2018

PLAN DE RECUPERACIÓN DE DESASTRES

Escuela Superior de Administración Pública

Oficina de Sistemas e Informática

1-6-2018

FIRMAS Y REVISIONES

TITULO	PLAN DE RECUPERACIÓN DE DESASTRES
AUTOR	Oficina de Sistemas e Informática - OSI
TEMA	Seguridad y Privacidad de la Información
FECHA DE ELABORACIÓN	Junio de 2018
FORMATO	PDF
VERSIÓN	1.0
PALABRAS RELACIONADAS	Sistema de Gestión de Seguridad de la Información – SGSI, Modelo de Seguridad y Privacidad de la Información – MSPI, Plan Estratégico de Tecnologías de Información y Comunicación – PETI, Plan de Seguridad Y Privacidad de la Información, Políticas, Confidencialidad, Integridad, Disponibilidad y Privacidad, Análisis de Impacto al Negocio,

CONTROL DE CAMBIOS

NOMBRE	VERSIÓN	AUTOR	FECHA
PLAN DE RECUPERACIÓN DE DESASTRES	1.0	Oficina de Sistemas e Informática - OSI	JUNIO DE 2018

COMITÉ	ACTA DE APROBACIÓN	FECHA
Comité Institucional de Gestión y Desempeño	Acta No. 03	**06 de Noviembre de 2018**

Contenido

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

Un DESASTRE se define como un evento repentino no planeado que ocasiona la “no disponibilidad” de los servicios informáticos por un tiempo tal que, para restablecer estos servicios, es necesario utilizar facilidades alternas de cómputo y comunicaciones en otra localidad.

Para poder restablecer estos servicios se hace necesario planear, desarrollar, probar y llevar a cabo procedimientos que aseguren la recuperación de estos servicios, documentando las estrategias, personal, procedimientos y recursos que serán utilizados para responder ante interrupciones que afecten los servicios de cómputo y comunicaciones.

El Plan de Recuperación (DRP) para los servicios de cómputo y comunicaciones es responsabilidad primaria de la ESAP, sin embargo, es la oficina de Sistemas e Informática la que tiene la responsabilidad de su desarrollo, mantenimiento y ejecución.

La necesidad de considerar un plan para recuperar los servicios de cómputo se desprende tanto de la posibilidad de un incidente que interrumpa la operación normal de la ESAP por un corto período, como de eventos catastróficos que impidan la continuidad del negocio.

1.1. Cómo usar este Plan

Este documento ofrece un panorama general de la estructura del plan, los objetivos, el alcance, las premisas iníciales, las estrategias predeterminadas, y las acciones para la recuperación de los Servicios de Cómputo. Las distintas fases, las tareas y los procedimientos deben ser revisados y seguidos con base en las circunstancias específicas de la contingencia. Además, el Plan debe seguirse cuidadosamente durante los ejercicios periódicos de prueba para entrenar concienzudamente al personal de recuperación y asegurar que las estrategias y acciones reflejen precisamente los requerimientos de recuperación de los Servicios de Cómputo a su condición operativa.

1.2. Objetivos

Este Plan de Recuperación fue desarrollado para alcanzar los siguientes objetivos específicos:

- Dar continuidad a los servicios informáticos de la ESAP en caso de presentarse una situación de contingencia mayor o catastrófica.

- Proveer un enfoque organizado para el manejo de las actividades de respuesta y recuperación luego de un incidente no planeado o de una interrupción prolongada de los servicios de cómputo, con el objeto de evitar confusión y reducir la probabilidad de error.

- Ofrecer respuestas oportunas y apropiadas a cualquier incidente no planeado, reduciendo así el efecto de una interrupción de los servicios de cómputo.

- Recuperar las aplicaciones críticas del negocio de una manera oportuna, incrementando la habilidad de la compañía para recuperarse de una pérdida o daños a las instalaciones y servicios.

1.3. Premisas

Este Plan de Recuperación será activado por la Oficina de Sistemas e Informática la cual se basa en dos premisas básicas:

- No se tiene acceso a las instalaciones físicas del Centro de Cómputo de la ESAP
- No se tiene acceso a algunos de los Servicios Críticos del Centro de Cómputo, en las instalaciones de la ESAP

En ambas instancias, la activación del Plan de Recuperación será considerada cuando el reporte de evaluación de daños indique que el tiempo estimado de acceso a las instalaciones o de disponibilidad de los servicios informáticos sea mayor a 8 horas. En ese punto se dará inicio a las actividades de recuperación de las aplicaciones críticas con los equipos de respaldo de acuerdo a la estrategia de acción definida en la sección 3.3 de este Plan.

Las premisas secundarias son las siguientes:

- Las instalaciones del Centro de Cómputo de la ESAP se encuentran localizadas en la calle 44 con cra 54 - CAN, Bogotá, se encuentran inhabilitadas o no hay acceso.
- Las áreas de almacenamiento de respaldos y de los archivos críticos de información que se encuentran fuera de la ESAP están intactas y disponibles.
- Los respaldos de la información y la rotación de los medios son efectuados reduciendo al máximo la pérdida de datos por eventualidad, cumpliendo con el Tiempo Objetivo de Recuperación (RTO) y Punto Objetivo de Recuperación (RPO) definidos para la ESAP.

- Los recursos identificados en la sección 2 “Configuración de Recuperación Mínima Aceptable” (Minimum Acceptable Recovery Configuration), “MARC” por sus siglas en inglés) estarán disponibles para llevar a cabo los procedimientos de recuperación.
- Las estrategias de recuperación por plataforma y aplicación están totalmente implementadas y se han probado con regularidad.
- Las estrategias y acciones de recuperación de recursos han sido aprobadas, se encuentran disponibles, implementadas y también han sido comprobadas.

- La estrategia de recuperación de las comunicaciones ha sido probadas e implementada.
- Las organizaciones externas a la compañía como proveedores y contratistas cooperarán razonablemente durante el período de recuperación.
- Se ha efectuado con regularidad la revisión, el mantenimiento y las mejoras del plan, a fin de asegurar su viabilidad.
- Se ha llevado a cabo el programa de concientización y capacitación referente a este plan.
- Se han desarrollado y puesto a prueba las estrategias de ejecución del plan para asegurar la validez de los procedimientos documentados.

1.4. Alcance

Este Plan de Recuperación (DRP) para los Servicios de Cómputo y Comunicaciones en caso de Desastre (DRP), considera a las instalaciones de la ESAP ubicadas en el CAN.

El Plan incluye las acciones y procedimientos individuales, así como a los responsables de dar respuesta y recuperación de la operación normal de los servicios de cómputo y comunicaciones ante cualquiera de los siguientes escenarios:

- Cualquier incidente externo que pudiera causar una interrupción de los servicios de cómputo por un tiempo prolongado, como un corte en el servicio de Comunicaciones o fallas en el suministro eléctrico.
- Cualquier incidente que cause daño físico a las instalaciones, como incendio, temblor o inundación.
- Cualquier incidente que afecte indirectamente el acceso a las instalaciones, como una huelga, evacuación urgente a las instalaciones debido a una amenaza de bomba, o una amenaza externa como el incendio de algún edificio contiguo.
- Desastre regional no esperado tal como la erupción de un volcán, un terremoto o una inundación.
- Cierre de las instalaciones por recomendación de la Secretaría de Salud.

1.5. Conceptos y Definiciones

Con objeto de homogeneizar conceptos se presenta la definición de algunos términos utilizados en el documento:

DRP

Acrónimo de Disaster Recovery Plan (en inglés). Plan de Recuperación en caso de Desastre.

Un DRP es un 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 de cómputo, aplicaciones y comunicaciones que permiten

mantener la continuidad de las operaciones de la organización soportadas por las Tecnologías de la Información.

En un DRP, las unidades de negocio no son las responsables de restablecer los servicios de cómputo, aplicaciones y comunicaciones. El responsable es la Oficina de Sistemas e Informática.

Unidad de Negocio (UN)

Cualquier área de la empresa que realiza actividades que forman parte del ciclo educativo de la Institución. Generalmente son dependientes de la tecnología de cómputo, comunicaciones y de servicios de apoyo.

Aplicaciones Críticas

Son aquellas aplicaciones que soportan los procesos relacionados con la misión de la institución y dependiendo de su naturaleza, estarán orientados principalmente a la operación misma del negocio y a aquellas actividades relacionadas con el flujo educativo de la entidad. Ante una contingencia, las aplicaciones críticas no pueden postergar su operación por un tiempo prolongado.

Grupos de Recuperación.

Grupos de personas con perfiles, responsabilidades y habilidades específicas con el fin de encauzar esfuerzos para dirigir, coordinar y habilitar los elementos que permiten la operación de los procesos informáticos del negocio.

Grupo Coordinador.

Personas encargadas de coordinar y controlar las acciones a realizarse antes, durante y después de la contingencia, a través de los Grupos de Recuperación.

Líder de Grupo.

Persona responsable de un Grupo de Recuperación quién toma a su cargo la responsabilidad global de las funciones de ese grupo durante una contingencia.

Líder suplente de Grupo.

Persona que asume las funciones del líder del grupo en caso de que éste no se encuentre disponible

Centro Alterno de Trabajo (CAT)

Es un área de oficinas provisional donde se llevan a cabo las actividades del negocio en tanto se restablecen y recuperan las condiciones para la operación normal de la institución en sus oficinas principales.

Centro de Control de Crisis (CCC)

Es una zona de encuentro dentro o fuera de la empresa desde donde se llevan a cabo las actividades iniciales de evaluación, coordinación y de toma de decisiones relativas a un incidente no planeado.

MARC

Acrónimo de “Minimum Acceptable Recovery Configuration” (en Inglés). Configuración de Recuperación Mínima Aceptable. Término que comprende los elementos humanos y materiales que se requieren como mínimo para cumplir con las funciones críticas de operación de sistemas y del negocio.

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 actuaran antes, durante y después de una recuperación, se llevarán a cabo diversas actividades encaminadas a este fin

2.1. Situación Actual de los Servicios de Cómputo y Comunicaciones

Los sistemas de cómputo y comunicaciones se encuentran en las instalaciones de la ESAP ubicadas en el CAN

2.2. Diagrama de Comunicaciones

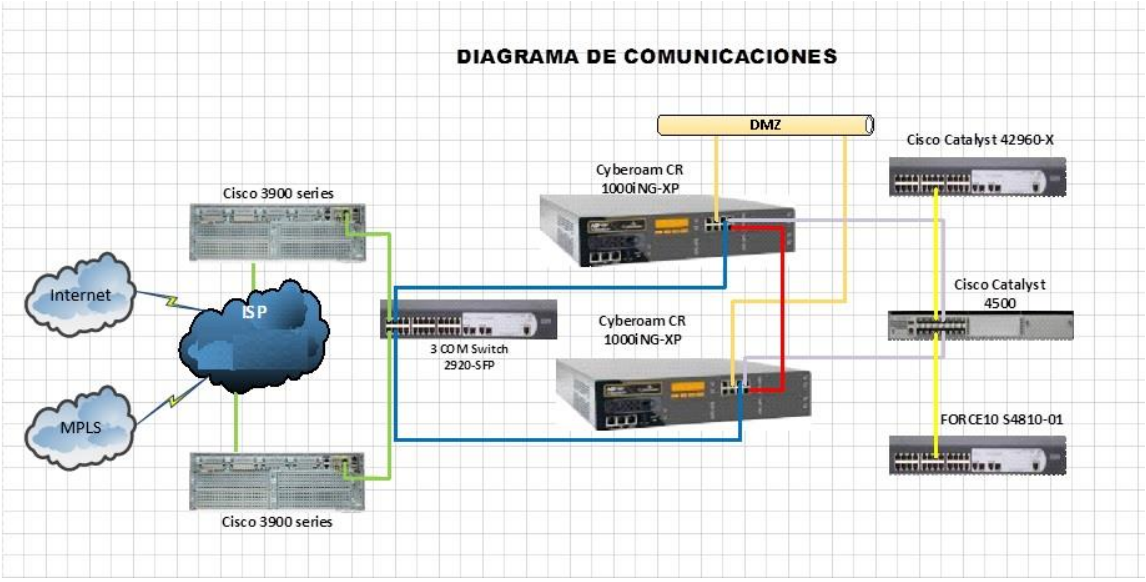


Ilustración 1. Diagrama de Comunicaciones

2.3. Topología de Red

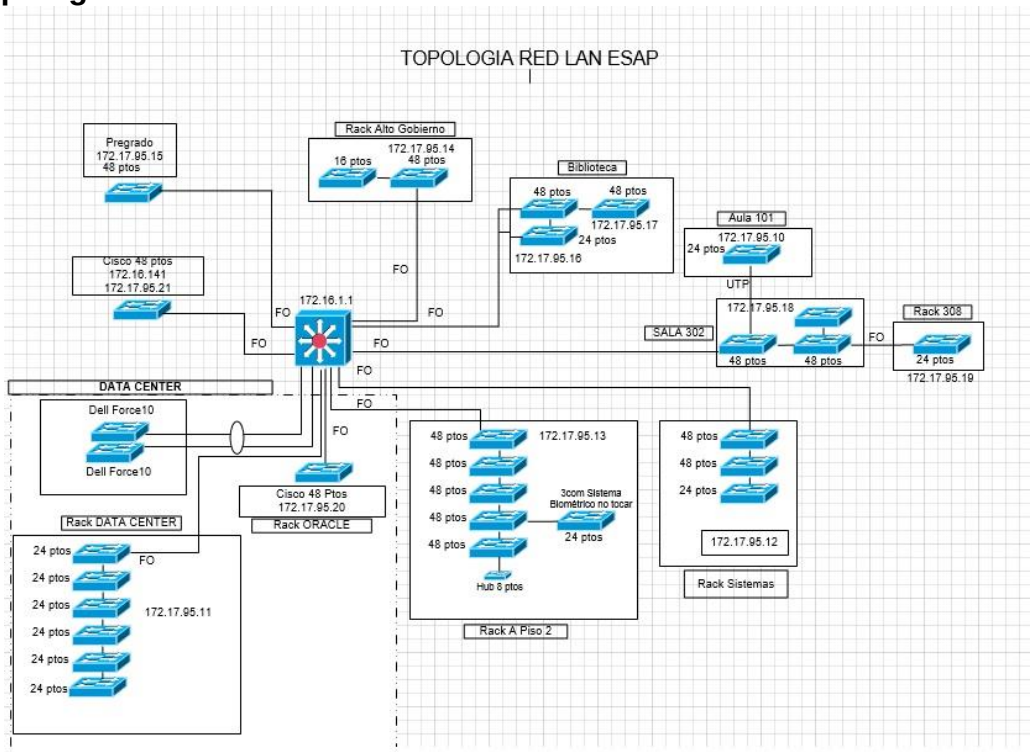
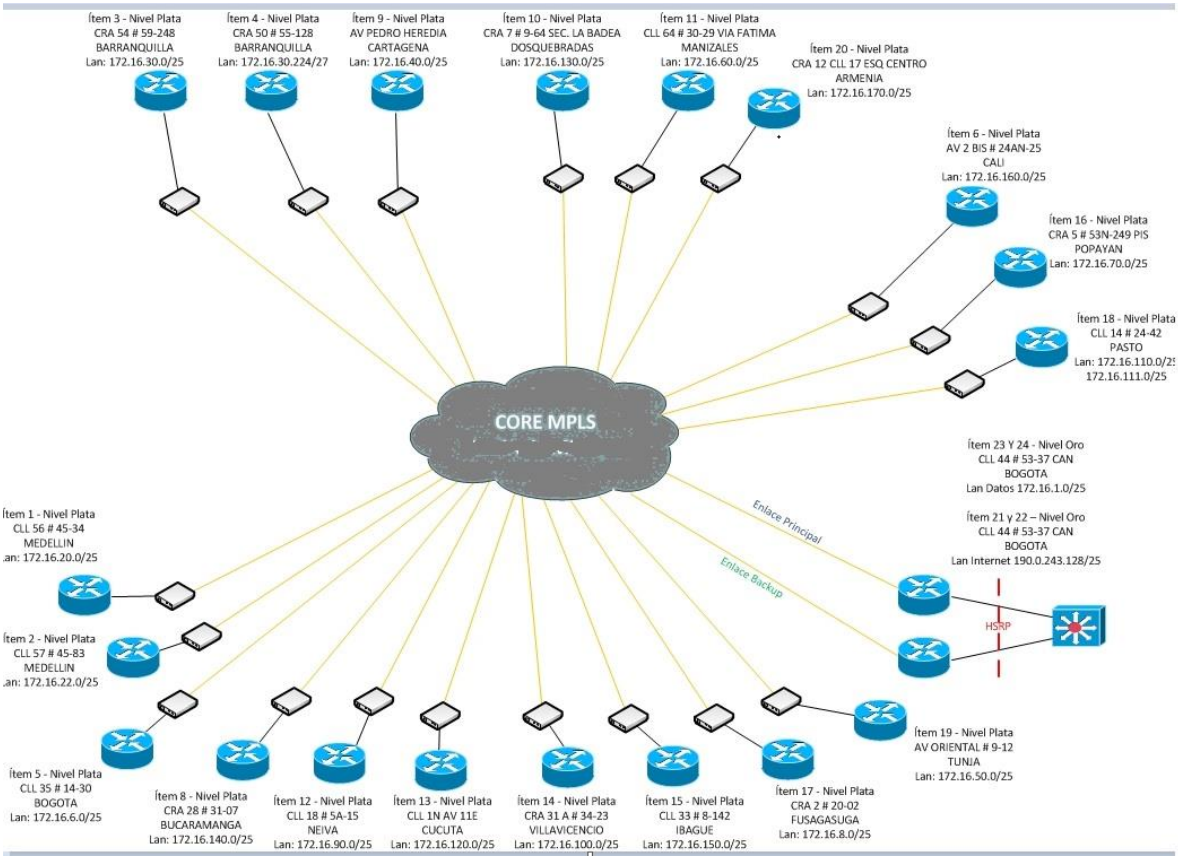


