

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

RST ASOCIADOS PROJECT SAS
Departamento de TI

Contenido

Departamento de TI.....	1
1. INTRODUCCIÓN.....	2
2. OBJETIVO.....	3
2.1. Objetivo General.....	3
2.2. Objetivos Específicos	3
3. ALCANCE	3
4. MARCO NORMATIVO	4
5. RESPONSABLES.....	4
6. DEFINICIONES.....	6
7. DESARROLLO DEL PLAN.....	7
7.1. DIAGNÓSTICO	8
7.2. INSTRUMENTOS QUE OPERATIVIZAN EL PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	12
7.3. ESTRATEGIA GENERAL	19
7.4. ACTIVIDADES PREVIAS A LA RECUPERACIÓN.....	20
7.5. ACTIVIDADES DE RESPUESTA Y RECUPERACIÓN	22
7.6. ADMINISTRACIÓN DEL PLAN	30
7.7. CRONOGRAMA	31
8. RECURSOS.....	32
9. SEGUIMIENTO Y MEDICIÓN DEL PLAN	32
9.1. Indicadores	32

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



PLAN DE CONTINUIDAD DE NEGOCIO - DRP

Clasificación: 2

Versión: 1.0

Fecha de Actualización:
17-Jun-2024

1. INTRODUCCIÓN

El Plan de Recuperación de Desastres establece las estrategias para mitigar el impacto ocasionado por una interrupción total de los servicios de tecnología definidos en el alcance del presente documento.

Este Plan de Continuidad de los servicios contempla los (n) planes de recuperación tecnológica (DRP) por cada servicio de TI, el cual se soporta con cada procedimiento de recuperación, en condiciones normales para su operación.

El Plan de Recuperación de Desastres (DRP) incluye los criterios para determinar cuándo un incidente afecta la Infraestructura o los servicios de Tecnologías de la Información y las Comunicaciones.

Para poder restablecer estos servicios se hace necesario planear, desarrollar, probar y llevara 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 Departamento de TI e RST Asociados tiene la responsabilidad de su desarrollo, mantenimiento y ejecución.

La necesidad de considerar un plan para recuperar los servicios tecnológicos se desprende de la posibilidad de un evento catastrófico que interrumpa la operación normal de RST ASOCIADOS PROJECT SAS afectando totalmente los servicios tecnológicos definidos como críticos en el análisis de impacto del negocio.

Este documento ofrece un panorama general de la estructura del plan, los objetivos, el alcance, las premisas iniciales, las estrategias predeterminadas, y las acciones para la recuperación de la Infraestructura Tecnológica. 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 Infraestructura Tecnológica a su condición operativa.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

2. OBJETIVO

2.1. Objetivo General

Definir los mecanismos y acciones a seguir para restablecer los servicios de tecnología de la información que soporta los procesos críticos RST ASOCIADOS PROJECT SAS.

2.2. Objetivos Específicos

- Dar continuidad a los servicios tecnológicos de RST ASOCIADOS PROJECT SAS 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 definidas por el Departamento de TI de una manera oportuna, incrementando la habilidad RST ASOCIADOS PROJECT SAS para recuperarse de una pérdida o daños a las instalaciones y servicios.

3. ALCANCE

El Plan de Recuperación de Desastres (DRP) se realiza para la infraestructura y servicios de Tecnología del DEPARTAMENTO DE TI, que se encuentran en las instalaciones de la RST ASOCIADOS PROJECT SAS ubicadas en el Datacenter Principal que soporta las aplicaciones críticas en las diferentes sedes.

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

- 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 un terremoto o inundación.
- Cierre de las instalaciones por recomendación de la Secretaría de Salud cuando sea aplicable.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

4. MARCO NORMATIVO

TIPO DE NORMA	NÚMERO	AÑO	Descripción – Epígrafe
ISO 27001	Seguridad de la información	2022	Establecer la política y los objetivos de gestión de la seguridad de la información y a comprender cómo se pueden gestionar los aspectos importantes, aplicar los controles necesarios y establecer objetivos claros para mejorar la seguridad de la información.

