Plan de recuperación de desastres

Código SG/MIPG	127-PPPGI-09
Vigencia desde	30/06/2021
Versión	1

Proceso Gestión de la tecnología y la información

ALCALDÍA MAYOR DE BOGOTÁ D.C.

DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

BOGOTÁ

Tabla de Contenido

1. INTRODUCCIÓN

La Defensoría del Espacio Público- DADEP es una entidad del Orden Central de la Alcaldía Mayor de Bogotá, adscrita a la Secretaría de Gobierno, cuya misión es: "*Contribuir al mejoramiento de la calidad de vida en Bogotá, por medio de una eficaz defensa del espacio público, de una óptima administración del patrimonio inmobiliario de la ciudad y de la construcción de una nueva cultura del espacio público, que garantice su uso y disfrute colectivo y estimule la participación comunitaria*". Sus procesos acceden mediante una infraestructura tecnológica dotada de elementos de seguridad perimetral a los diferentes sistemas de información; la administración está bajo la custodia de la Oficina de Sistemas, quien tiene la responsabilidad de mantener su disponibilidad.

Por lo anterior y consientes de la existencia de los riesgos asociados a las Tecnologías de la Información y Comunicaciones, la Oficina de Sistemas define el Plan de Recuperación de Desastres - DRP que define los objetivos, el alcance, las estrategias predeterminadas y las acciones que deben ser conocidas, interiorizadas y probadas periódicamente por el personal encargado de recuperar los servicios tecnológicos en el caso que se materialice un evento adverso.

1.1 OBJETIVO GENERAL

Definir las acciones y los responsables que permitan restaurar los servicios de tecnologías de la información y comunicaciones del análisis de impacto al negocio que se vean afectados parcial o total frente a eventos indeseados, logrando en lo menos posible la afectación de la confidencialidad, integridad y disponibilidad de la información.

1.2 OBJETIVOS ESPECÍFICOS

- Dar continuidad a los servicios tecnológicos establecidos en el análisis de impacto al negocio del DADEP ante situaciones adversas de interrupción mayores o catastróficas.
- Proveer una guía para la recuperación, luego de la materialización de un riesgo que pueda afectar los Servicios tecnológicos descritos en el análisis de impacto al negocio.
- Recuperar las aplicaciones críticas oportunamente, fortaleciendo su resiliencia.

1.3 ALCANCE

Este Plan de Recuperación de Desastres aplica a los Servicios tecnológicos y comunicaciones del DADEP identificados en el análisis de impacto al negocio.

El Plan define los procedimientos, los responsables de dar respuesta y recuperación de la operación normal de los servicios tecnológicos y comunicaciones ante los siguientes escenarios:

- Los incidentes que pueden interrumpir los servicios tecnológicos por un tiempo prolongado, corte en el servicio de comunicaciones o fallas en el suministro eléctrico.
- Eventos que cause daño físico a las instalaciones.
- Sucesos que afecten el acceso a las instalaciones.

1.4 SIGLAS

- **BIA**: Acrónimo de Business Impact Analysis (En inglés). Análisis del Impacto al Negocio.
- **DRP**: Acrónimo de Disaster Recovery Plan (en inglés). Plan de Recuperación de Desastres.
- **RTO**: Acrónimo de Recovery Time Objective (en inglés). Punto Tiempo objetivo de tiempo de recuperación).
- **RTO**: Acrónimo de Recovery Point Objective (en inglés). Punto objetivo de recuperación.

1.5 DEFINICIONES

- **Análisis del Impacto al Negocio (BIA)**: Proceso del análisis de actividades, funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300].
- **Plan de Recuperación de Desastres**: Documento que describe la organización y las acciones que deben llevarse a cabo antes, durante, y después de un desastre, así como los procedimientos para restablecer la disponibilidad de los Servicios tecnológicos, aplicaciones y comunicaciones que permiten mantener la continuidad de las operaciones de la organización soportadas por las Tecnologías de la Información.
- **Objetivo mínimo de continuidad de negocio (MBCO)**: Mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.
- **Punto objetivo de recuperación (RPO)**: Es el máximo periodo de tiempo que una organización está dispuesta a perder datos
- **Punto Tiempo objetivo de tiempo de recuperación (RTO)**: Es el periodo de tiempo que la entidad necesita para recuperar un sistema de información después de la inactividad producida por un incidente.
- **Resiliencia**: Habilidad, Capacidad de una organización para resistir cuando es afectada por un incidente.