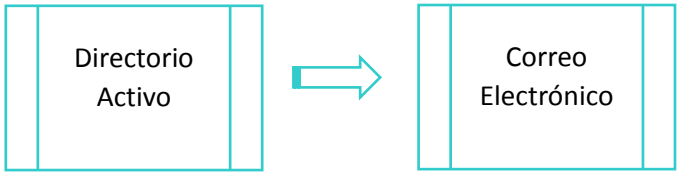
Ilustración 2. Topología de Red



2.4. Principales Plataformas y Aplicaciones

Las principales aplicaciones que soportan la operación de la ***ESAP*** se encuentran distribuidas en diferentes plataformas instaladas en las oficinas corporativas de la Institución, ubicadas en el CAN

2.5. Diagrama de Interrelación de Aplicaciones



2.6. Integración de los Grupos de Respuesta y Recuperación

Los Grupos de Recuperación han sido creados para el control y la coordinación de las actividades de respuesta y recuperación a un incidente no planeado. Está conformado por personal de las áreas de sistemas y unidades de negocio, a fin de responder a cualquier evento que se presente, mediante la participación en el desarrollo del plan y en las actividades de respuesta y recuperación de los servicios de cómputo y comunicaciones.

Estos Grupos se han integrado con base en las diferentes plataformas y por aplicaciones, de acuerdo a funciones o responsabilidades específicas. Cada uno de estos grupos tiene actividades asignadas a realizarse antes, durante y después de un evento. Sin embargo, cabe resaltar que las actividades previas son parte de una rutina a fin de mantener el plan preparado en cualquier momento. Los grupos definidos son:

- Comité Directivo
- Grupo Coordinador
- Grupo Operación Centro de Cómputo
- Grupo Servicios de Informática
- Grupo Telecomunicaciones
- Grupo Seguridad Informática
- Grupo Desarrollo de Sistemas
- Grupo Mesa de Ayuda
- Grupo Unidades de Negocio
- Un Vocero Oficial

2.7. Estructura del Grupo de Recuperación

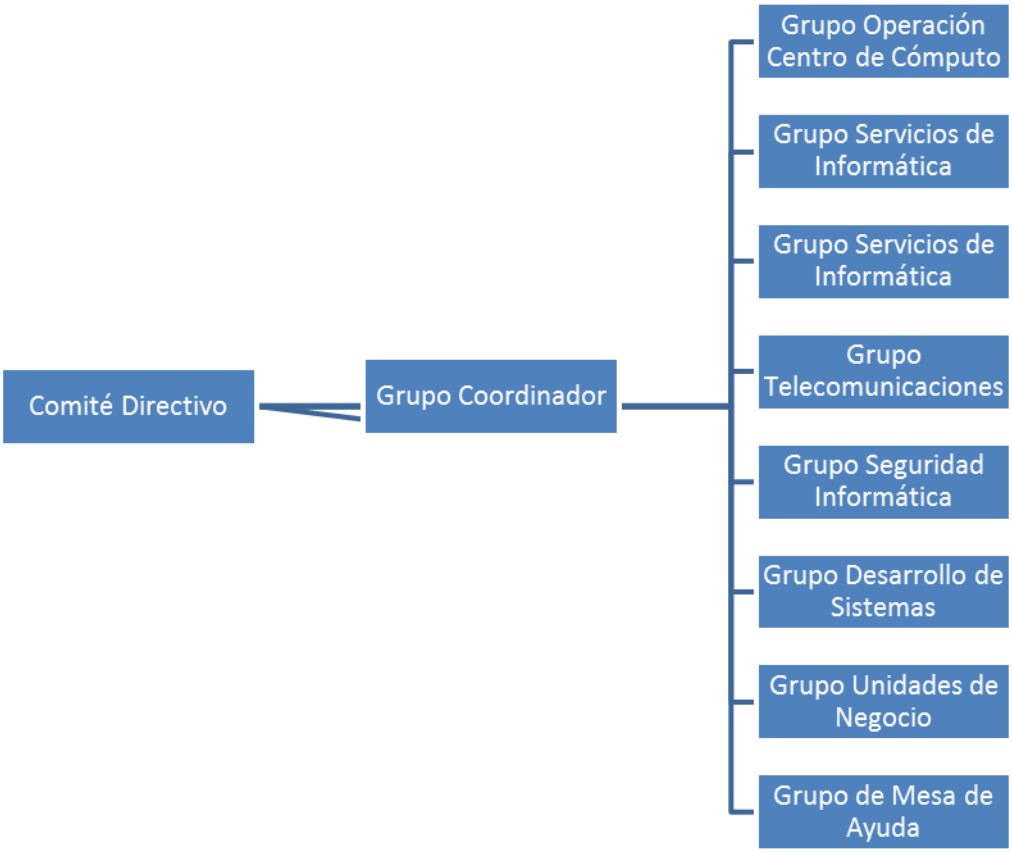


Ilustración 3. Estructura del Grupo de Recuperación

El objetivo principal de los Grupos de Recuperación, es realizar acciones de respuesta inmediata a cualquier evento que interrumpa la operación normal de los servicios de cómputo y toda actividad posterior relativa a la recuperación.

Estos Grupos serán los responsables de llevar a cabo acciones antes, durante y después de un incidente.

Las acciones antes del incidente se refieren a actividades que deben de ser efectuadas como parte de una rutina diaria, es decir, son prácticas orientadas a una preparación para enfrentar cualquier incidente y minimizar los riesgos e impactos que el evento pudiese causar.

Las acciones durante el incidente se refieren a las actividades efectuadas por los Grupos de Recuperación con sus funciones y responsabilidades específicas. Son ejecutadas justo después de ocurrido el incidente, como respuesta o atención inmediata. Por ejemplo, la detección y notificación del desastre o la evaluación preliminar de los daños y todas las tareas concernientes a la recuperación.

Las actividades después del incidente están encaminadas al retorno a la operación normal del negocio una vez restablecidos los servicios de cómputo, comunicaciones y restauradas las instalaciones del Centro de Cómputo primario.

2.8. Activación del Plan

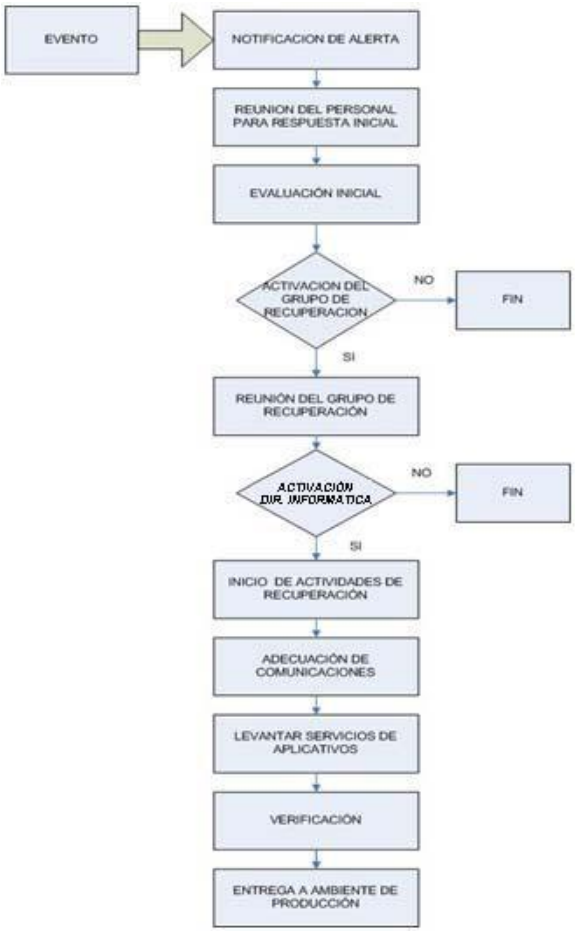


Ilustración 4. Activación del plan

2.9. Funciones de los Grupos de Recuperación

El Comité Directivo DRP jugará un papel específico en todo el proceso de recuperación al igual que cada uno de los grupos que lo integran.

El Comité Directivo DRP es responsable de las siguientes actividades generales:

- Determinar el momento preciso de la Declaración del Desastre con base a la evaluación inicial del incidente.
- Solicitar a la Dirección General, la aprobación para la adquisición del equipo y de los recursos necesarios para establecer y organizar las áreas alternas de trabajo y restablecer las oficinas principales.

El Grupo Coordinador, es responsable de las siguientes actividades generales:

- Coordinar y guiar el Plan de Acción para ese incidente en particular.
- Coordinar y ejercer la autoridad sobre las actividades de cada grupo de trabajo individual para asegurar la reanudación de las actividades del negocio dentro de los Tiempos Objetivos de Recuperación (RTO).
- Coordinar la restauración, reconstrucción y/o reemplazo de las instalaciones y equipo afectados.

Es importante notar que cada subgrupo que integra el Grupo de Recuperación, tiene a su cargo la implementación de su plan de recuperación además de ciertas responsabilidades comunes y/o equivalentes:

- Participar en las actividades iniciales de Recuperación y Respuesta
- Notificar y asignar personal de acuerdo al Plan de Acción.
- Participar en la evaluación de daños.
- Supervisar las operaciones en la localidad para la recuperación.
- Reportar la evolución del plan y los problemas a los Líderes de los Grupos de Recuperación para que a su vez informe al Grupo Coordinador DRP.
- Participar con los líderes de cada Grupo en la evaluación del proceso del Plan.
- Generar un reporte de evaluación final al concluir el proceso de recuperación**.**

2.10. Funciones del Vocero Oficial

- Contar con un mecanismo de evaluación de la opinión pública:

  El área o responsable de Relaciones Públicas deberá realizar diariamente una síntesis de las principales notas informativas de la prensa (programas de radio y televisión, prensa

escrita). Estos recursos permitirán tener un rápido conocimiento de lo que se difunde en el medio y actuar en consecuencia.

- Disponer de una política centralizada de comunicación:
  Desarrollar un plan global de comunicación. Este plan ha de ser ejecutado con acciones de comunicación dirigidas a los diversos destinatarios internos y externos. A saber:
  - Medios de comunicación (notas de prensa, discursos, etc.).
  - Público en general
  - Estudiantes
  - Empleados (charlas, entrenamiento para manejo de comunicación frente al cliente, etc.).
  - Entidades gubernamentales.
- Preparar un protocolo de comunicación de crisis interno y darlo a conocer los miembros de los Grupos de Recuperación (Guía del Vocero):
- De acuerdo al punto dos, NO USAR LA PALABRA CRISIS Utilizar otras palabras como “Situación potencialmente”
- Coordinar toda comunicación que se realice con los medios de prensa, clientes, proveedores y entidades gubernamentales:
  El área o responsable de Relaciones Públicas deberá estar a cargo de la redacción, producción y difusión de las cartas, notas de prensa, comunicados internos y charlas que se tengan sobre el tema.
  - Revisar y aprobar las declaraciones oficiales relacionadas con el incidente:

2.11. Funciones del Líder del Grupo Coordinador

Las responsabilidades fundamentales del Líder del Grupo Coordinador son:

- Coordinar la evacuación de las Instalaciones.
- Coordinar la evaluación de la situación debida al incidente.
- Autorizar la activación del Grupo de Respuesta y Recuperación.
- Evaluar el impacto y cálculo de los daños físicos.
- Coordinar el desarrollo del Plan de Acción.
- Coordinar las actividades de soporte centralizadas.
- Dirigir las operaciones generales de los Grupos de Recuperación.

Además, el Líder notificará de inmediato al Grupo Coordinador, la interrupción o probable interrupción por un período mayor a 8 horas, de las funciones normales del negocio a causa de un incidente no previsto.

Luego de haber transmitido la notificación inicial al Grupo Coordinador y de acuerdo a la magnitud del evento, el Líder del Grupo Coordinador se pondrá en contacto con los Líderes de los Grupos de Recuperación, a fin de que se reporten al Centro de Control de Crisis. Conforme continúe el proceso de recuperación, el Líder dará instrucciones a los Líderes de los Grupos de Recuperación, para poner en funcionamiento a cada uno de estos o ubicarlos bajo el estatus de reserva.

Las responsabilidades del Líder del Grupo Coordinador son:

- Recopilar, organizar, y documentar la información referente al incidente y a la respuesta correspondiente y a los requisitos para la recuperación, por ejemplo, definir los lugares de reunión de los Grupos de Recuperación, que se deberán de poner en funcionamiento.
- Asistir a los Líderes de los Grupos de Recuperación en el desarrollo, revisión y documentación del Plan de Acción.
- Mantener y difundir los reportes del estatus de la contingencia.
- Establecer y poner en marcha el Centro de Control de Crisis.
- Recopilar y documentar la información referente al incidente.
- Conservar registros por escrito de la contingencia y del estatus de recuperación.
- Coordinar el trabajo de recuperación entre los Grupos.
- Coordinar pruebas del Plan y la capacitación del personal.
- Mantener actualizado el Plan

Las responsabilidades del Grupo Coordinador

El Grupo Coordinador, está integrado por los líderes de los grupos de recuperación que atenderán las acciones necesarias de respuesta y suministrarán el apoyo centralizado para las actividades de recuperación.

En particular, el Grupo Coordinador es responsable de recopilar y difundir la siguiente información al Comité Directivo:

- El estatus de las actividades de respuesta urgente
- La descripción de la contingencia
- Presentar un reporte de los daños a las instalaciones y equipo de sistemas
- Áreas del negocio afectadas
- Atención/reacción de los clientes, proveedores y entidades externas
- Estatus actual del Plan de Acción

2.12. Resumen de Actividades

Actividades de preparación:

- Determinar la Configuración Mínima Requerida de Equipos de Cómputo y Comunicaciones (MARC).
- Revisar y validar las aplicaciones que soportan las funciones críticas de la institución.
- Definir las políticas y procedimientos de respaldo y recuperación de software, datos, equipos y comunicaciones para restaurar las funciones críticas de la institución.
- Elaborar y mantener un directorio de proveedores de bienes y servicios informáticos.
- Participar con el área responsable de contratos en el mantenimiento y vigencia de los contratos o convenios establecidos con estos proveedores para atender necesidades inmediatas en casos de desastre.