5. RESPONSABLES

Rol/Cargo	Actividades antes de evento de interrupción	Actividades durante el evento de interrupción	Actividades después del evento de interrupción
DIRECTOR DE TI	<ul style="list-style-type: none">• Determinar el momento preciso de la Declaración del Desastre con base a la evaluación inicial del incidente registrado en GLPI y el diagnostico del Departamento de TI.• 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.• Actualizar el plan de recuperación de desastres en el momento que se presenten cambios.	<ul style="list-style-type: none">• Autorizar la activación del Equipo de Respuesta y Recuperación (Comité de crisis).• Evaluar el impacto y cálculo de los daños físicos.• Dirigir las operaciones generales de los Equipos de Recuperación.• Mantener y difundir los reportes del estatus de la contingencia.	<ul style="list-style-type: none">• Analizar el impacto del incidente o desastre.• Apoyar el retorno a la normalidad.• Identificar oportunidades de mejora del plan de recuperación de desastres.• Validar la viabilidad del retorno a la normalidad.• Actualizar el plan de recuperación de desastres y/o procedimientos que tengan oportunidades de mejora.

Los roles y el personal actual responsable asignado se encuentra en el Anexo Personal técnico Equipo
DRP de este documento.

Rol/Cargo	Actividades antes de evento de interrupción	Actividades durante el evento de interrupción	Actividades después del evento de interrupción
Director de TI/ Líder DRP	<ul style="list-style-type: none">Planificar las pruebas del plan de recuperación de desastres.Coordinar la capacitación del personal.Coordinar la documentación de los planes de recuperación de cada uno de los componentes críticos de recuperación.	<ul style="list-style-type: none">Coordinar y guiar el Plan de Acción para ese incidente en particular.Coordinar y ejercer la autoridad sobre las actividades de cada Equipo de trabajo individual para asegurar la reanudación de las actividades del negocio dentro de los Tiempos Objetivos de Recuperación (RTO), no mayor a 5 horas.	<ul style="list-style-type: none">Coordinar la restauración, reconstrucción y/o reemplazo de las instalaciones y equipo afectados.Presentar un reporte de los daños a las instalaciones y equipo de sistemas.
Equipo de Recuperación / Equipo de Datacenter, Infraestructura de Servicios Tecnológicos, Telecomunicaciones, Seguridad y Privacidad de la Información, Desarrollo de Sistemas, Sistemas de Información y Mesa de Ayuda	<ul style="list-style-type: none">Documentar cada uno de los planes de recuperación.Ejecutar las pruebas de los planes de recuperación.	<ul style="list-style-type: none">Participar en las actividades de Recuperación y Respuesta.Notificar y asignar personal de acuerdo con el Plan de Acción.Participar en la evaluación de daños.	<ul style="list-style-type: none">Supervisar que la infraestructura principal se Encuentre lista para reanudar a la normalidad.Generar un reporte de evaluación final al concluir el proceso de recuperación.Realizar las actividades para el retorno a la normalidad.