2. ACTIVIDADES DE PREPARACIÓN

Con objeto de definir las estrategias, acciones y procedimientos de recuperación e identificar los recursos necesarios y grupos de trabajo que actuarán antes, durante y después de una recuperación, se llevarán a cabo diversas actividades encaminadas a este fin.

2.1 Situación Actual de los Servicios tecnológicos y Comunicaciones

2.1.1.1 En la nube

Por la seguridad, flexibilidad técnica y el acompañamiento brindado por el proveedor, la entidad opto por administrar y controlar sus principales sistemas de información en la nube, actualmente sus servicios tecnológicos y comunicaciones son proveídos por Microsoft (AZURE).

2.1.1.2 Servicios de ORACLE

Almacena las bases de datos de las aplicaciones consideradas críticas o Core de la entidad y de igual manera se aloja en la nube.

2.1.1.3 Servicios On premise

Se desarrollan desde el centro de cómputo ubicado en las instalaciones de la entidad el cual cumple con las condiciones físicas, eléctricas, térmicas y de seguridad para su operatividad. En él, se establece el modelo de hiperconvergencia el cual se compone de dos servidores DELL PowerEdge r810 con una capacidad de almacenamiento de 18 TB reales, estos son monitoreados por la Oficina de sistemas y sus principales funciones son:

- la virtualización de servidores que son utilizados como los ambientes de desarrollo y pruebas de las aplicaciones en producción de la entidad
- Almacenamiento de backup de Bases de datos
- Alojamiento de continuidad del servicio de dominio. Los servidores DELL cuentan con recursos de almacenamiento de 18 TB reales, los cuales son monitoreados por la Oficina de sistemas.

Componentes tecnológicos que tiene el centro de cómputo

Cantidad	Descripción
1	1638 enrutador
1	1625 sistema contra incendios
4	1298 SISTEMA ALMACENAMIENTO - NAS
4	1644 servidor
2	1615 aire Acondicionado
6	1662 PDU (MULTITOMA INTELIGENTE DEL CENTRO DE COMPU
1	1651 UPS
10	1636 Dataswitch
8	1636 Access Point / 2020
1	1670 equipo analizador de seguridad perimetral

Actualmente el centro de cómputo es monitoreado con la herramienta NAGIOS la cual notifica el comportamiento de equipos y servicios, alertando cuando se presente alguna anomalía sobre la carga de procesamiento, capacidad de discos, memoria y el funcionamiento de los servicios de red HTTP, ICMP.

2.2 Principales Plataformas y Aplicaciones

La Defensoría del Espacio Público actualmente tiene un catálogo servicios tecnológicos que dan apoyo al desarrollo de las funciones de procesos estratégicos, misionales, de soporte, de verificación y mejora. Dichos servicios han sido desarrollados utilizando distintos lenguajes de programación entre los que se destacan Java, PHP, JavaScript, HTML, Oracle Forms Oracle Reports (PL/SQL) y CSS; como plataforma o motor de base de datos para soportar las aplicaciones se encuentran Oracle 11g R2 y MySQL.

Cada servicio cuenta con personal dedicado a prestar soporte, mantenimiento, gestión de requerimientos e incidentes y desarrollo de nuevos módulos de acuerdo con las solicitudes realizadas por parte de los usuarios.

En la tabla 1 se listan los sistemas de información con características y atributos que actualmente posee la entidad.