Actividades de Respuesta y Recuperación:

- Participar en la evaluación de daños en la infraestructura tecnológica, en los sistemas y en las comunicaciones.
- Estimar el tiempo de reparación o reemplazo de equipos y/o sistemas afectados por una contingencia o que presentan fallas.
- Coordinar el rescate de equipos para que no sufran mayor daño.
- Montar y organizar los equipos y sistemas en el Centro de Cómputo o instalaciones Alternas de Trabajo.
- Restaurar y/o reconstruir archivos vitales.
- Reanudar los servicios de cómputo y comunicaciones que soportan los procesos identificados como críticos, tanto de oficinas corporativas como de las oficinas operativas, regionales y estatales.
- Asistir en la recuperación de los datos protegidos de las computadoras personales y de las redes locales.
- Coordinar la distribución de equipos necesarios para activar la operación en el Centro de Cómputo o instalaciones Alternas de Trabajo.
- Preparar equipos e instalar los clientes de las aplicaciones en el Centro de Cómputo o instalaciones Alternas de Trabajo.
- Restablecer el acceso a la red local y a los sistemas de cómputo centralizados.
- Obtener los datos protegidos (Back-up) conservados fuera de la empresa.
- Contactar a los proveedores de bienes y servicios de Infraestructura Tecnológica que sean necesarios para apoyar la recuperación.
- Coordinar todas las actividades de soporte para la restauración del Centro de
- Cómputo afectado.
- Coordinar la reinstalación del Centro de Cómputo afectado una vez que ha sido restaurado.
- Coordinar con todos los Grupos de Recuperación una reunión de evaluación del proceso del Plan.
- Generar un reporte de evaluación del Plan al Comité Directivo de la Organización y a la Dirección General.

2.13. Integrantes de los grupos de Recuperación

Para cada grupo se requiere la siguiente información

NOMBRE	CARGO	DEPENDENCIA
FRANCO DOMÍNGUEZ CLAUDIA MARCELA (Encargada)	DIRECTOR NACIONAL	DESPACHO DIRECCIÓN NACIONAL
PEDREROS PINZON MARIA MAYERLY	JEFE DE OFICINA	OFICINA DE CONTROL INTERNO
LIZARAZO ARAQUE BETTY CONSTANZA	JEFE DE OFICINA ASESORA	OFICINA ASESORA JURÍDICA
HERNANDEZ RUIZ LUZ STELLA	JEFE DE OFICINA ASESORA	OFICINA ASESORA DE PLANEACIÓN
ORTIZ SALGADO MARIO ALEXANDER	JEFE DE OFICINA	OFICINA DE SISTEMAS E INFORMÁTICA
GALEANO JIMÉNEZ MARYURI ROCIO	SECRETARIO GENERAL	SECRETARIA GENERAL
RAMÍREZ MÉNDEZ CLAUDIA INES	SUBDIRECTOR GENERAL DE ENTIDAD DESCENTRALIZADA	SUBDIRECCIÓN ACADÉMICA
CRUZ MARTINEZ ALEXANDER	SUBDIRECTOR GENERAL DE ENTIDAD DESCENTRALIZADA	SUBDIRECCIÓN DE PROYECCIÓN INSTITUCIONAL
BERNAL SANCHEZ OSWALDO	SUBDIRECTOR GENERAL DE ENTIDAD DESCENTRALIZADA	SUBDIRECCIÓN DE ALTO GOBIERNO

2.14. Análisis de Procesos y Aplicaciones.

Como parte preliminar al desarrollo del Plan de Recuperación (DRP) para los Servicios de Cómputo, fue necesario realizar un análisis de aplicaciones y definición de requerimientos, con objeto de determinar las aplicaciones que soportan procesos de misión crítica y la interrelación entre aplicaciones. El propósito fue examinar la composición de los procesos, la dependencia de estos en las aplicaciones para definir la prioridad de las aplicaciones a recuperar y los requerimientos mínimos necesarios (MARC).

La vulnerabilidad en los procesos del negocio se determinó asumiendo la pérdida de los sistemas críticos debido a una contingencia mayor o catastrófica interrumpiendo la operación normal de la operación.

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

Grado de Criticidad	Descripción
1	Aplicación con tolerancia mínima que requiere recuperarse de forma inmediata (< a 8 horas)

Grado de Criticidad	Descripción
2	Aplicación que debe levantarse en menos de 12 horas después de la declaración del desastre
3	Aplicación que puede levantarse en menos de 24 horas
4	Aplicación que puede levantarse después de 24 horas

En caso de que ocurriera un desastre que afectara el acceso a las instalaciones o a los servicios del Centros de Cómputo de LA ESAP, las aplicaciones que soportan los procesos críticos para la operación del negocio no podrían llevarse a cabo, afectando así la continuidad de la operación.

De acuerdo a los resultados obtenidos en el Análisis, el impacto causado por la interrupción de la operación del negocio, tanto a corto como a largo plazo, puede ser catastrófico, particularmente si el desastre ocasiona pérdida de información y de los servicios de procesamiento de datos.

El hecho de no contar con una estrategia preestablecida para recuperar las operaciones de las aplicaciones y servicios críticos y los procesos relacionados en un tiempo determinado, provocaría altas pérdidas financieras para LA ESAP representada principalmente en pérdida de ingresos y costos de oportunidad. Así mismo, se presentarían graves problemas en la operación, y su imagen se vería deteriorada a nivel nacional por la falta de los servicios de procesamiento de datos y de comunicaciones.

2.15. Estrategia de Recuperación de aplicaciones.

Considerando las necesidades de recuperación de la **ESAP** y de acuerdo a los resultados del Tiempo objetivo de Recuperación (RTO) definidos por las diversas Unidades de Negocio, 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 a través de una copia remota de las bases de datos y aplicaciones que puedan entrar en operación en una localidad alterna con instalaciones de cómputo disponibles capaces de operar de manera inmediata.

Hot Site Comercial: Aplica para aquellas aplicaciones que resultaron con un RTO entre 24 y 48 horas. Este esquema deberá considerarse a través de servicios de Hot Site comercial que ofrezca un lugar alternativo que tenga a disposición computadoras, telecomunicaciones, e infraestructura requerida para recuperar los procesos y aplicaciones críticas garantizando el tiempo de recuperación establecido por el RTO.

Adquisición de equipo adicional o actualizar 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, de acuerdo a la estrategia definida para la **ESAP** en el documento de presentación entregado como parte complementaria del reporte del EBIA.

Independientemente del Plan de Recuperación, la relación de aplicaciones y su nivel de criticidad, los recursos requeridos, los Grupos de Recuperación y los procedimientos documentados, la estrategia deberá quedar definida y documentada para estar en condiciones de ser probada y considerar que se puede lograr una recuperación exitosa.

2.16. Recuperación de los Servicios Críticos.

Para el caso de los servicios de Tecnología de Información que fueron identificados como críticos, se tienen los siguientes:

EQUIPO	FUNCIONARIO PRINCIPAL	CARGO	ROL (Líder, Integrante)	FUNCIONARIO ALTERNO	CARGO
INFRAESTRUCTURA	Josue Valenzuela	Responsable Infraestructura	Líder	Jairo Alexander Gomez	Responsable Infraestructura
	Jairo Alexander Gomez	Responsable Infraestructura	Integrante	John Montenegro	Responsable Infraestructura
	John Montenegro	Responsable Infraestructura	Integrante	Josue Valenzuela	Responsable Infraestructura
TELECOMUNICACIONES	Josue Valenzuela	Responsable Telecomunicaciones	Líder	Carlos Castro	Responsable Telecomunicaciones
	Carlos Castro	Responsable Telecomunicaciones	Integrante	Josue Valenzuela	Responsable Telecomunicaciones
BASES DE DATOS	Raul Ricardo Rubio	Responsable Bases de Datos	Líder	Mario Ortiz	Jefe Oficina Sistemas e Informática
APLICACIONES	Mario Ortiz		Líder		
	Carolina Vargas	Responsable Arca	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Mayerli Caro	Responsable Seven	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática

EQUIPO	FUNCIONARIO PRINCIPAL	CARGO	ROL (Líder, Integrante)	FUNCIONARIO ALTERNO	CARGO
	Sadi Sanchez	Responsable Gestasoft	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Diego Bertel	Responsable Portal WEB	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Gino Piñeros	Responsable Humano WEB	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Jenifer Carolina Cuellar	Responsable Sirecec	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Jenifer Carolina Cuellar	Responsable Concursos y Convocatorias	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Jenifer Carolina Cuellar	Responsable Moodle	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Diego Bertel	Responsable Intranet	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Jairo Rodriguez	Responsable OLIB	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Gino Piñeros	Responsable ISOLUCION	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Diego Bertel	Responsable MI CLIP	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Melkin Mejia	Responsable Lime Survey	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Maria Fernanda Guerrero	Responsable Service Manager	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Jairo Rodriguez	Responsable Sistema Satelital	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática
	Jairo Rodriguez	Responsable Streaming	Integrante	Mario Ortiz	Jefe Oficina Sistemas e Informática

EQUIPO	FUNCIONARIO PRINCIPAL	CARGO	ROL (Líder, Integrante)	FUNCIONARIO ALTERNO	CARGO
Seguridad	Daissy Mesa	Responsable Oficial de Seguridad	Líder	Mario Ortiz	Jefe Oficina Sistemas e Informática
Mesa de Ayuda	Maria Fernanda Guerrero	Responsable Mesa de Ayuda	Líder	Mario Ortiz	Jefe Oficina Sistemas e Informática

2.17. Análisis de Protección de la Información y de Ambiente de TI.

Para asegurar el éxito de cualquier Plan de Recuperación (DRP) para los Servicios de

Cómputo en Caso de Desastre y más específicamente para llevar a cabo las estrategias de recuperación contenidas en dicho plan, es necesario que se cuente con los procesos de respaldo, resguardo y recuperación de información necesarios que permitan reanudar los servicios de cómputo críticos en una localidad alterna, en los tiempos requeridos y con los niveles de servicio acordados.

Para tal efecto, se realizó un “Análisis de Protección de la información”. El objetivo de este estudio fue el siguiente:

“Conocer los procedimientos, organización, ubicaciones, equipos y componentes que intervienen en el resguardo, protección y recuperación de la información residente en los equipos de cómputo y en los medios de almacenamiento magnético, de manera que la **ESAP**, pueda orientar los esfuerzos y acciones necesarias para asegurar la capacidad de recuperación de los servicios de cómputo en caso de desastre”.

Los resultados de este trabajo se entregan por separado en el documento denominado

“Reporte de Análisis de Protección de la Información”.

En este reporte se integra información de detalle acerca de las prácticas de respaldos de LA ESAP.

El trabajo incluyó la revisión de lo siguiente:

- Que los Procedimientos de creación de respaldo de las aplicaciones incluyan corridas con las frecuencias necesarias de acuerdo a los Tiempos Objetivo de Recuperación (RTO) definidos, de manera que faciliten la recuperación de la información al mismo tiempo que minimicen el riesgo potencial de pérdida de datos.
- Frecuencias de rotación de datos de respaldo fuera de sitio.
- Diferenciación de los respaldos realizados con fines de recuperación de los respaldos mantenidos en sitio para recuperación de problemas locales o reprocesos.
- Capacidad para asegurar la recuperación del ambiente de cómputo en los Tiempos Objetivo de Recuperación (RTO) definidos.
- Procedimientos de restauración coordinados.
- Procedimientos de registro, custodia, seguridad y transporte de respaldos en sitio y en las instalaciones de almacenamiento externo.
- Realización de Pruebas de los procedimientos de respaldo y recuperación a fin de asegurar la integridad de los respaldos y la capacidad para soportar una recuperación completa.

- Programa de mantenimiento efectivo para asegurar la actualización periódica de los procedimientos de respaldo ya que el éxito de la recuperación de información está directamente relacionado con la calidad del esfuerzo dedicado al mantenimiento.

En este análisis se identifican los riesgos potenciales que pudieran afectar las estrategias de recuperación de los sistemas críticos y se proporcionan recomendaciones específicas y generales para la prevención y mitigación de dichos riesgos. En forma complementaria se realizó un análisis del ambiente de Tecnología de Información para identificar posibles riesgos para que la **ESAP** pueda trabajar en prevenirlos y mitigarlos.

2.18. Inventario para apoyo en la recuperación

Considerando la Estrategia de Recuperación definida y las aplicaciones que soportan los procesos de negocio críticos, se definieron los recursos mínimos de recuperación tanto de las Unidades de Negocio como los de Informática. Por lo anterior se muestra el inventario total del centro de cómputo principal, en donde se muestran los equipos con los que actualmente se cuenta

3. ESTRATEGIA GENERAL

3.1. Estrategia de Recuperación

Tal como se mencionó en las premisas de planeación identificadas anteriormente, este Plan de Recuperación está basado en el hecho de que no hay acceso a los servicios de cómputo centrales o las instalaciones donde se ubica el Centro de Cómputo han sido inhabilitadas o estarán inaccesibles por completo por un período inaceptable.

Las estrategias a 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 exhaustivo para determinar las acciones específicas que deberán seguirse de acuerdo al tipo de incidente.

3.2. Niveles de Contingencia

Es necesario tomar en cuenta que para cada situación contingente corresponde una respuesta específica. A continuación, presentamos una clasificación dependiente del nivel de contingencia:

- Contingencia Menor. - Provocada por eventos que afectan a una o varias Unidades de Negocio por un período corto pero que no afectan a toda la organización.

- Contingencia Mayor. - Provocada por incidentes que afectan el acceso a los servicios de cómputo y comunicaciones interrumpiendo la operación normal de la empresa por un periodo mayor a 24 horas.
- Contingencia Catastrófica. - Desastre que provoca una interrupción de la operación normal de una organización por un periodo prolongado provocando impactos de alto riesgo de permanencia de la organización.

Las contingencias Mayor y Catastrófica son los escenarios sobre los cuales se activa el Plan de Recuperación.

3.3. Estrategia de Acción

Las estrategias y planes de acción considerados para la recuperación de la **ESAP** han sido orientados a cubrir cualquier contingencia mayor o catastrófica que inhabilite el acceso del personal al edificio donde se ubican el Centro de Cómputo, o a los servicios de cómputo y comunicaciones en que se apoyan las Unidades de Negocio para operar las aplicaciones y procesos críticos.

La decisión para desarrollar dicha estrategia se basó en las características de operación actual de la **ESAP** y el nivel de dependencia de estas áreas en la tecnología de cómputo y comunicaciones.

Los planes y acciones a seguir dependerán del tipo de contingencia que se presente:

Contingencia Menor:

En caso de presentarse una contingencia menor, ésta podrá ser subsanada o corregida rápidamente por medio de los mecanismos de detección, diagnóstico y reparación de fallas, activando los procedimientos de atención de problemas utilizados día a día por la Oficina de Sistemas e Informática de la ESAP.

Contingencia Mayor:

De presentarse una contingencia mayor en los equipos y sistemas de las oficinas del CAN. que interrumpa la operación normal de los servicios de cómputo y comunicaciones, ésta deberá ser identificada y corregida a la brevedad. Si el tiempo estimado de reparación que determine el Grupo responsable de la aplicación o recurso técnico crítico excede de 8 horas, se deberá tomar la decisión de activar el Plan de Recuperación para los Servicios de Cómputo en Casos de Desastre (DRP).

Contingencia Catastrófica:

Si se presenta un incidente que provoque una Contingencia Catastrófica y que por consiguiente interrumpa las operaciones de la ESAP en sus oficinas del CAN por un período que se espera excederá de 24 horas, el Comité de Dirección DRP, declarará el desastre y activará, a través del Grupo de Respuesta y Recuperación a los líderes de cada Grupo y a los Grupos de Trabajo necesarios para la recuperación inmediata de los servicios de cómputo y comunicaciones de acuerdo a la estrategia definida.

Una vez activado el Plan de Recuperación, el Grupo Coordinador y los líderes de cada Grupo se reunirán en el Centro de Control de Crisis indicado en la sección 3 para sesionar y tomar decisiones acerca de la recuperación.

El tiempo de restablecimiento de los servicios informáticos de la ESAP en sus plataformas principales donde radican las aplicaciones y procesos críticos, será menor a 8 horas de acuerdo a la Estrategia de Recuperación definida.

En caso de un incidente que afecte el Centro de Cómputo por períodos prolongados:

- El personal del Centro de Cómputo efectuará inmediatamente respaldos de emergencia y procedimientos de apagado, si el tiempo y la seguridad lo permiten.
- Los Grupos de Recuperación ayudarán en la evaluación de daño del equipo, restauración de Comunicaciones y en la evaluación de las condiciones del Centro de Cómputo afectado.
- Los cartuchos de respaldo recuperadas en sitio (siempre que sea posible) y de la bóveda externa serán utilizadas para la recuperación de datos a la brevedad posible.
- Las aplicaciones y servicios de criticidad 1,2 y 3 serán restablecidas de acuerdo a las estrategias de recuperación y en los Tiempos Objetivos de Recuperación (RTO) definidos. Todas las otras aplicaciones que no fueron definidas como críticas, serán restablecidas después de 48 horas.