6. DEFINICIONES

Sigla / Término	Descripción
Aplicaciones Críticas	Son aquellas aplicaciones que soportan los procesos relacionados con la misión de RST ASOCIADOS PROJECT SAS y dependiendo de su naturaleza, estarán orientados principalmente a la operación misma del negocio y a aquellas actividades relacionadas con el flujo educativo de RST ASOCIADOS PROJECT SAS. Ante una contingencia, las aplicaciones críticas no pueden postergar su operación por un tiempo prolongado.
Datacenter 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 RST ASOCIADOS PROJECT SAS en sus oficinas principales.
Centro de Control de Crisis(CCC)	Es una zona de encuentro dentro o fuera de RST ASOCIADOS PROJECT SAS desde donde se llevan a cabo las actividades iniciales de evaluación, coordinación y de toma de decisiones relativas a un incidente no planeado.
Desastre	Evento repentino no planeado que ocasiona la “no disponibilidad” de los servicios informáticos por un tiempo tal que, para restablecer estos servicios, es necesario facilidades alternas de cómputo y comunicaciones en otra localidad.
DRP	<p>Acrónimo de Disaster Recovery Plan (en inglés). Plan de Recuperación de Desastres.</p> <p>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 ladisponibilidad de los servicios de cómputo, aplicaciones ycomunicaciones que permiten mantener la continuidad de las operaciones de la organización soportadas por las Tecnologías de la Información.</p> <p>En un DRP, las unidades de negocio no son las responsables de restablecer los servicios de cómputo, aplicaciones ycomunicaciones. El responsable es la Oficina de Tecnologías de la Información y las Comunicaciones.</p>
Equipos de Recuperación	Personas con perfiles, responsabilidades y habilidades específicascon el fin de encauzar esfuerzos para dirigir, coordinar y habilitar los elementos que permiten la operación de los procesos informáticos del negocio.
Equipo Coordinador	Personas encargadas de coordinar y controlar las acciones arealizarse antes, durante y después de la contingencia, a través de los Equipos de Recuperación.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

7. DESARROLLO DEL PLAN

Sigla / Término	Descripción
Líder de Equipo	Persona responsable de un Equipo de Recuperación quién toma asu cargo la responsabilidad global de las funciones de ese Equipo durante una contingencia.
Líder suplente de Equipo	Persona que asume las funciones del líder del Equipo en caso de que éste no se encuentre disponible.
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 críticasde operación de sistemas y de RST ASOCIADOS PROJECT SAS.
BCP	El BCP se enfoca en sostener las funciones de negocio de RST ASOCIADOS PROJECT SAS,durante y después de una interrupción mientras se recupera paralelamente. El BCP se orienta hacia los procesos de negocio. Por su parte, el DRP provee procedimientos detallados para facilitar la recuperación de las capacidades en sitio alternativo. Normalmente está enfocado en Tecnologías de la Información (enadelante TI) y limitado a interrupciones mayores con efectos a largo plazo. Los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y recuperarservicios críticos de TI después de una emergencia. Debido a que los planes de contingencia deben ser desarrollados para cada aplicación importante o sistema de soporte, se pueden contar conmúltiples planes de contingencia dentro de un BCP.
PUNTO OBJETIVO DE RECUPERACION (RPO)	Punto en el tiempo en que la información debe ser restaurada para permitir al proceso operar una vez se normalice la operación.
TIEMPO OBJETIVO DE RECUPERACION (RTO)	El tiempo establecido para la reanudar la entrega de productos, servicios o actividades después de ocurrir un incidente.
MDT	Porcentaje de servicio entregado durante la operación bajo el DRP. Corresponde a la determinación de los tiempos máximos tolerables de interrupción.
Unidad de Negocio (UN)	Cualquier área de RST ASOCIADOS PROJECT SAS que realiza actividades que forman parte del ciclo del CallCenter. Generalmente son dependientes de la tecnología de cómputo, comunicaciones y de servicios de apoyo.
BIA	Análisis de Impacto al Negocio, para identificar los procesos críticos.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

7.1. DIAGNÓSTICO

Desde el mes de mayo del año 2024 se realizó el Análisis de Impacto al Negocio Táctico y Operativo.

Como parte preliminar al desarrollo del Plan de Recuperación (DRP) para los servicios tecnológicos, 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). El listado de aplicaciones de RST ASOCIADOS PROJECT SAS y su criticidad.

