oficina de Tecnologías de la Información y las Comunicaciones	hsanchez@funcionpublica.gov.co	
Eduar Alfonso Gaviria Vera	Coordinador Grupo de Proyectos Estratégicos de TI	egaviria@funcionpublica.gov.co	
Francisco José Urbina Suarez	Coordinador Grupo de Servicios de Información	furbina@funcionpublica.gov.co	
Hilda Constanza Sánchez Castillo	Coordinador Grupo de Servicios de Tecnología	hsanchez@funcionpublica.gov.co	
	Apoyo de Seguridad		
Daniel Canal Franco	Jefe de Oficina Asesora de Comunicaciones	dcanal@funcionpublica.gov.co	

Fuente: Elaboración propia – personal de la Entidad

El equipo técnico tiene como objetivo establecer las distintas responsabilidades para conseguir una recuperación exitosa ante una emergencia, teniendo en cuenta el DRP establecido y es apoyado por: el personal de apoyo a la seguridad de la información, el responsable de la mesa de ayuda y el coordinador del grupo de gestión administrativa.

Tabla 10. Equipo de apoyo / equipo de comunicaciones y prensa / equipo de mesa de ayuda, para la recuperación ante desastres

Equipo 3	**Integrantes**		**Funciones**
Equipo de apoyo	Conformado por el grupo de servicios de información.		Son las personas que soportar la ejecución del DRP, cuando se les requiere
Equipo de apoyo			
Nombre	**Rol**	**Correo**	**Teléfono**
Francisco José Urbina Suarez	Coordinador Grupo de Servicios de Información	furbina@funcionpublica.gov.co	(1) 739 5656 Ext.200
Hilda Constanza Sánchez Castillo	Coordinador Grupo de Servicios de Tecnología	hsanchez@funcionpublica.gov.co	(1) 739 5656 Ext. 513
Edwin Vargas	Administrador de Servidores	evargas@funcionpublica.gov.co	(1) 739 5656 Ext.508
Evelio López	Administrador de correo	elopez@funcionpublica.gov.co	(1) 739 5656 Ext.504
Leonardo Calderón	Administradores de Infraestructura	lcalderon@funcionpublica.gov.co	(1) 739 5656 Ext.507
Administrador DBA	Rafael Rodríguez	rrodriguez@funcionpublica.gov.co	(1) 739 5656 Ext.517
Equipo 4	**Integrantes**		**Funciones**
Equipo de comunicaciones y prensa	Oficina Asesora de Comunicaciones.		Responsable del manejo de las comunicaciones con todas funcionarios, contratistas y partes interesadas de la Entidad
Equipo de comunicaciones y prensa			
Nombre	**Rol**	**Correo**	**Teléfono**
Daniel Canal Franco	Jefe de Oficina Asesora de Comunicaciones	dcanal@funcionpublica.gov.co	(1) 739 5656 Ext.521
Gabriela Rosalia Osorio Valderrama	Profesional Especializado	gosorio@funcionpublica.gov.co	(1) 739 5656 Ext.521 – 523 – 525
Equipo 5	**Integrantes**		**Funciones**

Equipo de Mesa de Ayuda	Mesa de ayuda interna y externa		Equipo de atención a usuarios externos
Equipo de Mesa de Ayuda Externa			
Nombre	**Rol**	**Correo**	**Teléfono**
Lidoska Julia Dolores Peralta Prieto	Jefe (E) Grupo de Servicio al Ciudadano Institucional	lperalta@funcionpublica.gov.co	(1) 739 5656 Ext.300
	Técnico Administrativo	@funcionpublica.gov.co	(1) 739 5656 Ext.306
Ada Hayde González García	Contratista	ahgonzalez@funcionpublica.gov.co	(1) 739 5656 Ext. 308
Erika Gissele Acosta Guerrero	Contratista	eacosta@funcionpublica.gov.co	(1) 739 5656 Ext.313
Fabiola Camacho Jimenez	Técnico Administrativo	fcamacho@funcionpublica.gov.co	(1) 739 5656 Ext.307
Laura Camila Gerena Vargas	Contratista	lgerena@funcionpublica.gov.co	(1) 739 5656 Ext.301
Mateo Eduardo Alarcón Pinzón	Técnico Administrativo	malarcon@funcionpublica.gov.co	(1) 739 5656 Ext.303
Yenny Stella Chacon Santamaria	Contratista	ychacon@funcionpublica.gov.co	(1) 739 5656 Ext.302
Equipo de Mesa de Ayuda Interna			
Nombre	**Rol**	**Correo**	**Teléfono**
Julián Mauricio Martínez	Jefe Grupo de Gestión Administrativa	jmartinez@funcionpublica.gov.co	(1) 739 5656 Ext.400
Edwin Sánchez Rozo	Supervisor Mesa de Servicio TI Primer Nivel	esanchez@funcionpublica.gov.co	(1) 739 5656 Ext.404
Claudia Liliana Borda Espitia	Mesa Ayuda	cborda@funcionpublica.gov.co	(1) 739 5656 Ext.404
Jonatan Dayan Archila Alonso	Mesa Ayuda	jarchila@funcionpublica.gov.co	(1) 739 5656 Ext.404
Rafael Norberto Coronado Blanco	Mesa Ayuda	rcoronado@funcionpublica.gov.co	(1) 739 5656 Ext.404