3.4. Centro de Control de Crisis (CCC)

El Centro de Control de Crisis (CCC) es una zona de reunión local o fuera de la institución desde donde las actividades iniciales de evaluación, coordinación y de toma de decisiones se llevan a cabo. El Centro de Control de Crisis alberga al Grupo Coordinador y a los Grupos de Recuperación durante las fases iniciales de respuesta y recuperación.

En caso de un incidente, la activación del Centro de Control de Crisis será necesario para llevar a cabo las actividades de respuesta y de recuperación. Este punto de reunión fue establecido con anterioridad y debe de tener el equipo necesario de comunicación para el control centralizado de las actividades de recuperación. El líder del Grupo Coordinador, basado en la magnitud de la contingencia, selecciona esta ubicación en el momento de la contingencia.

Si después de la evaluación del incidente, se estima que la recuperación de la operación normal se extenderá a más de 1 día y se decide ubicar a las áreas de negocio con aplicaciones críticas en los Centros Alternos de Trabajo, ubicar el Centro de Control de Crisis en un área de alguno de estos centros.

El Centro de Control de Crisis seleccionado, deberá de contar al menos con los siguientes recursos:

- Condiciones físicas adecuadas y espacio suficiente para todos los integrantes;
- Mobiliario y equipo de oficina
- Energía regulada
- Conexión a la LAN
- Impresora
- Al menos tres líneas telefónicas directas
- Conectividad Internet

Si el Centro de Control de Crisis se ubica temporalmente fuera de las instalaciones de la **ESAP**, el Grupo Coordinador y los integrantes de los Grupos de Recuperación deberán contar con teléfonos móviles o celulares cuyos números estén registrados en los directorios correspondientes.

3.5. Centro Alterno de Trabajo (CAT)

LA ESAP ha definido que su política de operación, en caso de que se tome la decisión de declarar un desastre y activar el Plan de Recuperación, consistirá en restablecer en forma inmediata las aplicaciones de Negocio identificadas como críticas y en una segunda instancia las otras aplicaciones de apoyo a la operación.

Después de obtener el reporte de evaluación de daños y el diagnóstico de restablecimiento sus oficinas del CAN, se tomarán las siguientes decisiones de ubicación de cada una de las áreas:

- Si se tiene acceso a las instalaciones, pero el Centro de Cómputo está dañado o no hay acceso a los sistemas de cómputo y comunicaciones y, se ha diagnosticado que el servicio de procesamiento de datos estará inactivo por un periodo mayor a 8 horas Se activará el Plan de Recuperación (DRP) para los servicios de Cómputo (DRP) y el personal que integran el Grupo Coordinador y los Grupos de Recuperación de cada plataforma que se considere necesario, se trasladarán al Centro de Cómputo alterno. El personal restante de sistemas y los usuarios con procesos críticos de las áreas de negocio continuará operando en las oficinas operativas.
- Si se estima que no habrá acceso a las instalaciones por un periodo mayor a 24 horas:

Se activará el DRP. El personal operativo identificado por cada Unidad de negocio crítica se trasladará al Centro Alterno de Trabajo a fin de continuar con sus actividades. El resto del personal deberá permanecer accesible y en constante comunicación con el líder o suplente del Grupo Coordinador o a la Mesa de Ayuda a los teléfonos que se indica en el directorio

Si el tiempo estimado para restablecer la operación normal en las oficinas del CAN es mayor a tres días, será necesario considerar la conveniencia de reubicar las Unidades de Negocio en salas de trabajo de Hoteles u Oficinas en Renta en forma temporal, mientras se instalan en nuevas oficinas y llevan a cabo las actividades de adaptación correspondientes.

3.6. Código de Notificación

Durante una contingencia es de vital importancia, que el personal conozca con claridad las actividades inmediatas de respuesta a un incidente. A continuación, aparece el Código de Notificación que utilizará la **ESAP** a fin de que todo empleado se conduzca con precisión al sitio que le corresponde.

“Prepararse para dar respuesta a una emergencia y activar los Grupos de Recuperación, por favor reportarse al Centro de Control de Crisis y posteriormente reportarse al Centro Alterno de Trabajo, Por favor permanezca localizable hasta nuevo aviso o repórtese a la mesa de ayuda.”

4. Actividades Previas a la Recuperación

Las actividades de los Grupos de Recuperación se dividen en actividades de Preparación y actividades de Respuesta y Recuperación.

Para que un Plan de Recuperación funcione adecuadamente, se requiere seguir ciertos pasos sencillos pero rutinarios con anticipación a lo que pueda suceder. Estas medidas preventivas se verifican y afinan con los procesos de pruebas.

Cada Líder de Grupo deberá ser responsable de que se sigan los pasos aquí indicados, a fin de que se mantengan actualizados los procedimientos y los recursos necesarios para la recuperación.

4.1. Tareas Previas del Grupo Coordinador.

El Grupo Coordinador deberá tomar las medidas y acciones necesarias para asegurar que los elementos que permitirán una adecuada recuperación se encuentren disponibles y poder enfrentar exitosamente cualquier incidente. Estas actividades deberán considerarse como tareas permanentes y con revisiones cada tres meses o ante cualquier cambio significativo en alguno de estos elementos:

- Apoyar a los líderes de cada grupo para que el Directorio de los Grupos de Recuperación se encuentre actualizado.
- Vigilar que el grupo de usuarios evalúe periódicamente la criticidad del portafolio de aplicaciones de la Empresa.
- Supervisar que el grupo de usuarios trimestralmente evalúe el portafolio de aplicaciones con base a los criterios de selección de aplicaciones críticas.
- Verificar que se definan los cambios en el portafolio de Aplicaciones Críticas en base al impacto en el negocio.
- Verificar que los cambios se documenten en el Plan de Recuperación.
- Asignar un responsable que se encargue de actualizar el plan.
- Apoyar a los Líderes de cada grupo para dar a conocer la mecánica de notificación de desastre al resto del personal.
- Verificar que el líder de cada grupo anuncie el desastre al personal que integra su Grupo.
- Supervisar que el directorio del personal crítico, teléfonos y direcciones particulares, teléfonos celulares y radio localizadores esté actualizado.
- Mantener actualizado los lugares de reunión del Comité Directivo en caso de desastre (Centro de Control de Crisis).
- Establecer las políticas de comunicación para la notificación del desastre.
- Asignar un número telefónico para que el personal involucrado en la recuperación de LA ESAP pueda recibir información de la contingencia.
- Establecer una política para comunicar el desastre a los niveles de Dirección.
- Definir el procedimiento de comunicación entre los Grupos.
- Obtener la información necesaria para mantener informado en forma constante al Comité Directivo.
- Solicitar al Comité Directivo que mantenga un presupuesto actualizado a ser ejecutado en caso de Desastre.
- Mantener a todo el personal de LA ESAP consciente de la necesidad de un Plan de Recuperación en caso de Desastre (DRP).
- Llevar a cabo juntas periódicas para mantener al personal motivado sobre la importancia del Plan.
- Nombrar a un suplente de los integrantes del grupo para operar en caso de ausencia del titular.
- Supervisar que el Centro de Cómputo Alterno esté totalmente operativo según requerimientos de recuperación.
- Coordinar la realización de al menos 2 pruebas anuales.

- Definir el objetivo y el alcance de las mismas.
- Coordinar las reuniones de trabajo para establecer procedimientos de mantenimiento del plan.
- Revisar y validar las estrategias y procedimientos.
- Determinar los procedimientos de almacenamiento y coordinar la seguridad y distribución del plan.
- Mantener respaldos del Plan en una localidad externa a la Empresa (bóveda).
- Definir donde estarán ubicadas las carpetas del Plan de Recuperación del Centro de Cómputo. Una carpeta será asignada al Director de Informática, otra al líder del Grupo Coordinador, otra a los líderes de cada Grupo y la cuarta en el lugar de almacenamiento externo.
- Capacitar al personal crítico de la empresa.
- Coordinar la capacitación de los integrantes de los grupos de recuperación para actuar de acuerdo a sus funciones y tareas definidas en el plan.
- Supervisar que el personal crítico susceptible a ser enviado al Centro Alterno de Trabajo esté identificado y pueda ser fácilmente localizado.
- Verificar la disponibilidad del mobiliario y equipo en el Centro Alterno de Trabajo.
- Equipo de oficina.
- Artículos varios.
- Establecer un plano de reubicación del Personal Crítico en el Centro Alterno de
- Trabajo.
- Asignar el área de trabajo a los usuarios de las aplicaciones críticas.
- Asignar el área de trabajo del personal crítico de sistemas.
- Coordinar y supervisar la elaboración y revisión periódica de las políticas y procedimientos de respaldo.
- Supervisar la ubicación de respaldos en bóveda.
- Verificar la seguridad de acceso.

4.2. Tareas Previas de los Grupos de Recuperación:

- Grupo Coordinador
- Grupo Operación Centro de Computo
- Servicios de Informática
- Grupo Comunicaciones
- Grupo Seguridad Informática
- Grupo Unidades de Negocio

Estos grupos deberán tomar las medidas y acciones necesarias para asegurar que los elementos de las aplicaciones, servicios de Informática y seguridad que permitirán una adecuada recuperación se encuentren disponibles y poder enfrentar exitosamente cualquier

incidente. Estas actividades deberán considerarse como tareas permanentes y con revisiones cada tres meses o ante cualquier cambio significativo en alguno de estos elementos.

- Definir un responsable del grupo que se encargue de mantener actualizado el plan. El cual va a ser actualizado de manera inmediata cada que haya cambios de equipos de cómputo, comunicaciones y de los servicios de informática. De no haber cambios de esta índole se hará una revisión obligatoria del plan cada 3 meses, haciendo las modificaciones necesarias para el plan de recuperación.
- Mantener actualizado el directorio del personal del área.
- Mantener actualizado el directorio de Proveedores.
- Nombrar un suplente del líder del grupo para que asuma sus responsabilidades en caso de ausencia del titular.
- Mantener actualizados los requerimientos mínimos de hardware, software y comunicaciones (MARC) para restablecer la operación en el Centro de Cómputo Alterno.
- Verificar la adecuada realización de los respaldos.
- Verificar que el procedimiento de respaldo diario y semanal de Bases de Datos y aplicaciones críticas termine exitosamente.
- Verificar que se obtengan juegos de los cartuchos de respaldo de datos por triplicado, ubicar una de ellas en el Site productivo, otra en la bóveda externa y la ultima en el Centro de Cómputo Alterno.
- Obtener respaldo del Sistema Operativo por triplicado cada vez que exista un cambio en la configuración. Ubicar un juego en el Sitio productivo, otra en la bóveda externa y el otro en el Centro de Cómputo Alterno.

- Obtener respaldo de perfiles de usuario, seguridad de acceso a usuarios a la información, configuración física y lógica cada vez que exista un cambio ubicar un juego en el Site productivo, otro en la bóveda externa y el otro del Centro de Cómputo Alterno.
- Confirmar que los procedimientos de respaldo y restauración sean operativos, funcionales, basados en media y compatibilidad y que se encuentren actualizados.
- Verificar el procedimiento de traslado y almacenamiento de los respaldos a la bóveda externa.
- Contar con manuales de operación.
- Mantener ubicados los manuales propios de la operación del equipo.
- Mantener una copia de los manuales de arranque del equipo en la bóveda externa y sitio alterno.
- Revisar mensualmente los procedimientos de respaldo, operación y arranque. Documentar los cambios en los manuales correspondientes, así como en el Plan de Recuperación DRP.
- Preparar la realización de al menos 2 pruebas anuales en el Centro de Cómputo Alterno.
- Realizar mensualmente una revisión de la carga de volúmenes, subsistemas y rendimiento (performance) del CPU.
- Informar al Grupo Coordinador cualquier variación en los recursos o configuración de recuperación requeridos. En su caso, reasignar o incrementar recursos de acceso, almacenamiento o proceso.

- Informar al líder y al suplente del Grupo Coordinador cualquier cambio en la configuración de respaldo para que, en caso de ser necesario, se solicite la modificación al equipo del Centro de Cómputo Alterno.
- Preparar los elementos de prueba: Verificar la distribución física de discos, media y densidad. Con el Grupo de Recuperación de Comunicaciones y verificar los enlaces, controladores y puertos.
- Efectuar la prueba y anotar cualquier ajuste “on site” para documentarlo en bitácora, procedimientos y Plan de Recuperación DRP.
- Confirmar la disponibilidad del personal de sistemas que se trasladará al Centro de Cómputo Alterno.
- Coordinar con los proveedores el uso de licencias de software base en equipo del Centro de Cómputo Alterno.
- Establecer comunicación con el proveedor de software aplicativo para solicitar licencias de uso temporal en el Centro de Cómputo Alterno.
- Solicitar carta con firma de autorización de uso y renovarla constantemente.
- Mantener contacto continuo con los otros Grupos de Recuperación y Comunicaciones.
- Participar en el diseño de nuevos mecanismos para el restablecimiento de las comunicaciones.
- Verificar y ajustar en conjunto las velocidades de transmisión y los protocolos de comunicaciones.
- Mantener actualizados los elementos de restauración en el Centro de Cómputo Alterno.

- Verificar que en el Centro de Cómputo Alterno se pruebe el sistema operativo cada vez que sea modificado y enviado.
- Verificar y asegurar que el equipo del Centro de Cómputo Alterno tenga la misma versión, configuración y definiciones de usuarios y los últimos Parches del Sistema Operativo
- Crear grupos de trabajo con horarios definidos, considerando al personal del área para operar en bajo contingencia, cubriendo todos los turnos tanto en el Centro de Cómputo principal como en el Centro de Cómputo Alterno.

4.3. Tareas Previas del Grupo de Recuperación de Comunicaciones:

Este grupo deberá tomar las medidas y acciones necesarias para asegurar que los elementos de comunicaciones que permiten una adecuada recuperación se encuentren disponibles y poder enfrentar exitosamente cualquier incidente. Estas actividades deberán considerarse como tareas permanentes y con revisiones cada tres meses o ante cualquier cambio significativo en alguno de estos elementos.

Este Grupo deberá tener previstos los elementos necesarios a fin de poder restablecer los enlaces requeridos de comunicaciones de voz y datos a nivel LAN y WAN, así como con el Centro de Cómputo Alterno y Centro Alterno de Trabajo.

- Definir un responsable del grupo que se encargue de mantener actualizado el plan.
    - Mantener actualizado el directorio del personal del área.
    - Mantener actualizado el directorio de Proveedores.

- Mantener actualizado la relación de software, equipos y componentes de comunicaciones.

- Nombrar un suplente del líder del grupo para que asuma sus responsabilidades en caso de ausencia del titular.
- Mantener actualizada la Configuración Mínima Aceptable de Recuperación (MARC) para restablecer la red de comunicaciones.
- Mantener actualizado el directorio de los integrantes del grupo.
- Mantener constante comunicación con el Grupo Coordinador.
- Determinar alternativas de comunicación viables.
  - Determinar costos de las alternativas
- Contar con manuales de operación de los componentes de comunicaciones.
  - Mantener ubicados los manuales de operación de equipos de comunicaciones y redes.
  - Revisar trimestralmente los procedimientos de recuperación y documentar los cambios en los manuales correspondientes.
- Participar en la definición y alcances de las pruebas del Centro de Cómputo Alterno y Centro Alterno de Trabajo.
  - Establecer contacto con los proveedores de comunicaciones para determinar enlaces y sus características para la prueba.
  - Recuperar y verificar la copia del software base que deberá ser utilizado para levantar los enlaces.
  - Participar en la programación de distribución de enlaces definiendo interfaces físicas, direccionamiento y protocolos de comunicaciones.
  - Restablecer el acceso a la red LAN, WAN y a los sistemas de cómputo centralizados.
  - Anotar en bitácora los ajustes “on site” y documentarlos en los procedimientos correspondientes y en el Plan de Recuperación (DRP).
- Establecer las conexiones necesarias en el Centro Alterno de Trabajo y la Mesa de Ayuda para casos de contingencia.
  - Contratar los circuitos alternos de comunicaciones de las localidades incluyendo las foráneas, hacia el centro de cómputo alterno.
  - Elaborar la documentación (datos técnicos, contactos con proveedores y procedimientos de escalamiento) de estos circuitos dentro del Plan.
  - Verificar, y en su ausencia, cablear para datos.
  - Verificar y asegurar la instalación de las líneas telefónicas
- Mantener contacto periódico con los proveedores de comunicaciones para determinar:
  - El estado y condición de enlaces al Centro de Cómputo Alterno y al Centro Alterno de Trabajo. Efectuar “LoopTest” periódicamente.
  - Las condiciones de enrutamiento.
- Mantener en condición de pendiente y preparado el siguiente equipo de comunicaciones del nodo del Centro de Cómputo Alterno y al Centro alterno de Trabajo:

- El equipo de ruteo.
- La configuración alterna de contingencia.
- La versión de software y los “parches”.