La vulnerabilidad en los procesos de RST ASOCIADOS PROJECT SAS 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 que fueron evaluadas por cada uno de los líderes de los procesos:

Nivel de impacto	Tiempo Objetivo de Recuperación (RTO)
1	Se podría generar un impacto alto para RST ASOCIADOS PROJECT SAS al detenerse el proceso por más de 15 días
2	Se podría generar un impacto alto para RST ASOCIADOS PROJECT SAS al detenerse el proceso por un rango de tiempo entre 5 y 10 días
3	Se podría generar un impacto alto para RST ASOCIADOS PROJECT SAS al detenerse el proceso por un rango de tiempo entre 5 y 3 días
4	Se podría generar un impacto alto para RST ASOCIADOS PROJECT SAS al detenerse el proceso por un rango de tiempo entre 3 y 1 día
5	Se podría generar un impacto alto para RST ASOCIADOS PROJECT SAS al detenerse el proceso por 8 horas o menos

Se determinaron las aplicaciones y servicios críticos, su RTO`s, RPO`s y MTD`s de cada aplicación de acuerdo con la información recolectada en el Análisis de Impacto al Negocio Táctico y Operativo, con el siguiente resultado de acuerdo con la información dada por cada uno de los líderes de los procesos:

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



PLAN DE CONTINUIDAD DE NEGOCIO - DRP

Clasificación: 2

Versión: 1.0

Fecha de Actualización:
17-Jun-2024

ACTIVO DE INFORMACIÓN	RTO	RPO	MDT	PERCEPCIÓN DE CRITICIDAD
Correo electrónico	8 horas	2 horas	2 horas	MUY CRITICO
Office 365 (Correo, Teams, Google Drive, PBI)	8 horas	2 horas	2 horas	MUY CRITICO
Internet Dedicado claro	8 horas	2 horas	2 horas	MUY CRITICO
Internet Dedicado BK Claro	8 horas	2 horas	2 horas	MUY CRITICO
Internet dedicado Movistar	8 horas	2 horas	2 horas	MUY CRITICO
Neotel	8 horas	2 horas	2 horas	MUY CRITICO
Anw	8 horas	2 horas	2 horas	MUY CRITICO
Bytecol Technology Systems SAS	8 horas	2 horas	2 horas	MUY CRITICO
U-contact	8 horas	2 horas	2 horas	MUY CRITICO
Red MPLS Claro	8 horas	2 horas	2 horas	MUY CRITICO
Troncal SIP PBX Distribuida Claro	8 horas	2 horas	2 horas	MUY CRITICO
Troncal SIP Centralizada Claro	8 horas	2 horas	2 horas	MUY CRITICO
Troncal SIP Fija Movistar	8 horas	2 horas	2 horas	MUY CRITICO
018000 nacional ETB	8 horas	2 horas	2 horas	MUY CRITICO
SQL, MySQL, PostgreSQL	8 horas	2 horas	2 horas	MUY CRITICO
Página Web RST Asociados Project SAS	8 horas	2 horas	2 horas	CRITICO
Iperius Backup	8 horas	2 horas	2 horas	CRITICO
Zabbix	8 horas	2 horas	2 horas	CRITICO
GlpI	8 horas	2 horas	2 horas	CRITICO
ZTECO-Biométrico	8 horas	2 horas	2 horas	CRITICO
Moodle	8 horas	2 horas	2 horas	CRITICO
File Server	3 días	2 horas	2 horas	CRITICO
Directorio Activo	3 días	2 horas	2 horas	CRITICO