Tabla 1. Sistemas de información de la entidad

Nombre	Descripción	Módulos
SIDEP II	Sistema de información misional que contiene la información del patrimonio inmobiliario, administración, cartografía e imágenes documentales del mismo.	Inventario, defensa y administración.
SIGDEP	Sistema de información geográfico que permite la gestión, análisis y visualización de información cartográfica de los bienes fiscales, predios públicos de cesión y predios públicos de no cesión de propiedad del Distrito.	Urbanizaciones, predios y construcciones.
SUMA	Sistema de información para el manejo y aprovechamiento de espacio públicos.	Pufa y Suma.
Observatorio de Espacio Público	Portal web el cual presenta las investigaciones, indicadores y documentos resultados del grupo de investigación del DADEP.	Observatorio.
Portal WEB Institucional	Portal web de la entidad.	Portal WEB.
SI-CAPITAL	Sistema de información que soporta procesos y procedimientos de apoyo a la gestión de la entidad.	PERNO, SAI-SAE, SISCO, LIMAY, TERCEROS, OPGET, PREDIS.
ROYAL	Sistema de Información documental, encargado de digitalizar e indexar la documentación de la entidad.	Producción, Administración de imágenes y OCR.
ORFEO	Sistema de información que permite la gestión electrónica, producción, trámite y almacenamiento digital de documentos de la entidad.	Radicación.

MAP – CPM	Gestión de acciones correctivas y de mejora	Acciones correctivas, preventivas y de mejora.
Visor MIPG	Sistema donde se publica la documentación perteneciente al sistema de gestión de la entidad.	Sistema de Gestión.
Control de Horario	Sistema que permite llevar el registro de la entrada y salida de los funcionarios de planta a las instalaciones de la entidad.	Registro, Administración, Reportes.
Plataforma de mesa de ayuda	Sistema de apoyo que cuenta con el registro de requerimientos e incidentes sobre los servicios tecnológicos y sistemas de información de la entidad	Registro, Reportes, Administración.
Intranet	Portal web que contienen información relevante para los colaboradores del DADEP usada como herramienta de divulgación interna de información.	Intranet

Fuente: Información corporativa de la entidad

2.3 Análisis de Procesos y Aplicaciones.

Como parte preliminar al desarrollo del Plan de Recuperación (PRD) para los Servicios tecnológicos, es necesario realizar un análisis de aplicaciones para:

- Definir sus de requerimientos técnicos y operativos.
- Determinar cuáles soportan procesos misionales críticos y la interrelación entre ellas.
- Examinar la composición de los procesos
- Identificar la dependencia de los procesos en las aplicaciones
- Definir la prioridad de recuperación y la Configuración de Recuperación Mínima Aceptable (MARC).

La vulnerabilidad en los procesos de la entidad se determinó asumiendo la pérdida de los sistemas críticos debido a un evento mayor o catastrófica interrumpiendo el funcionamiento normal de la operación.

Como resultado del estudio, se clasificaron las aplicaciones en las siguientes categorías de criticidad:

IDENTIFICACIÓN DE RTO	
El Tiempo de Recuperación Objetivo (RTO), define el tiempo máximo de recuperación de un servicio de tal forma que el impacto no afecte a la organización. Encontrar el RTO es definir el punto de equilibrio entre el costo de la estrategia de recuperación y las perdidas por el impacto de la no disponibilidad, si el RTO es muy pequeño entonces las perdidas por el impacto también son pequeñas sin embargo el costo de la estrategia de recuperación es alto, por el contrario, si el RTO es muy grande, el costo de la estrategia de recuperación es pequeño, pero las pérdidas por el impacto de la no disponibilidad son altas.	
Calificación	Rango de Tiempo de Interrupción Tolerable
5	Entre 0 y 8 Horas
4	Entre 8 y 24 Horas
3	Entre 24 y 48 Horas
2	Entre 2 y 5 Días
1	Entre 5 y 10 Días
0	Superior a 10 Días