4.4. Tareas Previas del Grupo Operación Centro de Cómputo:

Este grupo deberá tomar las medidas y acciones necesarias para asegurar que los elementos del Centro de Cómputo que permitirán una adecuada recuperación se encuentren disponibles y poder enfrentar exitosamente cualquier incidente. Estas actividades deberán considerarse como tareas permanentes y con revisiones cada tres meses o ante cualquier cambio significativo en alguno de estos elementos.

Este Grupo deberá tener previstos los elementos necesarios a fin de poder restablecer los equipos críticos, del Centro de Cómputo Alterno y Centro Alterno de Trabajo.

- Definir un responsable del grupo que se encargue de mantener actualizado el plan.
  - Mantener actualizado el directorio del personal del área.
  - Mantener actualizado el directorio de Proveedores.
  - Mantener actualizado la relación de software base de equipos y componentes de cómputo.
- Nombrar un suplente del líder para que asuma sus responsabilidades en caso de ausencia del titular.
- Mantener actualizada la Configuración de Recuperación Mínima Aceptable (MARC) para restablecer la operación de cómputo.
  - Mantener un respaldo del software requerido de los servidores de aplicaciones y servicios críticos.
- Mantener actualizado el directorio de los integrantes del grupo.
- Mantener constante comunicación con el Grupo Coordinador
- Determinar alternativas de Operación viables.
  - Determinar costos de las alternativas.
- Contar con manuales de operación.
  - Mantener ubicados los manuales de operación de equipos del Centro de Cómputo.
  - Revisar trimestralmente los procedimientos de recuperación y documentar los cambios en los manuales correspondientes.
- Participar en la definición de las pruebas del Centro de Cómputo Alterno y Centro Alterno de Trabajo.
  - Establecer contacto con los proveedores de Hardware y Software para determinar su uso y características para la prueba.
  - Llevar a cabo las tareas en Sitio Alterno y Productivo de:
    - Revisión de la infraestructura (Parámetros ambientales),
    - Monitoreo de infraestructura y aplicaciones,

  - Respaldos (ejecución, montaje/desmontaje de y verificación de grabación),
  - Ejecución de procesos Batch (programados)
  - Verificación de capacidad disponible de medios de almacenamiento,
  - Control de cintoteca.
  - Transportar respaldos
  - Producción (reportes impresos)
  - Control de biblioteca técnica (sistemas operativos, paquetes producto y aplicaciones), en Centro Productivo y Alterno
- Anotar en bitácora los ajustes “on site” y documentarlos en los procedimientos correspondientes y en el Plan de Recuperación (DRP).
- Elaborar la documentación (datos técnicos, contactos con proveedores y procedimientos de escalamiento) dentro del Plan.
- Mantener contacto periódico con los proveedores de Hardware y Software para determinar el estado y condición del Equipo de Cómputo del Centro de Cómputo Alterno y del Centro Alterno de Trabajo. Efectuar “LoopTest” periódicamente.
- Mantener en condición de pendiente y preparado del equipo de Centro de Cómputo Alterno
  - La configuración alterna de contingencia.
  - La versión de software y los “parches”.

4.5. Tareas Previas del Grupo de Recuperación de Servicios de Informática

Este grupo deberá tomar las medidas y acciones necesarias para asegurar que los elementos que permitirán una adecuada recuperación se encuentren disponibles y poder enfrentar exitosamente cualquier incidente. Estas actividades deberán considerarse como tareas permanentes y con revisiones cada tres meses o ante cualquier cambio significativo en alguno de estos elementos.

Este Grupo deberá tener previstos los elementos necesarios a fin de poder restablecer los equipos críticos, en el Centro de Cómputo Alterno y Centro Alterno de Trabajo.

- Definir un responsable del grupo que se encargue de mantener actualizado el plan.
  - Mantener actualizado el directorio del personal del área.
  - Mantener actualizado el directorio de Proveedores.
  - Mantener actualizado la relación de software, equipos y componentes de cómputo bajo la responsabilidad del Grupo Mesa de Ayuda.
- Nombrar un suplente del líder del grupo para que asuma sus responsabilidades en caso de ausencia del titular.
- Mantener actualizado el directorio de los integrantes del grupo.
- Mantener constante comunicación con el Grupo Coordinador
- Determinar alternativas de Operación viables.
- Contar con manuales de operación.

- Identificar los manuales de operación de equipos del Centro de Cómputo.
- Revisar trimestralmente los procedimientos de recuperación y documentar los cambios en los manuales correspondientes.

- Participar en la definición de las pruebas del Centro de Cómputo Alterno y Centro Alterno de Trabajo.
  - Establecer contacto con los proveedores de Hardware y Software para determinar sus características para la prueba.
  - Llevar a cabo las tareas en Sitio Alterno de:
    - Soporte de Service Desk en reportes, Correo, Bases de Datos, Instalación de Clientes, Standalone, etc.
    - Instalación de Hardware / Software
    - Coordinación de mantenimiento a los equipos Alternos
    - Monitoreo de Equipos Centrales y Alterno
    - Monitoreo del servicio de antivirus central y alterno
    - Mantener el filtrado de contenido en el servicio de antivirus central y alterno
    - Monitoreo de las colas de mensajes de correo
    - Mantener y Controlar las cuentas de correo
    - Liberación de aplicaciones
    - Control y Habilitación de acceso a usuarios y cambio de password
    - Control de Colas de Impresión Remotas
    - Administración y soporte de servidores de domino y de aplicaciones.
    - Mantener scripts (shells) de seguridad
    - Monitoreo procesos (jobs) y procesos Batch (programados
    - Realizar pruebas de seguridad
    - Revisión de la infraestructura (Parámetros ambientales),
    - Monitoreo de infraestructura y aplicaciones,

5. Activación del Plan de Recuperación.

Como se ha mencionado con anterioridad, el ***Plan de Recuperación (DRP) para los Servicios de Cómputo y Comunicaciones en caso de Desastre (DRP)***se basa en el peor de los escenarios, es decir, una total interrupción de las operaciones del negocio por una contingencia mayor o catastrófica, esto permite al Grupo Coordinador, modificar cualquier procedimiento de recuperación y de un incidente en particular. Esta sección ofrece un panorama general del proceso de recuperación del desastre seguida de procedimientos detallados.

Un incidente incluye cualquier evento que haya interrumpido, o que podría interrumpir, las operaciones del Centro de Cómputo. La magnitud del evento 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.

La identificación o reconocimiento de un evento provoca el inicio de las actividades de respuesta a una emergencia y los Procedimientos de Evaluación de Daños. Dependiendo del diagnóstico de la evaluación, 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 sistemas de comunicación, tanto de voz como de datos estarán disponibles para continuar las funciones de la institución

El siguiente diagrama muestra el flujo de acciones a realizarse, después de ocurrido un evento, y antes de la declaración del desastre y activación del Plan

Declaración de Desastre

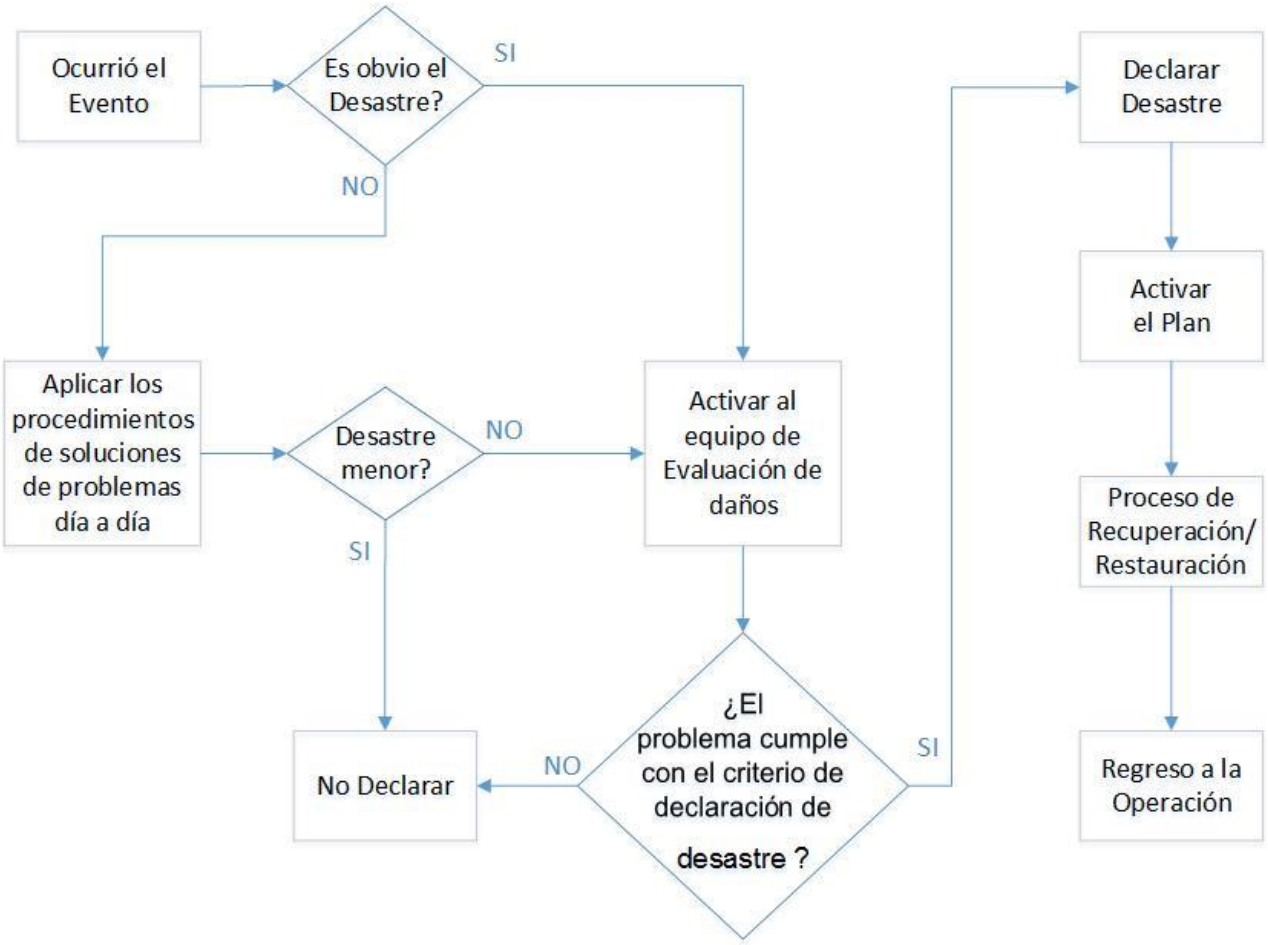


Ilustración 5. Declaración de desastre

Una vez que se haya identificado y reconocido un evento, el tiempo es vital. Los procedimientos que se presentan a continuación incluyen decisiones que son críticas con respecto al tiempo y que pueden estar basadas únicamente en la magnitud de la contingencia, en su evaluación, y en el impacto de éste en las operaciones del negocio.

5.1. 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 institución. 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 son inminentes.

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 organización y las prácticas estándares de operación.

Nota: Los procedimientos de respuesta a una emergencia se presentan sólo como información y tienen el objeto de complementar cualquier procedimiento de respuesta a una emergencia que esté vigente en la ESAP.

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 da cuenta de 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 se le asignó el nivel 1 de notificación.

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 del aviso;
- 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 a 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 (DRP) para los Servicios de Cómputo (DRP).

5.2. 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:

1 Al momento de la notificación del incidente poner en estado de alerta a todos los proveedores críticos.

2 Verificar la disponibilidad de lo siguiente:
- Localidad de Recuperación;
- Bóveda de almacenamiento externo;
- Bóveda de externa de Consumibles, papelería y accesorios

3 Obtener información pertinente con respecto al incidente:

3.1 Estado de las actividades de respuesta a la emergencia:
- Estado de la evacuación de las instalaciones
- Respuesta de Protección Civil.

3.2 Descripción del incidente:
- Tipo de incidente;
- Ubicación del incidente;
- Hora del suceso;
- Posible causa;
- Probabilidad de que el incidente continúe.
- Probabilidad de re-ocurrencia.

3.3 Lesionados y decesos:
- Nombres y estado de las víctimas;

- Naturaleza de las lesiones;
- Probabilidad de heridos y muertos adicionales.

3.4 Daño estimado:

- Daño al edificio. Describir el estado de muros, techos, pisos, estructura, etc.;
- Daño al contenido;
- Daño al equipo de cómputo;
- Daño al equipo de comunicaciones;
- Probabilidad de daños adicionales;

3.5 Seguridad:

- Posibles violaciones a la seguridad;
- Requerimientos de seguridad.

3.6 Acceso al edificio:

- Acceso actual;
- Posible acceso en el futuro inmediato.

3.7 Atención y reacción inmediata a los medios de prensa.

4 Determinar si es necesario contactar de inmediato a personal adicional:

4.1. Directivos;
4.2. Proveedores;
4.3. Personal de Apoyo:

- Mantenimiento e Instalaciones;
- Comunicación Corporativa;
- Recursos Humanos;
- etc.

5 Ayudar al Área de Seguridad en la evaluación de daños al Centro de Cómputo.

5.1. Participar en la sesión de evaluación revisando lo siguiente:
- Procedimientos de evaluación;
- Formas y requerimientos informativos;
- Asuntos de seguridad y salvamento;
- Asuntos especiales del seguro.

NOTA: *El acceso a las instalaciones después de un Terremoto, una probable contaminación química o de un incendio puede ser negado por 24 horas o más.*

6. Si se permite el acceso al edificio o a las instalaciones, llevar a cabo una inspección física en el área a supervisar para calcular el daño de lo siguiente:

6.1 Instalaciones físicas (Sistema eléctrico incluyendo UPS, generadores de Energía, Sistema de aire acondicionado, Sistema de detección de incendios, condiciones ambientales, integridad de la estructura, etc.)

6.2 Equipos electrónicos y/o de Cómputo (Servidores, Oracle, Dispositivos de almacenamiento, dispositivos de grabación de video)

6.3 Equipos de comunicaciones (routers switch, firewall) Mobiliario, trabajo en proceso, archivos, formas y consumibles. Analizar el estado de los procesos al momento de la ocurrencia del desastre. Identificar la información que ya no fue procesada o perdida, la programación de los procesos en línea, tareas y procesos batch (“jobs”), etc. Evaluar el impacto en la producción si se necesita restaurar la información a partir de respaldos

6.4 Registros vitales – impresos (archivos, manuales, documentos, etc.) y almacenados en otros medios (computadoras personales, CD´s, etc.) – como apoyo para concluir las estrategias específicas de recuperación y para determinar un plan general de salvamento y restauración.

6.5 Registrar todos los daños y de ser posible obtener documentación necesaria (fotografías, video, seguros, etc.), a efecto de contar con elementos de prueba en caso de proceder la solicitud de pago de las Compañías Aseguradoras.

7. Obtener información del daño ocasionado por los siguientes aspectos:
   7.1. Tiempo de reparación del equipo de Cómputo Central, Servidores y de Comunicaciones, PC´s locales y terminales de los Equipos.
   7.2. Estado físico del edificio e instalaciones (condiciones ambientales, estado físico de la firmeza de la estructura, etc.).
8. El líder del Grupo Coordinador instruirá los miembros de su Grupo para que entreguen la siguiente información después de la inspección del área:

.1. Resultados documentados del análisis utilizando las Formas de Evaluación de Archivos, Trabajos y Equipo, indicadas en el Anexo 4;

8.2 Identificar el equipo rescatable, marcar cuáles registros vitales y que equipo electrónico se necesita para la Recuperación de actividades y qué puede ser reparado rápidamente y los que potencialmente afectan más adversamente ala ***ESAP***.