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



PLAN DE CONTINUIDAD DE NEGOCIO - DRP

Clasificación: 2

Versión: 1.0

Fecha de Actualización:
17-Jun-2024

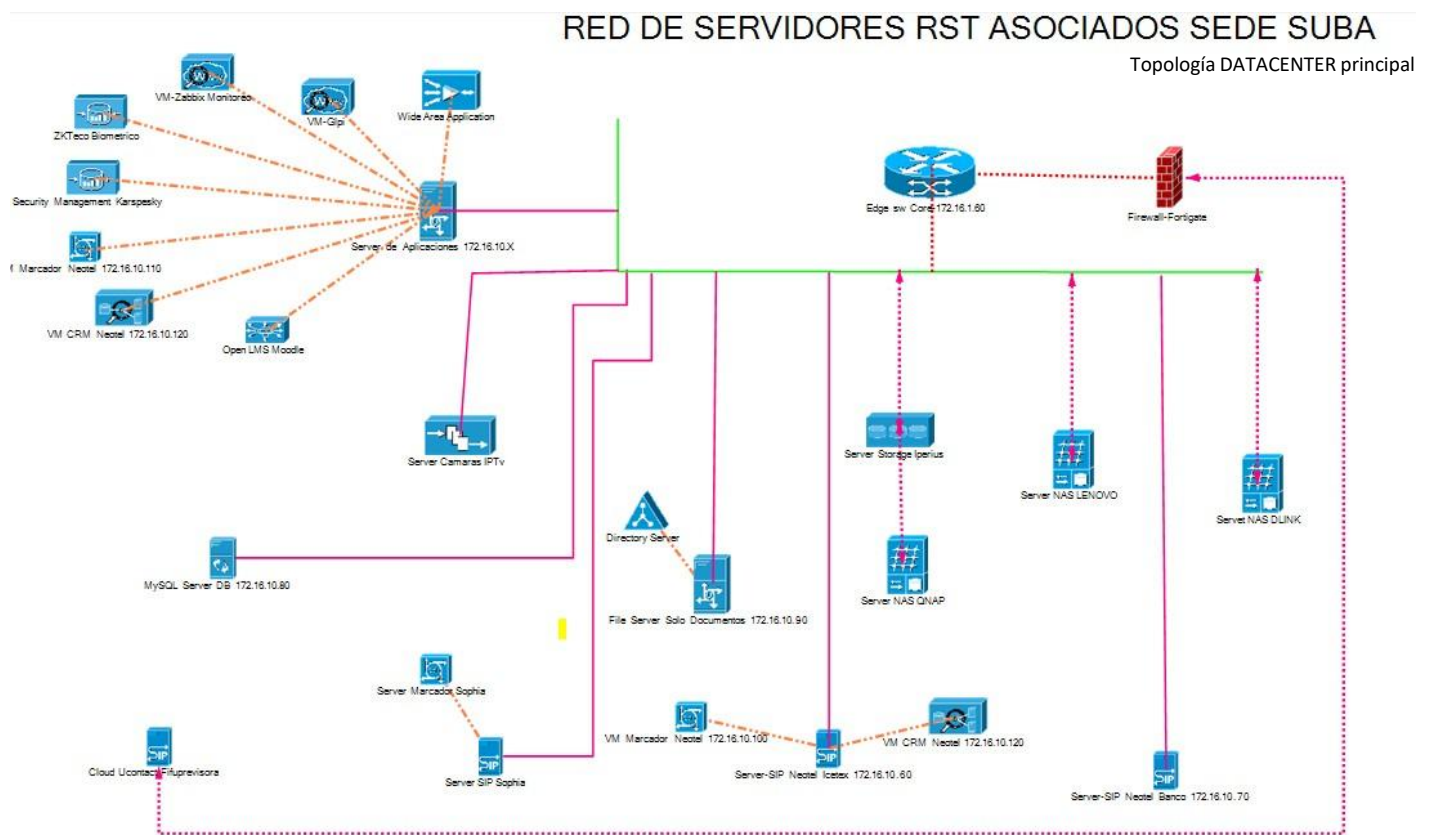
En el Análisis de Impacto al negocio se incluyen la información consolidada de los servicios de tecnología, y el listado de los procesos con sus procedimientos y las aplicaciones críticas que utilizan para determinar el RTO y la criticidad de estos.

RST ASOCIADOS PROJECT SAS Cuenta con un Departamento de TI con Ingenieros profesionales en Infraestructuras de Servidores y de Telecomunicaciones, Helpdesk, Desarrollo de Software y Seguridad de la información.

7.1.1. Situación Actual de los Servicios de Cómputo y Comunicaciones

El Data Center Principal se encuentran en las instalaciones de RST ASOCIADOS PROJECT SAS en la sede SUBA.