IDENTIFICACIÓN DE RPO	
Punto Objetivo de recuperación. (Recovery Point Objetive - RPO): Punto en el tiempo en el cual los datos deberían ser recuperado después de que una interrupción ocurra. Se refiere a la cantidad de datos que se pierden y no son recuperables debido a la interrupción. Esto se representa en una línea de tiempo como la cantidad de tiempo entre la última copia de respaldo buena y cuando el evento de interrupción ocurre. El RPO varía en función de la estrategia de recuperación de servicios de TIC empleada, particularmente en la disposición de la copia de respaldo.	
Calificación	Punto en el cual deben ser recuperados los datos
5	Entre 0 y 8 Horas
4	Entre 8 y 24 Horas
3	Entre 24 y 48 Horas
2	Entre 2 y 5 Días
1	Entre 5 y 10 Días
0	Superior a 10 Días

De acuerdo con los resultados obtenidos en el análisis, el daño causado por la interrupción de la operación de la entidad, tanto a corto como a largo plazo, puede ser catastrófico, particularmente si el evento ocasiona pérdida de información.

El hecho de no planificar una estrategia que permita recuperar las operaciones de las aplicaciones, servicios críticos y los procesos relacionados en un tiempo estimado, podría

ocasionar a la entidad incumplimientos legales, sanciones financieras, problemas operacionales y reputacionales.

2.4 Estrategia de Recuperación de aplicaciones.

Considerando las necesidades de recuperación de DADEP y de acuerdo con los resultados del Tiempo objetivo de Recuperación (RTO) definidos por los procesos de la entidad, las estrategias de recuperación consideradas son las siguientes:

Alta Disponibilidad: Para aquellas aplicaciones que resultaron con un RTO menor de 8 y 12 horas y que requieren un nivel muy elevado de confiabilidad y disponibilidad. La estrategia es la restauración de una copia de seguridad (Snapshot) la cual restaura la interfaz, la base de datos y los datos de la aplicación afectada permitiendo restablecer el servicio en menos de una hora.

Incremento en capacidad del equipo actual: Aplica para aquellas aplicaciones que resultaron con un RTO tanto de 6 y 12 horas, de entre 24 y 48 horas y mayor a 72 horas, la estrategia se basa en la flexibilidad que brinda el servicio contratado con Microsoft el cual permite incrementar y reducir a criterio y necesidad de la entidad la infraestructura tecnológica utilizada.

2.5 Recuperación de los Servicios Críticos.

Para el caso de los servicios de Tecnología de Información críticos para la entidad se identificaron los siguientes:

NOMBRE DEL SERVICIO	DESCRIPCIÓN	COMPONENTE	TIEMPO DE RECUPERACIÓN OBJETIVO (RTO)	OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO)
Conectividad	Servicio que brinda soporte a acceso a la red de internet a través de dispositivos móviles y computadores portátiles, Permite el uso de impresoras, scanner, carpetas compartidas, telefonía IP interna, sistemas de información	Canal de datos	5	5
		Directorio Activo	5	5
		Fluido eléctrico	5	5
		Firewall	5	5

	específicos como apoyo a los procesos, entre otros recursos.			

3. ESCENARIOS DE CRISIS

3.1 Riesgos de contingencia

Para los escenarios de crisis, se ha identificado el riesgo *Interrupción de la Operación de la Plataforma Tecnológica* en la matriz institucional, con los siguientes detalles:

Nombre del Riesgo	Interrupción de la Operación de la Plataforma Tecnológica.
Descripción del Riesgo	No operación de la plataforma tecnológica por diferentes aspectos que generen no operación de las actividades de la entidad.
Clasificación del Riesgo	Riesgo de Seguridad Digital.
Tipología del Riesgo	Seguridad digital
El Riesgo inherente de seguridad digital afecta: (Confidencialidad, Integridad y Disponibilidad)	Disponibilidad
Activo de Información (Seguridad Digital)	Información física o digital
Amenazas (Seguridad Digital)	Interrupción de la Operación de la Plataforma Tecnológica.
Causas / vulnerabilidades	1. Acciones humanas voluntarias e involuntarias
Consecuencias	1.Incumplimiento de tipo legal o contractual 2.Indisponibilidad colateral de otros servicios 3.Interrupción del servicio 4. Pérdida de imagen / credibilidad 5.Pérdida económica 6.Retraso en la toma de decisiones 7.Fraude
Probabilidad	Probable
Impacto	Mayor
Zona del riesgo	EXTREMA

3.2 Estrategia de Recuperación

Las estrategias para seguir serán acordes a la magnitud y duración esperada del incidente y se deberán tomar en cuenta los siguientes aspectos:

- Evaluación de los daños
- Evaluación del tiempo estimado de la recuperación.
- Análisis detallado para determinar las acciones específicas que deberán seguirse de acuerdo con el tipo de incidente.