Finalmente, el equipo de DRP se define de la siguiente manera:

Tabla 11. Equipo de DRP para la recuperación ante desastres

Equipo 6	Integrantes	Funciones
Equipo de DRP	Jefe de OTIC, Coordinador Mesa de Ayuda, Oficina (profesional designado) de	• 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.

	seguridad de la información, Coordinador Administrativa	• 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 12. Tabla de roles y responsabilidades para la recuperación ante desastres

Rol	Antes del evento de interrupción	Durante el evento de interrupción	Después del evento de interrupción
Responsable del DRP **Jefe de la Oficina de Tecnologías de la Información**	Velar por la actualización, y pruebas del DRP. Así mismo, los recursos requeridos del DRP. Gestionar los recursos necesarios para el DRP. Establecer comunicación con las personas encargadas o responsables sobre la situación de contingencia.	Activar el DRP, las estrategias de recuperación y planes de contingencia establecidos. 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.	Garantizar la actualización del DRP conforme con las oportunidades de mejora generadas durante el evento de interrupción. Informar a los Directivos, personal y contratistas sobre el retorno a la normalidad del servicio.
Responsable de la Mesa de ayuda	Informar las interrupciones ocurridas y requerimientos que se deban ajustar. Participar en la ejecución de las pruebas al DRP.	Evaluar el desastre, interrupción o evento. Comunicar el evento o interrupción al responsable del DRP. Verificar disponibilidad y 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.	-Proveer soporte a los profesionales especializados. - Verificar, revisar y evaluar la continuidad de la	Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados.

	Identificar los recursos necesarios para la operación del DRP.	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	
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

13. Estrategia de pruebas al DRP

La programación y metodología para utilizar en la realización de pruebas al DRP están relacionadas en el Documento Técnico del Plan de Continuidad del Negocio (Escenario 3: fase 2). 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 por lo menos una vez al año, 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 13. 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	Falla en dispositivos de hardware (Switch Core, fibra óptica, enlaces de comunicación con ISP, firewall.)	Indisponibilidad de los servicios de comunicaciones por fallas en la infraestructura.
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 14. 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 accedo 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.

14. 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 15. 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.	Definir

	- Si el incidente afectó considerablemente los servicios TIC.	
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 se requiera algún trámite con otra área de la Entidad.	Comunicar

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

- Si es un evento que afectó las comunicaciones, se debe configurar firewall y swicth de contingencia y comunicarse con proveedor de comunicaciones, en caso de una falla de conexión.
- Si es un evento que afectó los servidores, se debe configurar y activar el servidor de contingencia.
- 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).

Anexo 1

Lista de Chequeo del Plan de Recuperación de Desastres 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			
Soporte físico en el Centro de Computo: Fluido eléctrico, Aire acondicionado, Extintores			

Favor realizar una breve descripción de cómo se encuentra los servicios del DAFP.

_____
_____
_____
_____

Favor exponer las mejoras para un nuevo evento

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma de funcionario o contratista

Plan de recuperación ante desastres tecnológicos

Proceso de Tecnologías de la Información
Oficina de Tecnologías de la Información y las Comunicaciones
OCTUBRE DE 2022

Departamento Administrativo de la Función Pública
Carrera 6 n.º 12-62, Bogotá, D.C., Colombia
Conmutador: 7395656 Fax: 7395657
Web: www.funcionpublica.gov.co
eva@funcionpublica.gov.co
Bogotá, D.C., Colombia.