9. Después de la inspección de las instalaciones dañadas, dirigirse al Centro de Control de Crisis establecido e indicar a los miembros del Grupo Coordinador que se reporten de inmediato a dicho Centro para la evaluación correspondiente.
10. Establecer la junta de avance y preparar un reporte de la evaluación de los daños para presentarlo al Comité Directivo y Dirección General.

5.3. Organizar Calendarios de los Grupos de Recuperación

El Grupo Coordinador será responsable de establecer los horarios y turnos de trabajo de los Grupos de Recuperación, basándose en la carga de trabajo, recursos y personal disponible.

1. Revisar cómo se está llevando a cabo la notificación a los empleados y verificar la actividad de recuperación asignada en la que participará el personal disponible.

1.1 Confirmar cuáles empleados deberán trabajar en la recuperación de inmediato y cuáles deberán permanecer localizables, disponibles y en constante comunicación

1.2 Verificar en el directorio de personal crítico, al personal responsable de recuperar cada una de las plataformas del Centro de Cómputo Alterno.

1.3 Reasignar al personal inactivo para apoyar en las actividades de salvamento u otras funciones prioritarias.

1.4 Supervisar la reubicación del personal inactivo durante la recuperación.

2. Establecer un programa de rotación de personal o turnos para balancear los horarios y cargas de trabajo, en función de las prioridades de recuperación del Centro de Cómputo Alterno.
3. En las juntas de avance incluir la siguiente información sobre:

3.1 El Portafolio de Aplicaciones Críticas del Plan actual.

3.2 La Implementación del MARC, mostrando la configuración de hardware del Centro de Cómputo Alterno.

3.3 La(s) localidad(es) asignadas al proceso de recuperación;

3.4 Contactar al Grupo de Unidades de Negocio para establecer las condiciones del Centro Alterno de Trabajo

5.4. Determinar el Estado Actual de los Respaldos y las Aplicaciones

Determinar el estado de las aplicaciones en proceso al momento de la interrupción, así como el estado esperado después de recuperar los datos requeridos.

1. Proceder a la obtención de los respaldos más recientes. Estos pueden encontrarse en el sitio o bien en la bóveda externa, dependiendo del momento del desastre. Tratar de obtener físicamente el mayor número posible de volúmenes partiendo del más reciente y hacia atrás. Utilice la información sobre Registros Vitales y asegure que todos los registros y datos críticos están físicamente presentes para ser transportados al Centro de Cómputo Alterno.
2. Determinar cuáles aplicaciones se restaurarán a partir de los respaldos disponibles, tomando el último que se puede encontrar en el sitio al momento del desastre o en bóveda.

5.5. Protección de los Medios de respaldo y Equipo contra Daños Posteriores.

Mitigar cualquier impacto potencial del incidente protegiendo el equipo de cómputo y medios de un daño mayor. Los procedimientos siguientes resumen los Procedimientos de Recuperación, respecto a la protección de equipo y medios de respaldo.

NOTA IMPORTANTE - la seguridad y salud del Personal son de interés primario. ¡Estos procedimientos son solamente para ser ejecutados si pueden ser efectuados sin riesgo!

1 Ejecutar un respaldo completo de todos los servidores y enviarlo fuera del sitio, si el tiempo y las circunstancias lo permiten. Asegurarse que todos los usuarios no estén conectados o firmados en las aplicaciones, antes de iniciar el respaldo.

2 Cortar la energía eléctrica del equipo de cómputo, siguiendo los procedimientos documentados:

- 2.1 Ejecutar los procedimientos de desactivación y apagado normal; si el tiempo lo permite desconectar todo el equipo de soporte (ejemplo: el sistema de aire acondicionado de las instalaciones).
- 2.2 Ejecutar los procedimientos de emergencia de corte de electricidad en caso de bomba u en otras circunstancias de riesgo.

3. Cubrir todo el equipo de cómputo, equipo de comunicaciones y medios de almacenamiento como sigue (después del procedimiento de corte de energía eléctrica):

- 3.1 Proteger los servidores, terminales y equipo de comunicaciones ante los diferentes escenarios de riesgo. (Incendio, Inundación, Desprendimientos Estructurales, etc.)
- 3.2 Proteger todos los medios de almacenamiento Magnético y Óptico.
- 3.3 Resguardar todos los discos y cintas en gabinetes de almacenaje o cajones.

4. En caso de humedad excesiva o humo, ventile el centro de cómputo:

- 4.1 Asegúrese que no haya peligro alguno antes activar el sistema de ventilación.
- 4.2 Abra todas las puertas y ventanas.
- 4.3 Busque y coloque los ventiladores especiales en las salidas.

Solicite al área de Seguridad de la empresa que acordone la zona o marque el perímetro hasta que la seguridad total sea restablecida

5.6. Procedimientos de Respuesta Inmediata

Implementar los procedimientos de respuesta inmediata basados en las circunstancias específicas del evento de acuerdo al Manual de Seguridad de la empresa; Estos procedimientos, normalmente desarrollados por recomendación de Protección Civil, tienen el objetivo de disminuir el impacto al personal, hasta que las condiciones vuelvan a situación normal para los siguientes casos:

- Que hacer en caso de Sismo.
- Que hacer en caso de Incendio.
- Que hacer en caso de Inundación.
- Que hacer en caso de Desastres Naturales.
- Que hacer en caso de Amenaza de Bomba.
- Que hacer en caso de falla del suministro eléctrico

5.6.1. Que hacer en caso de falla del equipo de Cómputo.

Responsables:

- Operación del Centro de Cómputo.

En caso de existir una falla en cualquier componente del Equipo de Cómputo:

- Documentar la falla existente al máximo detalle posible indicando los síntomas que presenta.
- Realizar una revisión general del dispositivo presunto de falla y si es posible diagnosticar el daño.
- Notificar al Grupo Coordinador de inmediato
- Contactar de inmediato, al (los) proveedor(s) del equipo que presentó problema, consultando la relación de Proveedores que se encuentra en el Anexo

5.6.2. Que hacer en caso de falla del equipo de apoyo.

Responsables:

- Operación del Centro de Cómputo.
  - Si fallan los equipos de Aire Acondicionado, intente restaurar los dispositivos que fallan accionando los switches de arranque.
  - Notificar de inmediato al área de Mantenimiento y soporte de la ***ESAP***
  - Notificar al Grupo Coordinador de inmediato

- Apague las lámparas no indispensables en la sala de Cómputo.
- Siga las instrucciones de la Oficina de Sistemas para reducir la temperatura en la sala de Cómputo.

Nota: El Área donde se encuentra instalado el equipo de cómputo es área restringida y no se permite la presencia de personal ajeno.

5.6.3. Que hacer en caso de falla de Software base.

Responsables:

- Operadores del Centro de Cómputo.

Solución de Problemas

- Identifique el Problema para ser reportado al Grupo de Operación del Centro de Cómputo de inmediato
- Contacte al Grupo de Mesa de Ayuda

5.6.4. Que hacer en caso de falla de Software Aplicativo.

Responsables:

- Operadores del Centro de Cómputo.
- Responsable de Sistemas de la Aplicación

Solución de Problemas

- Identifique el máximo detalle posible del problema antes de reportar
- Contacte al Grupo de Mesa de Ayuda

5.7. 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 Unidades de Negocio para hacerlo llegar a todos los contactos clave de las diversas Unidades de Negocio. Incluir sólo los hechos sin hacer suposiciones. Esta declaración debería contener:
   1.1 Breve comunicado respecto al incidente;

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

1.3 Fecha y hora en que sus aplicaciones serán restablecidas, si se tiene conocimiento de ello.

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.

5.8. Reaccionar a la Interrupción de Comunicaciones de voz.

En el caso de que el servicio telefónico se vea interrumpido será necesario habilitar líneas telefónicas directas. Estas líneas deberán ser colocadas en el Centro de Computo Alterno y al Centro Alterno de Trabajo a fin de que el personal operativo tenga contacto con personal interno y/o externo, proveedores, servicios de emergencia, etc.

Es también posible habilitar líneas de cobro revertido (01 800) con destino en estas localidades, en donde están habilitadas estaciones de trabajo en el caso de una interrupción por mayor tiempo.

5.9. Tareas del Grupo Coordinador.

En el momento de declarar un desastre, deberán efectuarse las acciones correspondientes con objeto de restaurar la infraestructura de cómputo y comunicaciones en el Centro de Cómputo Alterno y en su caso la reubicación del personal crítico al Centro Alterno de Trabajo.

De acuerdo a los daños provocados por el incidente, el Grupo Coordinador deberá:

- Asignar un Grupo de Trabajo al Centro de Cómputo colapsado, para su restauración.
- Asignar los Grupos de Recuperación que deberán trasladarse al Centro de Cómputo Alterno,
- Definir, en conjunto con los responsables de las Unidades de Negocio con procesos críticos, el grupo de trabajo que deberá trasladarse al Centro Alterno de Trabajo, de acuerdo a la lista de usuarios críticos que se presenta en el capítulo 3.6.

Las diversas tareas a realizarse para la recuperación y restauración de los servicios de cómputo y comunicaciones son:

1. Evaluar el impacto del desastre en coordinación con el personal de apoyo.

1.1. Realizar una inspección visual de sus instalaciones en el CAN y confirmar a los líderes de los grupos la activación del plan.

1.2. Declarar el desastre.

2. Llevar a cabo la comunicación para la notificación del desastre.
   2.1 Comunicar el desastre y el estado que guarda al Grupo Comité Directivo y al Vocero Oficial.
   2.2 Mantener comunicación con la Dirección General y con el personal designado por cada Unidad de Negocio.

3. El Grupo Coordinador a través de los líderes de cada Grupo de Recuperación realizará las siguientes actividades:

   3.1. Evaluar las condiciones en que se encuentra el personal.

   3.2. Seguir las políticas de emergencia establecidas por la ***ESAP***.

4. Activar a los Grupos de Recuperación.

   - Grupo Operación Centro de Computo
   - Grupo Servicios de Informática
   - Grupo Comunicaciones
   - Grupo Seguridad Informática
   - Grupo Desarrollo de Sistemas
   - Grupo Mesa de Ayuda
   - Grupo Unidades de Negocio

5. Verificar que se cuenta con el equipo necesario en el Centro de Cómputo Alterno con base al reporte del M.A.R.C.

   5.1. Reubicar al personal y asignar equipo basándose en el reporte del MARC.
   5.2. En caso de equipo faltante coordinar la renta o compra de los necesarios.
   5.3. Coordinar la preparación de las posiciones de las Unidades de Negocio en el Centro Alterno de Trabajo.

6. Coordinar al personal que se trasladará al Centro de Cómputo Alterno.

   6.1. Ratificar al personal seleccionado que será enviado y cuál será su misión dentro del grupo.

   6.2. Preparar los medios de traslado del personal.
   6.3. Verificar que el personal a trasladar lleve consigo: cintas de respaldo y configuración tanto de equipo de cómputo como de comunicaciones.
7. Dar seguimiento al desarrollo del plan.
   7.1. Confirmar actividades de los grupos de acuerdo al plan de acción.

8. Coordinar y Mantener los servicios de apoyo al personal en el Centro Alterno de Trabajo.
   8.1 Notificar al Personal Crítico que será trasladado al Centro Alterno de Trabajo.
   8.2. Coordinar el traslado del personal crítico al Centro Alterno de Trabajo.
   8.3. Coordinar la disponibilidad de los servicios necesarios para la operación en el Centro Alterno de Trabajo.
   8.4. Apoyar a los usuarios para que tengan disponibilidad de los servicios que requieran, como Registros Vitales, Papelería, Equipo especial, etc.
   8.5 Asignar las áreas de trabajo del personal crítico.
   8.6. Verificar que las terminales de acceso estén listas en el momento que los enlaces estén activados.
   8.7. Establecer los horarios de trabajo y la rotación del personal.
9. Iniciar los trámites necesarios con las compañías aseguradoras.
   9.1. Notificar el desastre al ejecutivo de la cuenta asignado a la ***ESAP***.
   9.2. Dar seguimiento al cobro del seguro conforme a las condiciones establecidas en la Póliza.
10. Evaluar la disponibilidad del personal de la ***ESAP***.
   10.1. Apoyar al personal.
   10.2. Atender solicitudes del servicio médico.
11. Evaluar el estado de los equipos.
   11.1. Verificar si el equipo es rescatable.
   11.2. Verificar si el equipo es utilizable.
   11.3. Verificar si el equipo es reparable.
   11.4. Verificar si es pérdida total del equipo.

12. Rescatar el equipo, suministros o datos que no hayan sufrido daño.
13. En caso de pérdida de equipo, proceder a su reposición.
14. Evaluar el estado del Centro de Cómputo.
15. De acuerdo al resultado de la evaluación del Centro de Cómputo, Coordinar la reunión para tomar la decisión si se utiliza, se repara o se instala en otro lugar.
16. Realizar un estudio económico de los requerimientos del Centro de Cómputo Alterno.

17. Conseguir la aprobación económica de la Dirección General de la ***ESAP*** para el Centro de Cómputo Alterno.
18. Mantener informado al Grupo Coordinador y a la Dirección General del tiempo en el que estará funcionando el Centro de Cómputo Principal.
19. Coordinar con los proveedores de los equipos la llegada de los mismos.
   19.1 Coordinar la puesta en marcha del Centro de Cómputo Alterno.
20. Establecer un plan para la restauración o reconstrucción de las instalaciones dañadas.
   20.1 Confirmar con el Grupo Coordinador y la Dirección General la restauración o reconstrucción de las instalaciones dañadas.

5.10. Tareas de los Grupos de Recuperación:

- Grupo Operación Centro de Cómputo
- Grupo Servicios de Informática
- Grupo Comunicaciones
- Grupo Seguridad Informática
- Grupo Desarrollo de Sistemas
- Grupo Mesa de Ayuda
- Grupo Unidades de Negocio

En el momento de declarar un desastre, deberán efectuarse las acciones correspondientes con el objeto de restaurar la infraestructura de cómputo, comunicaciones y las operaciones del personal crítico en el Centro Alterno de Trabajo.

Las actividades de estos Grupos en caso de una declaración de desastre, deberán ser lo más ágil y eficaz posible, siempre que las circunstancias lo permitan.

5.11. Tareas del Grupo de Operación del Centro de Cómputo:

1. Reportarse al Centro de Control de Crisis o al lugar señalado por el Grupo Coordinador.
2. Notificar al Grupo Coordinador el estado del equipo.
3. Recuperar y verificar de la bóveda externa que las cintas del último respaldo de datos y programas de aplicación estén completas y en orden.
4. Recuperar y verificar de la bóveda externa que el manual de software y los procedimientos de levantamiento de equipos sean trasladados al Centro de Cómputo Alterno.
5. Coordinar con el Grupo de Recuperación de Comunicaciones cuáles serán las acciones y la infraestructura de enlaces.

6. Instalarse en el área designada por el Grupo Coordinador y comprobar que se tienen disponibles en el área las cintas de respaldo de datos y programas de aplicación más reciente y las previas a éstas.

6.1. Verificar los manuales de operación del hardware y software de aplicación.

6.2. Tener a la mano los números telefónicos del Centro de Cómputo Alterno y proveedores críticos.

6.3. Verificar para cada plataforma. Que el sistema operativo de los Servidores Críticos ha sido cargado, así como la última versión de Parches de seguridad. El Sistema operativo debe estar en el mismo release (Versión y Service Packs) del equipo dañado.

7. Cargar y poner en marcha los equipos de respaldo.

7.1. Poner en funcionamiento los equipos de acuerdo a los procedimientos internos de la Oficina de Sistemas Informáticos de la ***ESAP***.

8. En tanto estén disponibles los equipo, coordinar e identificar en conjunto con el personal técnico de comunicaciones lo siguiente:

8.1 Las direcciones de enlace. (IP's en las Comunicaciones).

8.2 Las interfaces físicas, velocidad y protocolo.

9. Restaurar aplicaciones Con base en el último respaldo disponible, restaurar aplicaciones.

10. Una vez restauradas las aplicaciones, verificar, y de ser necesario, modificar:

10.1 Las listas de autorización de acceso a la información,

10.2 La integridad de las bibliotecas.

10.3 Que los perfiles de usuario se encuentren completos y actualizados

10.4 Que los archivos de control y de parámetros estén presentes e íntegros.

10.5 Que se cambien los valores de sistema por omisión, se inicien subsistemas y se corra afinación automática.

10.6 Que los puertos de enlaces estén activados, direccionados y en condición de conectividad y operación.

10.7 Coordinar con el Grupo de Comunicaciones la configuración de los enlaces y efectuar los cambios que sean necesarios para que éstos operen.