4. Activación del Plan de Recuperación

La magnitud del incidente dicta los procedimientos apropiados y el personal necesario para la evaluación del impacto y de los daños, que, a su vez, proporciona las premisas bajo las cuales se basa la decisión de la Declaración del Desastre (Actividades de respuesta a una emergencia y los procedimientos de evaluación de Daños), dependiendo el resultado del diagnóstico, se decide la Activación del Plan, y la notificación al Grupo Coordinador

Los procedimientos de recuperación documentan la evaluación inicial, la decisión y las actividades de inicio del Grupo Coordinador. Como se ha mencionado, este grupo ofrece una coordinación y comunicación centralizadas de toda respuesta al incidente y de las actividades de recuperación.

Al menos de que se trate de un desastre inminente, el elemento más importante del proceso de recuperación es la ventana de decisión. Esto es, el tiempo predeterminado de 8 horas en el que el Grupo Coordinador tiene que tomar una decisión sobre la Declaración del Desastre. Esta decisión se basa en la evaluación del daño causado y el diagnóstico de tiempo en el que las instalaciones, el equipo y los servicios tecnológicos y de comunicación, tanto de voz como de datos estarán disponibles para continuar las funciones de la entidad.

Una vez que se haya identificado y reconocido un evento, las respuestas y acciones de recuperación van contra reloj. Los procedimientos que se presentan a continuación incluyen decisiones que son críticas con respecto al tiempo y que pueden estar basadas en la magnitud del incidente, su evaluación, y en el impacto que generó en las operaciones de la entidad.

4.1 Reconocimiento del evento y su notificación.

La identificación o reconocimiento del evento ocurre cuando se ha presentado un incidente y es evidente que causará una interrupción en los procesos normales de la entidad. Es el punto en el tiempo en que la implementación de las respuestas y acciones de recuperación, incluyendo la notificación y la activación del Grupo Coordinador y de los Grupos de Recuperación es inevitable.

La notificación de un peligro potencial puede llegar de varias fuentes dependiendo de la naturaleza del incidente y la hora en que suceda. La respuesta inicial a la notificación está dictada por los procedimientos de respuesta a la emergencia de la entidad y las prácticas normales de operación.

Es importante que todo el personal sepa a quien acudir en caso de que se presente un incidente, y el personal de Seguridad debe de tener un listado de las personas que componen el Grupo Coordinador para que en caso de que suceda un incidente en horarios no laborables, puedan contactar a los líderes y así iniciar el proceso.

Si se detecta un probable incidente dentro de las instalaciones...

1. Lleve a cabo los pasos para notificar la emergencia (ejemplo accione la alarma contra incendio),

2. Notifique a seguridad lo siguiente:

- Su nombre;
- Descripción del incidente;
- Reporte preliminar de daños y heridos;
- Número telefónico y dirección dónde puede ser localizado.

En el caso de evacuación del edificio o de falla de servicio, diríjase al Centro de Control de Crisis.

Si fue notificado mucho tiempo después o porque le escalaron un problema tome nota de la información que a continuación se especifica:

- Fecha y hora en que recibe el aviso del problema;
- Nombre de la persona que avisa;
- Descripción de la situación;
- Punto de reunión (en caso de ser diferente del Centro de Control de Crisis);
- Instrucciones especiales de cualquier tipo.

De acuerdo con lo que le solicite el portavoz haga las notificaciones utilizando la información que le fue proporcionada.

Diríjase a la localidad alterna asignada o al lugar que le especifique el portavoz con su copia del Plan de Recuperación (PRD) para los Servicios tecnológicos (PRD).