La infraestructura y recursos actuales que soportan los servicios muy críticos y críticos indicados anteriormente corresponden a la siguiente arquitectura:



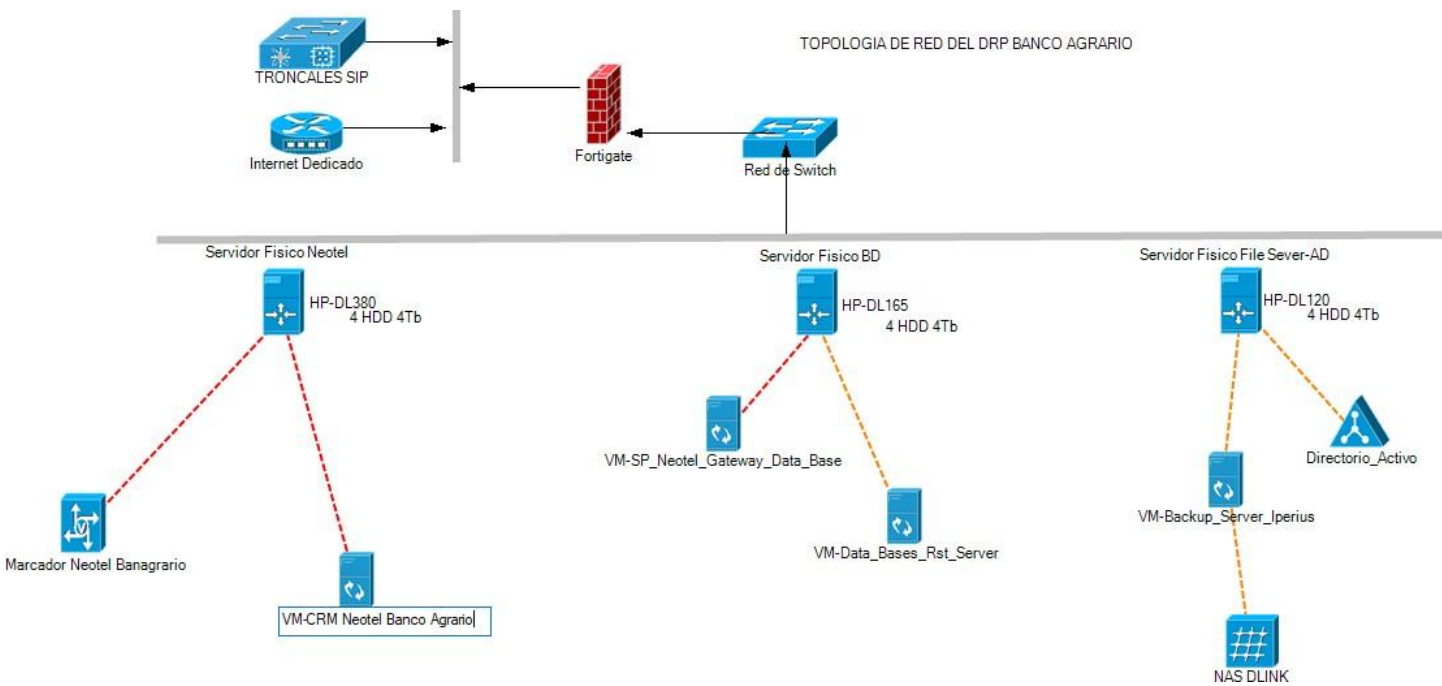
Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



PLAN DE CONTINUIDAD DE NEGOCIO - DRP

Clasificación: 2
Versión: 1.0
Fecha de Actualización: 17-Jun-2024

Diagrama DRP en Datacenter



Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

7.2. INSTRUMENTOS QUE OPERATIVIZAN EL PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS

7.2.1. Estrategia

Objetivo General:

Validar que los procedimientos, acciones, y estrategias de recuperación sean eficaces y suficientes para que el Equipo 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 Equipos de Recuperación.
- Verificar la funcionalidad de los procedimientos de activación del plan, la respuesta a la emergencia, de recuperación y el nivel de preparación del personal que participará en las actividades.
- Verificar que los usuarios de las aplicaciones críticas puedan operar en el centro Alternativo de Trabajo en los tiempos definidos.
- Validar que los recursos definidos en el MARC (Herramienta para evaluar el desempeño de un programa o aplicación) cubran las necesidades de operación en modo contingente y de recuperación.