10.8 Verificar que las aplicaciones operen correctamente.

10.9 Notificar al Grupo Coordinador que el equipo se encuentra verificado y operando.

11. Coordinar con el personal técnico de Comunicaciones el mecanismo de conexión entre el equipo de respaldo restaurado, las otras plataformas con las que se tiene interface y con la LAN.

12. Llevar una bitácora de los hechos y las respuestas o medidas tomadas, con el fin de documentar los sucesos durante la contingencia para contar con la información que permita una mejor actualización en la siguiente revisión del Plan.

5.12. Tareas del Grupo de Servicios de Informática:

1. Reportarse al Centro de Control de Crisis o al lugar señalado por el Grupo Coordinador.

2. Coordinar el control y manejo de los respaldos.

3 Garantizar los suministros de Energía, Aire acondicionado, UPS.

4. Coordinar y realizar la operación de las distintas aplicaciones en los Equipos y Servidores instalados en el Centro de Computo Alterno

5. Proporciona los servicios y enlace con las distintas entidades externas.

6. Llevar una bitácora de los hechos y las respuestas o medidas tomadas, con el fin de documentar los sucesos durante la contingencia para contar con la información que permita una mejor actualización en la siguiente revisión del Plan.

5.13. Tareas del Grupo de Recuperación de Comunicaciones:

En el momento de declarar un desastre, deberán efectuarse las acciones correspondientes con objeto de restaurar la infraestructura de cómputo y comunicación dañada y las operaciones del personal crítico en el Centro Alterno de Trabajo.
Las actividades de este Grupo en caso de una declaración de desastre, deberán ser lo más ágil y eficaz posible, siempre que las circunstancias lo permitan.
En el momento de declararse un desastre, el Grupo de Recuperación de Comunicaciones deberá efectuar diversas actividades encaminadas a recuperar los enlaces críticos de acuerdo a las prioridades e indicaciones del Grupo Coordinador.

1. Reportarse al Centro de Control de Crisis o bien, al lugar en donde sea indicado por el Grupo Coordinador.
2. Activar enrutamiento.
   2.1 Establecer contacto con proveedores e indicar que deberán ser enrutados los enlaces al Centro de Cómputo Alterno.
   2.2 Activar enlace del centro de cómputo de acuerdo a la estrategia seleccionada.
3. Preparar recepción de enlaces en el Centro de Cómputo Alterno.
4. Recuperar y verificar el manual y software de levantamiento de equipo.
5. Trasladarse al Centro de Cómputo Alterno de acuerdo a las instrucciones del Grupo Coordinador
6. Instalarse en el área designada por el Grupo Coordinador.
7. Tener a la mano los números telefónicos del Centro Alterno de Trabajo y proveedores de comunicaciones.
8. Restaurar enlaces determinados en el DRP.

9. Confirmar con los Grupos de Recuperación la configuración de los enlaces y efectuar los cambios que sean necesarios.
10. Verificar que los enlaces y la configuración operen correctamente.
    - Contactar con los Proveedores de comunicaciones, entidades externas de servicios y entidades regulatorias con las que se tienen enlaces y hacer pruebas de señal entre ambos nodos.

11. Verificar la carga y grado de utilización de los enlaces y efectuar los ajustes necesarios.
12. Notificar al Grupo Coordinador que la red se encuentra activa y operando.

Llevar una bitácora de los hechos y las respuestas o medidas tomadas, con el fin de documentar los sucesos durante la contingencia para contar con la información que permita una mejor actualización en la siguiente revisión del Plan

5.14. Tareas del Grupo de Seguridad Informática:

1. Reportarse al Centro de Control de Crisis o al lugar señalado por el Grupo Coordinador.

2.- Verificar que el traslado de la información que está en la Bóveda Central tal como los cartuchos o medio de respaldos, documentación, procedimientos y manuales, sea trasladada al Centro de Cómputo Alterno bajo las medidas de seguridad y control establecidas en la ***ESAP***.
3. Una vez establecido e instalado los equipos con sus sistemas operativos, aplicaciones y datos, asegurarse que el establecimiento de contraseñas, accesos y perfiles de usuarios a los sistemas, tanto locales como remotos, cumple con los lineamientos y políticas establecidas por la ***ESAP***.
4. Verificar que los diferentes medios de enlace de la topología de Comunicaciones cumplan con los lineamientos y políticas de seguridad establecidos por la ***ESAP***, para evitar riesgos de accesos no autorizados e intrusos.

Llevar una bitácora de los hechos y las respuestas o medidas tomadas, con el fin de documentar los sucesos durante la contingencia para contar con la información que permita una mejor actualización en la siguiente revisión del Plan

5.15. Tareas del Grupo de Desarrollo de Sistemas:

1. Reportarse al Centro de Control de Crisis o al lugar señalado por el Grupo Coordinador.
2. Verificar con el Grupo de Operación del Centro de Cómputo que los equipos donde radica cada una de las aplicaciones ya esté operando.
3. Confirmar con el Grupo de Operación del Centro de Cómputo que los datos de la bóveda externa y las cintas del último respaldo de datos y programas de aplicación estén completos, instalados y con los datos cargados
4. Asegurarse que el Grupo de Operación del Centro de Cómputo recuperó de la bóveda externa los manuales de cada una de las aplicaciones y que fueron trasladados al Centro de Cómputo Alterno.
5. Verificar con el Grupo de Recuperación de Comunicaciones que los enlaces ya estén operativos.
6. Instalarse en el área designada por el Grupo Coordinador.
7. Verificar los manuales de operación del software de aplicación.
8. Tener disponibles los números telefónicos del Centro de Cómputo Alterno y proveedores de las aplicaciones críticas.
9. Verificar para cada plataforma, que las aplicaciones ya han sido levantadas y si es el caso que están instaladas las actualizaciones correspondientes.
10. Corroborar que la restauración de las aplicaciones se realizó de acuerdo a los procedimientos.
11. Verificar que las aplicaciones están operando de acuerdo a los procedimientos internos de Sistemas de la ***ESAP*** considerando:

- Que las claves de acceso y perfiles de usuarios están habilitadas y operando satisfactoriamente.
- El acceso a las pantallas de inicio de sesión
- La navegación por las diferentes opciones de menú de la aplicación.

- Determinar que la aplicación puede ser accedida desde posiciones de trabajo remotas, utilizando los medios y enlaces de comunicación establecidos como respuesta al evento.
- Verificar la congruencia y consistencia de los datos e información cargada.

12. Notificar al Grupo Coordinador el estado de las Aplicaciones.

13. Llevar una bitácora de los hechos y las respuestas o medidas tomadas, con el fin de documentar los sucesos durante la contingencia para contar con la información que permita una mejor actualización en la siguiente revisión del Plan.

5.16. Tareas del Grupo de Mesa de Ayuda:

1. Reportarse al Centro de Control de Crisis o al lugar señalado por el Grupo Coordinador.

2. Preparar los Equipos que operarán en el Centro de Trabajo Alterno en cuanto a la instalación de los dispositivos de Hardware, como discos duros, memoria, Tarjetas de Red, etc.
3. Instalar el Sistema Operativo y Paquetería estándar que deberán contener los equipos del Centro de Trabajo Alterno.
4. Instalar los equipos preparados en las posiciones de trabajo de las unidades de Negocio en el Centro Alterno de Trabajo y verificar su funcionamiento y conectividad a la red y periféricos requeridos.

Llevar una bitácora de los hechos y las respuestas o medidas tomadas, con el fin de documentar los sucesos durante la contingencia para contar con la información que permita una mejor actualización en la siguiente revisión del Plan

5.17. Tareas del Grupo Unidades de Negocio:

1. Reportarse al Centro de Control de Crisis o al lugar señalado por el Grupo Coordinador.
2. Coordinar que el traslado del personal al Centro Alterno de Trabajo o las instalaciones que el Grupo Coordinador indique, se realice con la oportunidad y condiciones de seguridad establecidas.
3. Estar en comunicación con el Grupo Coordinador para determinar el momento en que los equipos y aplicaciones están instalados y disponibles para su operación y certificar que las aplicaciones correspondientes están operando satisfactoriamente.
4. Llevar una bitácora de los hechos y las respuestas o medidas tomadas, con el fin de documentar los sucesos durante la contingencia para contar con la información que permita una mejor actualización en la siguiente revisión del Plan.

6. PROCEDIMIENTOS DE RECUPERACIÓN DE LOS SERVICIOS DE CÓMPUTO

Estos Procedimientos de Recuperación se basan en el peor escenario, es decir el no acceso a los servicios de cómputo 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 Comité Directivo DRP.

6.1. Procedimientos para la Declaración de Desastre

Una vez que el Grupo Coordinador y el Comité Directivo han evaluado el nivel de contingencia y la duración de la interrupción en las operaciones normales de la ***ESAP***, 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:

- Recabar la información de diagnóstico y tiempo de recuperación.
- Analizar el alcance de los daños y si la interrupción a la operación normal del negocio (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 al incidente (ver capítulo 3.4).
- Solicitar a los líderes de los Grupos de Recuperación iniciar de inmediato la recuperación de acuerdo al Plan.

Los procedimientos en detalle para recuperar y restaurar equipos y sistemas por cada una de las plataformas tecnológicas se presentan en el anexo 1.
A continuación, se indican algunos procedimientos de logística que apoyan la recuperación y restauración

Asignar y Organizar las Áreas de Trabajo del Centro de Cómputo Alterno

Preparar el Centro de Cómputo Alterno para las operaciones de recuperación, organizando las áreas de trabajo y los materiales de recuperación. El Centro de Cómputo Alterno debe estar disponible inmediatamente después de la declaración del desastre. Si el tiempo lo permite se correrá un diagnóstico del equipo.

Obtener y Organizar la Recuperación de Materiales y Registros Vitales

Una vez declarado el desastre, se deberá solicitar al Grupo de Recuperación la obtención de los respaldos del área de almacenamiento externo.

Inmediatamente después de la llegada al Centro de Cómputo Alterno se procederá a desempacar todos los respaldos de registros vitales, asegurar que todos los respaldos identificados están presentes y disponibles. Distribuir toda la documentación impresa a los miembros del grupo apropiado.

1. Reunirse con el personal que integra el Grupo Coordinador para revisar las actividades de coordinación para la operación de recuperación.

2. Revisar la configuración de recuperación contra los recursos requeridos, asegurando que todos los recursos estén disponibles y accesibles. Verificar que todos los dispositivos estén accesibles e inicializados para la asignación de actividades pre-definidas.
3. Revisar que todos los materiales han llegado al Centro de Cómputo de Respaldo.
   - Organizar archivos y materiales tan pronto sean recibidos.
   - Ordenar cintas en la secuencia que serán utilizados, así como separar las que serán de "*scratch*".
4. Asegurarse que ningún archivo contaminado llegue al centro de cómputo alterno sin tomar las precauciones apropiadas para evitar contaminación de las operaciones de recuperación.
5. Desempacar y organizar cintas usando estantes diseñados especialmente para resguardo de los mismos. Considerar estos puntos mientras se organizan las actividades de restauración iniciales:
   - Si es posible, use cajas de empaque existentes para reducir tiempo y posibles daños.
   - Almacenar cintas y cajas en orden ascendente para agilizar el proceso de restauración.
5. Determinar el rango de cintas salvables a fin de organizar una nueva biblioteca.
6. Asegurar que se dé una rotación apropiada de respaldos continua al centro de cómputo alterno.
7. Revisar las cintas existentes de repuesto de acuerdo a las políticas y procedimientos. (NO borrar ningún dato de los juegos de producción durante las fases iniciales de la recuperación, particularmente si las corridas normales de producción se han alterado para acomodar procesos en el centro de cómputo alterno). No reutilizar las cintas originales de respaldo para un nuevo respaldo, independientemente del número de juegos que se lleven.

6.2. Restaurar los Sistemas de Cómputo

Los Grupos de Recuperación llevarán a cabo las tareas necesarias para recuperar las operaciones de producción en el Centro de Cómputo Alterno. Se le dará prioridad a la restauración de la configuración para el ambiente de producción y finalmente a las comunicaciones de las redes de datos.

Restaurar los Enlaces de Comunicaciones al Centro de Cómputo Alterno

Direccionar los enlaces del Centro de Cómputo dañado al punto donde se encuentra el Centro de Cómputo Alterno.

Una vez en el área de trabajo que ha sido asignada, proceder a preparar los elementos que serán requeridos en la restauración.

- Cargar la configuración de comunicaciones.
- Verificar con el personal del Grupo de Operación del Centro de Computo y Comunicaciones, la puesta a punto de los puertos entre las plataformas de los servidores críticos.
- Elaborar un “mapa” de las coordenadas, interfaces, puertos y velocidad de los enlaces.

6.3. Activar la Red de Respaldo

El Grupo de Comunicaciones, enruta la red de datos hacia el Centro de Cómputo alterno, de acuerdo al procedimiento indicado, y desde ahí restablecerá las comunicaciones de datos hacia todos los nodos de producción dentro de la red.

- Proceder desde el Centro Alterno de Trabajo a:
- Distribuir los enlaces y ruteo hacia las terminales locales.
- Asignar los números telefónicos y líneas dedicadas de contingencia.
- Distribuir las extensiones locales.

Verificar los balanceadores de carga, ancho de banda y velocidad de los enlaces

6.4. Notificación de Accesibilidad

Una vez que las comunicaciones y servidores hayan sido enlazados, notificar al Grupo Coordinador, que los sistemas de comunicaciones han sido habilitados para operar bajo el esquema de contingencia. El Grupo Coordinador efectuará los contactos con áreas internas y entidades externas a fin de notificar que se opera bajo esquema de contingencia.

6.5. Concluir las operaciones en el Centro de Cómputo Alterno

Al concluir la contingencia, efectuar una desactivación e inicialización controlada del sistema para asegurar la confidencialidad de todos los datos de la empresa.

- Imprimir los históricos de la consola, y si se considera apropiado, correr un informe de bibliotecas de cinta.
- Asegurar que toda la información generada y procesada esté respaldada en tres juegos antes de abandonar el centro de cómputo respaldo.
- Cerrar el sistema operativo.
- Re empacar todas las cintas, documentación y datos de prueba.

7. 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.

7.1. Apoyo en las Actividades de Salvamento y Recuperación de Media

Apoyar al Grupo de Recuperación en la planeación de la restauración del centro de cómputo. Dado que el equipo y medios de respaldo requieren de personal con habilidades especiales, el Grupo de Recuperación guiará los esfuerzos necesarios.

- Revise los requerimientos de personal y notifique al Grupo de Recuperación sobre personal disponible que pueda participar en las actividades de salvamento y de recuperación de medios. El personal normalmente involucrado en actividades de desarrollo a largo plazo y aquellos inactivos debido a la restricción de recursos son fuertes candidatos para desarrollar estas actividades.
- Actualice los reportes y formas según avance el proceso de recuperación comunicando cualquier cambio en prioridades o requerimientos.
- Informe al Grupo de Recuperación sobre cualquier artículo crítico adicional que considere perdido. Solicite instrucciones de cómo hacer la notificación y a quién se informa sobre el artículo perdido

7.2. Plan de Retorno

Desarrollar una 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 de cómputo, 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 sesiones 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 a las circunstancias. Verificar que los procedimientos de respuesta puedan ser usados para proveer una contingencia durante el movimiento.
2.2 Considerar agregar respaldos especiales para toda la media de almacenamiento a 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.

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. Estas actividades comprenden el restablecimiento de los servicios y un mecanismo 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 Dirección General la terminación del desastre.
4. Notificar al personal de Sistemas el regreso a la operación normal.
5. Verificar que obtengan los respaldos 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.

Tareas de los Grupos de Recuperación

- Grupo Operación Centro de cómputo.
- Grupo de Mesa de Ayuda.
- Grupo Unidades de Negocio.
- Grupo de Seguridad Informática.

Restaurar la infraestructura de cómputo en las instalaciones propias. Estas actividades comprenden el restablecimiento de los servicios y un mecanismo de reincorporación de los movimientos efectuados durante la contingencia.

Una vez que el hardware ha sido instalado proceder a levantar el equipo de acuerdo a las condiciones del mismo (si fue reconstruido o es nuevo) y preparar los elementos que serán requeridos en la restauración.