4.2 Evaluación de los Daños.

La evaluación de daños es la actividad inicial que debe efectuarse inmediatamente después de un incidente. Esta actividad es realizada por el Grupo Coordinador, el cual está constituido por los líderes de los grupos y los responsables de Mantenimiento de Edificios y Seguridad

Institucional. El conjunto de estrategias y acciones que el grupo seleccione para tratar una situación en particular constituye lo que se denomina Recomendaciones de Recuperación.

El Grupo Coordinador 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.

El objetivo de la evaluación es identificar de manera precisa los daños físicos al Centro de Cómputo, su contenido, equipos y materiales.

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

4.3 Procedimientos de Respuesta Inmediata

Implementar los procedimientos de respuesta inmediata basados en las circunstancias específicas, estos procedimientos, normalmente desarrollados por recomendación de protección civil, su objetivo es disminuir el impacto al personal, hasta que las condiciones vuelvan a situación normal para los siguientes casos:

4.4 Notificaciones de Emergencia a Usuarios Finales

Contactar a los usuarios finales críticos, por medio de un comunicado sobre el incidente.

1. Desarrollar un comunicado de emergencia para ser entregado al Grupo de Procesos de la entidad para hacerlo llegar a todos los contactos clave de las diversas Unidades de la entidad. Incluir sólo los hechos verídicos y no hacer suposiciones. Esta declaración debería contener:

   1.1 Breve comunicado respecto al incidente;

   1.2 Fecha y hora probable se conocerá el estado en el que se encuentra el servicio y Fecha y hora en que se espera que el servicio sea restablecido (si se tiene conocimiento)

1.3 Si es posible, de acuerdo con el tiempo de restauración del servicio, indicar la fecha y hora en que sus aplicaciones serán restablecidas

2. Informar la situación REAL de la emergencia y las consecuencias inmediatas.

3. No especular sobre lo que se ignora. No hacer ningún compromiso más allá de lo que se está absolutamente seguro de cumplir.

5. PROCEDIMIENTOS DE RECUPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS

Estos Procedimientos de Recuperación se basan en el peor escenario, es decir el no acceso a los Servicios tecnológicos y comunicaciones o al Centro de Cómputo, requiriéndose la reubicación y recuperación de los servicios informáticos en un centro de cómputo alterno. El Grupo Coordinador actúa como una central de control para supervisar la reubicación de recursos disponibles para la recuperación de Los servicios del centro de cómputo y apoyar a cualquier usuario en sus requerimientos finales informando al Grupo Directivo PRD.

5.1 Procedimientos para la Declaración de Desastre

Una vez que el Grupo Coordinador y el Grupo Directivo han evaluado el nivel de contingencia y la duración de la interrupción en las operaciones normales del DADEP, las actividades de Declaración de Desastre y el Desarrollo del Plan de Acción encaminadas a la Recuperación se inician de inmediato.

Para declarar un desastre el Grupo Coordinador realiza las siguientes actividades:

- Obtener la información de diagnóstico y tiempo de recuperación.
- Analizar el alcance de los daños y si la interrupción a la operación normal de la entidad (por fallas de infraestructura tecnológica o la imposibilidad de acceso al edificio de las oficinas corporativas o fallas en las comunicaciones), va a ser mayor a 8 horas, se determina a la declaración del desastre.
- Notificar telefónicamente a los integrantes de los Grupos de Recuperación

- Promover una reunión de retro alimentación de información en el Centro de Control de Crisis seleccionado de acuerdo con el incidente (ver capítulo 3.1.4 Centro de Control de Crisis (CCC)).

- Solicitar a los líderes de los Grupos de Recuperación iniciar de inmediato la recuperación de acuerdo con el Plan.

5.2 Notificación de Accesibilidad

Una vez que las comunicaciones y servidores hayan sido habilitados, se le notificará al Grupo Coordinador que los servicios tecnológicos han sido habilitados para operar bajo el esquema de contingencia.

El Grupo Coordinador notificará a las áreas internas y entidades externas el modo de operación (bajo esquema de contingencia).

6. PROCEDIMIENTOS DE RESTAURACIÓN DEL CENTRO DE CÓMPUTO

Las determinaciones para activar los siguientes Procedimientos de Restauración del Centro de Cómputo serán hechos por el Grupo de Recuperación basados en las circunstancias específicas del incidente. El grupo activará personal apropiado para la restauración del Centro de Cómputo dañado. El Grupo de Recuperación supervisará las actividades de planeación e implementación para los Grupos de Recuperación asociados a este punto.

6.1 Plan de Retorno

Desarrollar la estrategia de reubicación detallada en el "Plan de Acción de Restauración" para volver a las instalaciones restauradas usando el procedimiento del Plan de Recuperación del Centro de Cómputo como una guía. Después, coordinar el regreso a las instalaciones permanentes (nuevas o reconstruidas) al concluir la operación de recuperación.

1. Participar en reuniones para planear la restauración del centro de cómputo dirigidas por el Grupo de Recuperación. El propósito de esta reunión será discutir las estrategias generales de regreso. El Grupo de Recuperación definirá y desarrollará las siguientes normas:

    1.1 Fecha y hora de la disponibilidad de regreso de cada Grupo de Recuperación;

    1.2 Condición de los servicios de apoyo (teléfono, Servicios tecnológicos, etc.);

1.3 Cualquier requerimiento especial de logística o soporte que deberá estar disponible para los Grupos de Recuperación (transporte para el equipo y registros, asistencia con registros de empaque, etc.).

2. Conducir al Líder de cada Grupo de Recuperación a reuniones de planeación para revisar y actualizar Procedimientos de Recuperación para reflejar el movimiento de retorno a las instalaciones permanentes desde el Centro de Cómputo Alterno.

   2.1 Revisar cada paso del procedimiento de recuperación, modificándolo de acuerdo con las circunstancias. Verificar que los procedimientos de respuesta puedan ser usados para proveer una contingencia durante el movimiento.

   2.2 Considerar ejecutar copias de seguridad especiales con el fin de reducir las posibilidades de pérdida de información.

   2.3 Identificar cualquier aspecto pendiente, requerimiento o recomendaciones para el Grupo de Recuperación.

   2.4 Proporcionar esta entrada como retroalimentación al Grupo de Recuperación con quien se desarrollará un plan de acción consolidado final y actualizado.

3. Desarrollar una agenda final aprobada y revisar con todo el personal participante del Grupo de Recuperación.

4. Implementar el procedimiento de Retorno a la operación normal

Tareas del Grupo de Respuesta y Recuperación

Restaurar la infraestructura de cómputo en las instalaciones propias, requieren las siguientes actividades para el restablecimiento de los servicios y un protocolo de reincorporación de los movimientos efectuados durante la contingencia:

1. Probar que el Centro de Cómputo nuevo esté listo para ser utilizado.

2. Coordinar la fecha de regreso a las actividades normales.

3. Comunicar a la Alta Dirección la terminación del desastre.

4. Notificar al personal de Sistemas el regreso a la operación normal.

5. Verificar que obtengan copias de seguridad de los archivos modificados del Centro de Cómputo Alterno.

6. Verificar que las comunicaciones estén enrutadas al Centro de Cómputo nuevo.

7. Cancelar y liquidar los servicios contratados durante el desastre.

8. Coordinar la reinstalación de las actividades en las Oficinas administrativas.

9. Coordinar que cada Grupo revise que los documentos, manuales, catálogos, directorios, etc. utilizados en el Centro de Trabajo Alterno estén de nuevo en las Oficinas Administrativas.

10. Evaluar el Plan de Contingencia y el desempeño del personal durante el desastre.

    10.1. Solicitar retroalimentación de los participantes del Plan.

7. PROCEDIMIENTOS ADMINISTRATIVOS DEL CENTRO DE CÓMPUTO

7.1 Distribución y Disponibilidad del Plan

Asegurar que el Plan de Recuperación (PRD) para los Servicios tecnológicos, incluyendo todos los recursos de recuperación identificada, así como los procedimientos, se encuentren preparados para su utilización:

1. Mantener una copia actualizada de su Plan de Recuperación (PRD) para los Servicios tecnológicos en centro de cómputo alterno y la oficina administrativa.