1. Efectuar los respaldos de los archivos modificados y utilizados durante la contingencia en el Centro de Cómputo Alterno.

1.1 Empacar la media de respaldo en forma adecuada.
1.2 Preparar la documentación de traslado de media.
1.3 Enviar la media por la vía más rápida disponible.
1.4 Desplazarse hacia el lugar indicado por el Grupo de Respuesta y Recuperación.

2. Al arribar al lugar designado por el Grupo de Recuperación verificar el estado físico de las instalaciones de cómputo y determinar, en conjunto con el proveedor de los equipos restaurados, que los siguientes elementos se encuentren dentro de los parámetros establecidos:

2.1 La temperatura de operación.
2.2 La humedad relativa.
2.3 La energía eléctrica.

3. Recuperar la copia tanto de la aplicación, sistema operativo y bibliotecas.
4. Tener disponibles el manual de software y los procedimientos de levantamiento de los equipos
5. Coordinar con el Grupo de Recuperación de Comunicaciones cuáles serán las acciones y la infraestructura y condición de los enlaces.
6. Levantar Equipo restaurado.
6.1 Arrancar los equipos del Centro de Cómputo
7. Restaurar aplicaciones
8. Una vez restauradas las aplicaciones verificar, y de ser necesario, modificar:
8.1. Las listas de autorización de acceso a la información.
8.2. La integridad de las bibliotecas de usuario.
8.3. Que los programas de aplicación de usuarios hayan sido restaurados correctamente.

8.4. Que los archivos estén presentes e íntegros.
8.5. Que los puertos de enlaces estén presentes, direccionados
9. Coordinar con el Grupo de Recuperación de las Comunicaciones la configuración de los enlaces y efectuar los cambios que sean necesarios para que éstos operen.
10. Verificar con el Grupo de Recuperación de Comunicaciones el mecanismo de conexión hacia la LAN.
11. Verificar que las aplicaciones transaccionales operen correctamente.
12. Notificar al Grupo de Respuesta y Recuperación que el equipo esté verificado y en operación.

Tareas del Grupo de Recuperación de Comunicaciones:

Comunicaciones

Restaurar la infraestructura de comunicaciones en las instalaciones propias. Estas actividades comprenden el restablecimiento de los servicios.

Una vez que el hardware ha sido instalado proceder a levantar el equipo de acuerdo a las condiciones del mismo (si fue reconstruido o es nuevo) y preparar los elementos que serán requeridos en la restauración.

1. Activar enrutamiento.

    1.1 Establecer contacto con el proveedor del enlace e indicar que el mecanismo de retorno se ha puesto en marcha, por lo cual es necesario el enrutamiento hacia el Centro de Cómputo nuevo o restaurado (en caso necesario):

    1.2 Indicar a proveedores del servicio pasar a estado de condición de espera en los enlaces hacia el Centro de Cómputo de Respaldo.
2. Coordinar con los Grupos Técnicos de cada plataforma cuáles serán las acciones en la infraestructura de enlaces.
3. Confirmar con los Grupos de Recuperación de cada plataforma la configuración de los enlaces y efectuar los cambios que sean necesarios.
4. Verificar que los enlaces y la configuración operen correctamente.
    4.1 Contactar con proveedores de los enlaces para efectuar pruebas de señalización entre los nodos.
5. Distribuir la carga y utilización de los enlaces y efectuar ajustes necesarios.
6. Notificar al Grupo de Respuesta y Recuperación que la red se encuentre activa y operando.

8. PROCEDIMIENTOS ADMINISTRATIVOS DEL CENTRO DE CÓMPUTO

Estas responsabilidades administrativas resumen las políticas de la ***ESAP,*** así como la definición de algunas recomendaciones prácticas de recuperación basadas en la experiencia de recuperación de otras organizaciones.

Familiarizarse con esas responsabilidades y guías de procedimientos y posteriormente aplicarlas durante la respuesta inicial y actividades subsecuentes de recuperación del negocio.

8.1. Reforzar las Políticas de la ESAP

Monitorear las políticas y procedimientos de control y seguridad. La experiencia indica que las compañías son particularmente vulnerables a fraudes y sabotaje durante los períodos de interrupción. Obtener de la Oficina de Sistemas o de la Dirección General las autorizaciones para cualquier cambio a las políticas estándar de control.

Mantener un control y seguimiento del costo relacionado al desastre. Todos los gastos efectuados como resultado de la recuperación del negocio deben ser cargados a una cuenta especial de contabilidad.

> *NOTA: Esta cuenta contable deberá usarse únicamente para registro de pedidos de compra; anticipo de gastos; reportes de tiempo, etc., esto únicamente en referencia a la recuperación de las operaciones y no del mantenimiento y pruebas.*

8.2. Asegurar el Bienestar del Personal

Monitorear estrechamente el horario de trabajo del personal asegurando el bienestar de los empleados participantes en el esfuerzo de recuperación.

Durante las situaciones de emergencia se requerirá que el personal trabaje tiempo extra, sin embargo, se deberá enfatizar que es necesario un descanso adecuado a fin de reducir la tensión y aumentar al máximo la eficiencia.

La experiencia indica que varios días o semanas posteriores a un desastre se presentan problemas emocionales. Se debe considerar la necesidad de recompensar al personal por su esfuerzo extra durante la operación de recuperación.

Deberá tomarse en cuenta cualquier esfuerzo especial dado que cualquier desigualdad podría generar y/o aumentar problemas de esta índole

8.3. Monitorear y Reportar el Avance de la Recuperación

Monitorear frecuentemente el progreso de los Grupos de Recuperación (cada hora el primer día, después hacerlo al menos diario). Recopilar diariamente reportes escritos del avance de

cada Grupo de Recuperación. Enviarlos verbalmente y por escrito al Líder del Grupo Coordinador DRP

Las actividades clave que conforman este plan y los procedimientos de los Grupos sirven como base para dar seguimiento al progreso logrado.

8.4. Mantenimiento de los Registros Relacionados a la Recuperación

Mantener una bitácora detallada durante el proceso de recuperación, ya que la bitácora detallada y completa es invaluable para reducir la confusión durante la recuperación, así como conciliar los gastos efectuados y la adquisición de materiales.

- Mantener una buena documentación escrita de cualquier cambio o modificación a los procedimientos normales de operación. Asegurar que las modificaciones o cambios temporales no retrasen o pospongan las operaciones normales después de finalizar la recuperación.

- Reúna, revise y apruebe todos los controles de asistencia y horario. Es importante el seguimiento del tiempo invertido en cada actividad de la recuperación y restauración puesto que la contabilidad necesitará comprobante

- Mantener un registro de todos los gastos personales incurridos durante la operación de recuperación (los recibos deberán ser anexados).

- Anotar cualquier cambio del Plan de Recuperación (DRP) para los Servicios de Cómputo (DRP) para su actualización.

8.5. Distribución y Disponibilidad del Plan

Asegurar que el Plan de Recuperación (DRP) para los Servicios de Cómputo, 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 (DRP) para los Servicios de Cómputo 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 los respaldos y actividades de rotación externas para registros vitales incluyendo aquellos de PC´s están siendo efectuados.

5 Dar mantenimiento a su Plan de Recuperación (DRP) para los Servicios de Cómputo (DRP) 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 del negocio, sistemas de soporte (i.e. nuevas aplicaciones computarizadas) o nuevas prácticas o cambios de organización.

6 Participar sobre todo en el programa de pruebas del Plan de Recuperación

(DRP) para los Servicios de Cómputo tan frecuente como sea requerido

8.6. Revisión y Validación de Estrategias y Procedimientos

En los intervalos anotados coordinar las siguientes revisiones al plan con los miembros de los Grupos de Recuperación, incluyendo los líderes y subordinados

1. Trimestralmente, asegurar que cada Grupo de Recuperación esté actualizado de acuerdo a sus respectivas Tareas de Preparación.

2. Trimestralmente, revisar y actualizar lo siguiente:

2.1 Configuración de Recuperación Mínima Aceptable;

2.2 Respaldos y Registros Vitales;

2.3 Estructura y funciones de los Grupos de Recuperación.

3. Anualmente, lleve a cabo las siguientes mejoras a los procedimientos del plan:

3.1 Revisar los requerimientos de Recuperación definidos en el Cuadro de Aplicaciones Críticas;

3.2 Revisar las estrategias y procedimientos de respaldo para la recuperación y asegurar que reflejen adecuadamente los requerimientos de la ***ESAP***;

3.3 Llevar a cabo una prueba de la "Notificación" a los integrantes del grupo y documentar los resultados para propósito de auditoría;

3.4 Llevar a cabo una prueba con el equipo y documentar los resultados para propósito de auditoría;

3.5 Conducir una auditoria a todos los recursos de recuperación, incluyendo los Respaldos de Registro Vitales, identificados según se vayan almacenando en el Sitio Alterno o Bóveda de almacenamiento Externo

9. CAPACITACIÓN Y PRUEBAS

9.1. Programa de Capacitación

El plan de capacitación al personal se llevará a cabo en dos fases:

1ª. Sesiones de sensibilización y capacitación con los Grupos de Recuperación y responsables de la activación del DRP y ejecución de los procedimientos de logística, recuperación y restauración de las aplicaciones y de los servicios críticos de Tecnología de Información.

2ª. Sesiones de sensibilización y de capacitación al personal del Grupo de las Unidades de Negocio responsables a nivel de usuario de las aplicaciones críticas, quienes de acuerdo a la estrategia de recuperación serán trasladados al Centro Alterno de Trabajo para la continuidad de sus operaciones.

Los temas a cubrir en la capacitación están divididos en tres partes:

En la parte 1 se presentará un vídeo de sensibilización.

En la parte 2 serán cubiertos los siguientes temas:

1. Qué es un Incidente
2. Qué es un Desastre
3. Características y tipos de desastre
4. Causas de un desastre
5. Impactos provocados por un desastre
6. Qué es un Plan de Recuperación y su importancia

7. El Plan de Recuperación y la Continuidad del Negocio

En la parte 3 serán cubiertos los siguientes temas:

1. Objetivos y Alcances del Plan de Recuperación de La ESAP
2. Actividades de Preparación
3. Organización de los Grupos de Recuperación
4. Funciones y responsabilidades de los Grupos de Recuperación
5. Acciones de Respuesta ante un Desastre
6. Declaración del Desastre
7. Estrategia de Recuperación
8. Actividades de Respuesta y Recuperación
9. Activación del Plan de Recuperación
10. Actividades de Restauración
11. Regreso a la operación norma
12. Programa de Pruebas, capacitación y Mantenimiento del Plan
13. ¿Cómo actuar ante un Desastre?

Nota: Durante la parte 3 y únicamente a los Grupos de Recuperación, se llevarán a cabo una revisión de las actividades y asignación de las responsabilidades definidas en el Plan y en los procedimientos que se utilizarán para responder y recuperar la operación normal.

La capacitación se llevará a cabo en las oficinas administrativas de la **ESAP**, en sus oficinas del CAN Bogotá

9.2. Plan de Pruebas

Objetivo General:

Validar que los procedimientos, acciones, y estrategias de recuperación sean eficaces y suficientes para que los Grupos de Recuperación DRP puedan restablecer los Servicios de Cómputo 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 personales 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.

Nota: Los objetivos mencionados, son sólo enunciativos; dependiendo del alcance que se pretenda dar en la prueba, estos objetivos pueden ser modificados.

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 de la ***ESAP*** de acuerdo a la estrategia que se defina.

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

9.3. Estrategia de la Prueba:

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

Los Grupos de Recuperación de la ***ESAP*** 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, equipos y recursos que se utilizarán en las pruebas se definirán cuando se desarrolle el programa de pruebas.

Un modelo del Programa de Actividades sin considerar en este momento el detalle, podría el siguiente:

Horario	Actividades
8:00 hrs.	Llegada del Personal
8:30 a 9:00 hrs.	Requerimientos Previos
9:00 a 14:00 hrs.	Prueba
14:00 a 15:00 hrs.	Almuerzo

Horario	Actividades
15:00 a 18:00 hrs.	Resultados
18:00 a 18:30 hrs.	Reunión de Trabajo para retroalimentación y conclusiones

9.4. 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 (DRP) en general y de los procedimientos de respuesta y recuperación en particular.

Para la documentación de los resultados de la prueba, se podrá utilizar el formato que se presenta a continuación o alguno que cubra los requerimientos específicos de la **ESAP:**

DOCUMENTACIÓN DE PRUEBAS

ÁREA PARTICIPANTE: _____

FECHA DE LA PRUEBA: _____

NOMBRE Y FIRMA DEL DOCUMENTADOR DE LA PRUEBA: _____

Proceso /Procedimiento	***Probado***	***% Logro***	***Observaciones (Problema/Solución)***

Puestos Participantes	***Función /Responsabilidad***	***% Logro***	***Observaciones (Problema/Solución)***

Recursos utilizados	***Cantidad***	***Observaciones (Problema/Solución)***

Puestos Participantes	***Función /Responsabilidad***	***% Logro***	***Observaciones (Problema/Solución)***

10. ADMINISTRACIÓN DEL PLAN

Para conservar un nivel satisfactorio de preparación, es imperativo mantener toda la documentación del Plan de Recuperación y al personal que integra los Grupos de Recuperación al día y listos para responder en cualquier momento. Esta sección ofrece un panorama general de las actividades administrativas en uso que se necesitan para mantener el plan de recuperación.

10.1. Mantenimiento del Plan

Este ***Plan*** es sólo tan válido como la información que contiene. Para asegurar que el plan puede utilizarse de manera eficaz en una emergencia, debe ser preciso y estar completo. Es entonces necesario que el plan sea actualizado periódicamente, lo recomendable es que se realicen reuniones para la revisión del plan al menos cada tres meses. De igual manera, el líder de cada grupo es responsable de la identificación de todas las modificaciones y mejoras, que pueden requerirse para reflejar con precisión las responsabilidades y procedimientos de su equipo en la recuperación.

Cuando sea necesario efectuar cambios en el *Plan de Recuperación*, el líder del Grupo responsable enviará los cambios requeridos al Plan al líder del Grupo de Recuperación para su revisión. Será la responsabilidad del líder de este Grupo revisar los cambios propuestos y verificar que estos procedan.

Si el cambio es de naturaleza técnica, refleja un cambio en la logística de la recuperación, o afecta a otro Grupo de Recuperación, el líder del Grupo de Recuperación enviará la propuesta a todos los grupos afectados para su notificación y/o aprobación, si se justifica tal aprobación. Subsecuentemente, el líder del Grupo distribuirá copias de la sección(es) mejorada a todos los grupos afectados.

Luego de recibir una sección mejorada o actualizada, cada líder de grupo debe remplazar de inmediato todas las copias de la sección vieja del plan con la nueva sección actualizada y destruir las hojas sustituidas.

10.2. Distribución del Plan

Este ***Plan de Recuperación*** se distribuye al personal autorizado para auxiliar en la definición y el entendimiento de las responsabilidades y procedimientos relacionados con una interrupción no planeada de las operaciones de los Servicios de Cómputo y Comunicaciones, y en consecuencia los procesos de negocio, causada por una contingencia mayor o catastrófica. Tiene el propósito de ser utilizado sólo por el personal que sea empleado de la ***ESAP*** y que tenga alguna responsabilidad en el Plan. En caso de que se presente algún cambio de estatus del empleado miembro del Grupo de Recuperación, es responsabilidad del mismo devolver su copia y todos los duplicados de ésta o las secciones duplicadas, líder del Grupo de Recuperación. Nadie fuera de la ***ESAP*** debe ser autorizado para leer, revisar, copiar o efectuar una auditoría del plan sin una aprobación previa por escrito.

Debido al volumen y a la naturaleza de marca registrada del *Plan de Recuperación*, sólo los integrantes del Grupo de Recuperación conservarán una versión completa.

La distribución se hará como sigue:

Miembros a quienes se les distribuirá una versión completa del *Plan de Recuperación en caso de Desastre del Centro de Cómputo (DRP)* (Titular y Suplente)

- Comité Ejecutivo,
- Vocero Oficial,
- Grupo Coordinador,
- Grupo Operación Centro de Cómputo,
- Grupo Servicios de Informática,
- Grupo Comunicaciones,
- Grupo Seguridad Informática,
- Grupo Desarrollo de Sistemas,
- Grupo Mesa de Ayuda, y
- Grupo Unidades de Negocio.