2. Asegurar que todos los miembros del equipo y sus suplentes mantengan una copia actual de este Plan.

3. Asegurar que todo el personal de los grupos de recuperación considere la preparación de recuperación como parte de sus deberes normales.

4. Asegurar que las copias de seguridad y actividades de rotación externas para registros vitales están siendo efectuados.

5. Hacer mantenimiento a su Plan de Recuperación (PRD) para s Servicios tecnológicos (PRD) incluyendo todos los procedimientos, lista de comprobación, equipos agrupados y actualizados.

   Actualice este plan para cualquiera de las siguientes circunstancias:

5.1 Cambios en el personal del departamento que forman parte de los Grupos.

5.2 Cambios significativos a los requerimientos de recuperación del centro de cómputo que reflejen cambios en el marco de Recuperación o en la Configuración de Recuperación Mínima Aceptable;

5.3 Cambios significativos a los procedimientos de recuperación, tales como la adición de una nueva función de la entidad, sistemas/aplicaciones de soporte o nuevas prácticas o cambios de organización.

6. Participar sobre todo en el programa de pruebas del Plan de Recuperación (PRD) para los Servicios tecnológicos.

8. CAPACITACIÓN Y PRUEBAS

8.1 Plan de Pruebas

Objetivo General:

Validar que los procedimientos, acciones, y estrategias de recuperación sean eficaces y suficientes para que los Grupos de Recuperación PRD puedan restablecer los Servicios tecnológicos y Comunicaciones y lograr la continuidad de las operaciones ante una contingencia mayor o catastrófica.

Objetivos Específicos:

- Verificar el nivel de coordinación y comunicación de los integrantes de los Grupos de Recuperación.
- Verificar la funcionalidad de los procedimientos de activación del plan, la respuesta a la emergencia, de recuperación y el nivel de preparación del personal que participará en las actividades.
- Verificar que los usuarios de las aplicaciones críticas puedan operar en el Centro Alterno de Trabajo y en los tiempos definidos.
- Validar que los recursos definidos en el MARC cubran las necesidades de operación en modo contingente y de recuperación.

Alcance:

- El alcance, fecha y tipo de prueba a realizarse, se definirá antes de la prueba y se tomará como base el nivel de preparación del DADEP de acuerdo con la estrategia que se defina.

- Sobre la base a dicha definición, se armará el escenario y se elaborará el programa de pruebas.

8.2 Estrategia de la Prueba:

La prueba estará relacionada con las estrategias definidas por el DADEP para la recuperación de la operación normal.

Los Grupos de Recuperación del DADEP intervendrán en el desarrollo de la prueba y en la validación de los resultados. Las funciones y responsabilidades de los participantes se definirán por cada Grupo antes de la misma.

Como responsables de la Coordinación General, participarán el Grupo de Recuperación y los líderes de cada Grupo, involucrados en el desarrollo del Plan.

Dentro del ámbito de responsabilidad de cada participante, se asume un trabajo en equipo, debiendo ser responsabilidad de todos los participantes proporcionarse apoyo mutuo para el logro de los objetivos.

Los procesos, procedimientos, personal, hardware, software y demás recursos que se utilizarán en las pruebas se definirán cuando se desarrolle el programa de pruebas.

8.3 Documentación de la Prueba

Los líderes de cada Grupo de Recuperación y el líder del Grupo de Recuperación llevarán un registro de los resultados desde el inicio hasta el fin de la prueba realizada. Los resultados servirán de base para la corrección y perfeccionamiento del Plan de Recuperación (PRD) en general y de los procedimientos de respuesta y recuperación en particular.

Elaboró: Juan Nicolás Ayala
Revisó: Guiomar Cortés Ávila
Aprobó: Syrus Pacheco
Código de archivo: 140

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
1	29/06/2021	Versión inicial