Alcance:

El alcance, fecha y tipo de prueba a realizarse, se definirá antes de la prueba y se tomará como base el nivel de preparación de la RST ASOCIADOS PROJECT SAS de acuerdo con la estrategia que se defina.

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

7.2.2. Estrategia de la Prueba

La prueba estará relacionada con las estrategias definidas por la RST ASOCIADOS PROJECT SAS para la recuperación de la operación normal.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

Los Equipos de Recuperación de RST ASOCIADOS SAS 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 Equipo antes de la misma.

Como responsables de la Coordinación General, participarán el Equipo de Recuperación y los lideres decada Equipo, 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 (ejemplo) 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
15:00 a 18:00 hrs.	Resultados
18:00 a 18:30 hrs.	Reunión de Trabajo para retroalimentación y conclusiones

7.2.3. Tipo de Prueba

Pruebas de escritorio (Detallada y documental): Se trata de un tipo de prueba programada y controlada que consiste en una revisión detallada del DRP con sus procedimientos. Para su ejecución se verifica la existencia del plan y sus procedimientos, y se convoca a los diferentes equipos de recuperación a participar del Líder del equipo Coordinador del DRP, con el fin de determinar fallas y omisiones con el criterio experto de quienes participan.

Pruebas reales (Tecnológicas): Son pruebas en donde se involucra la activación del Datacenter Alterno. Este tipo de prueba puede ser parcial o total, donde se prueban secciones o elementos individuales del Plan de Recuperación, como puede ser un aplicativo o una plataforma, o se prueban todos los componentes.

Pruebas de unidad: Se prueba cada elemento que compone la solución de respaldo en forma independiente. No se afectan los servicios de producción.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

Pruebas integrales (Cerradas): Se prueban en forma integrada todos los componentes de la solución de respaldo sin afectar los servicios de producción.

Pruebas totales: Verifican el funcionamiento de todos los elementos descritos en el Plan de Recuperación de Desastres.

Es importante repetir este ejercicio tantas veces como se considere necesario para adquirir un muy buen nivel de conocimiento y práctica. Una vez realizado este último tipo de ejercicio en varias oportunidades, el cual es programado y controlado, se puede pasar a la ejecución de estas pruebas en forma no programada, pero si controlada, teniendo en cuenta seguir un protocolo como el expuesto antes. Las primeras veces en horario no hábil y luego en horario hábil.

7.2.4. Documentación de la Prueba

Los líderes de cada Equipo de Recuperación y el líder del Equipo 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.

7.2.5. Análisis Riesgos - 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 Riesgos de TI”. En este análisis se identifican los riesgos potenciales que pudieran afectar las estrategias de recuperación de los sistemas críticos para a través de los planes de tratamiento se establezcan las acciones para prevenirlos y mitigarlos.

- Riesgos a nivel de Administración de Datacenter: 79% de potenciales amenazas controladas.

Dentro de los riesgos identificados a nivel de Datacenter se encuentra:

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

LISTA DE RIESGOS IDENTIFICADOS				
No.	¿QUÉ PUEDE SUCEDER? (Consecuencia)	¿POR QUÉ PUEDE SUCEDER? (Fuente de Riesgo)	¿CÓMO PUEDE SUCEDER? (Escenario o Evento Puntual)	DESCRIPCIÓN DEL EVENTO DE RIESGO POTENCIAL IDENTIFICADO
1	Posible accidente por traslado de equipos	Los equipos del asesor debes ser trasladados de la sede principal a la sede alterna	La sede alterna se encuentra a 5 km de distancia de la sede principal y se pueden presentar accidentes con el transporte de equipos de RST ASOCIADOS PROJETC SAS por parte de los proveedores	Posible daño de equipos en la sede alterna de RST ASOCIADOS PROJETC SAS
2	Espacio locativo limitado para acceder al Datacenter	La distribución del espacio de las instalaciones es pequeña	Si se requiere que ingresen más de dos personas se va a generar un inadecuado flujo para entrar y salir	Posible pérdida de tiempo para solucionar algún incidente.
3	Incendio	Sala de UPS y banco de Baterías no cuenta con extractor de aire	Incendio en la sala de UPS y banco de Baterías	Incendio en Datacenter
4	Incendio	Falta espacio entre Racks para controlar el flujo decalor en el Datacenter	Sobrecalentamiento de equipos	Incendio en Datacenter. Daño de equipos por sobrecalentamiento de los mismos.

- Riesgos a nivel de Telecomunicaciones: 65% de potenciales amenazas controladas.

Dentro de los riesgos identificados a nivel de Telecomunicaciones se encuentra:

LISTA DE RIESGOS IDENTIFICADOS				
No.	¿QUÉ PUEDE SUCEDER? (Consecuencia)	¿POR QUÉ PUEDE SUCEDER? (Fuente de Riesgo)	¿CÓMO PUEDE SUCEDER? (Escenario o Evento Puntual)	DESCRIPCIÓN DEL EVENTO DE RIESGO POTENCIAL IDENTIFICADO
1	Posible apagado o daño de equipos	Falla en Routers y Switches por falta de redundancia de fuente de poder y procesadores	Por falta de redundancia en todos los equipos de fuente de poder y procesadores en Routers y Switches se puede presentar daño o apagado de equipos	Posible daño apagado inesperado y/o daño de equipos en el Datacenter por no contar con redundancia en fuente de poder y procesadores
2	No identificación correcta de equipos y posible desconexión de equipos	Falta de rotulado de equipos en la parte frontal y trasera	Al no tener la debida rotulación de los equipos se puede presentar accidentes al desconectar equipos no identificados	Desconexión de equipos por falta de rotulado y deficiencia en la identificación de estos

- Riesgos a nivel Eléctrico: 42% de potenciales amenazas controladas. De ellas la mayoría se encuentran pendientes por confirmar con Infraestructura TI.

Dentro de los riesgos identificados a nivel Eléctrico se encuentra:

LISTA DE RIESGOS IDENTIFICADOS				
No.	¿QUÉ PUEDE SUCEDER? (Consecuencia)	¿POR QUÉ PUEDE SUCEDER? (Fuente de Riesgo)	¿CÓMO PUEDE SUCEDER? (Escenario o Evento Puntual)	DESCRIPCIÓN DEL EVENTO DE RIESGO POTENCIAL IDENTIFICADO
1	No disponibilidad de equipos para la prestación del servicio	Falta de Sistema EPO (Emergency Power Off) para sala de computadores y sala de baterías	Por falta de configuración del EPO se puede presentar daño en el equipo conectado al no apagarse instantáneamente la UPS y el equipo conectado en caso de un incendio o una emergencia	Posible daño de equipos que no permiten la continuidad del servicio
2	Desatención de alertas	Falta de un Sistema de Monitoreo: Energía Central, variables ambientales y control de sistema con ingeniero en consola remota y manual con resumen de todos los controles automáticos y puntos de referencias	Al no tener el sistema de monitoreo se puede presentar desatención de alertas que pueden generar daños a los equipos	Daño de equipos por falla en el sistema eléctrico.
3	Falla eléctrica	No se cuenta con una segunda planta eléctrica en caso de que la planta principal falle	Al solo tener una Planta eléctrica se puede presentar riesgo eléctrico en los equipos de computo	Daño de equipos por falla en el sistema eléctrico

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

- Riesgos a nivel de Seguridad Informática: 75% de potenciales amenazas controladas.

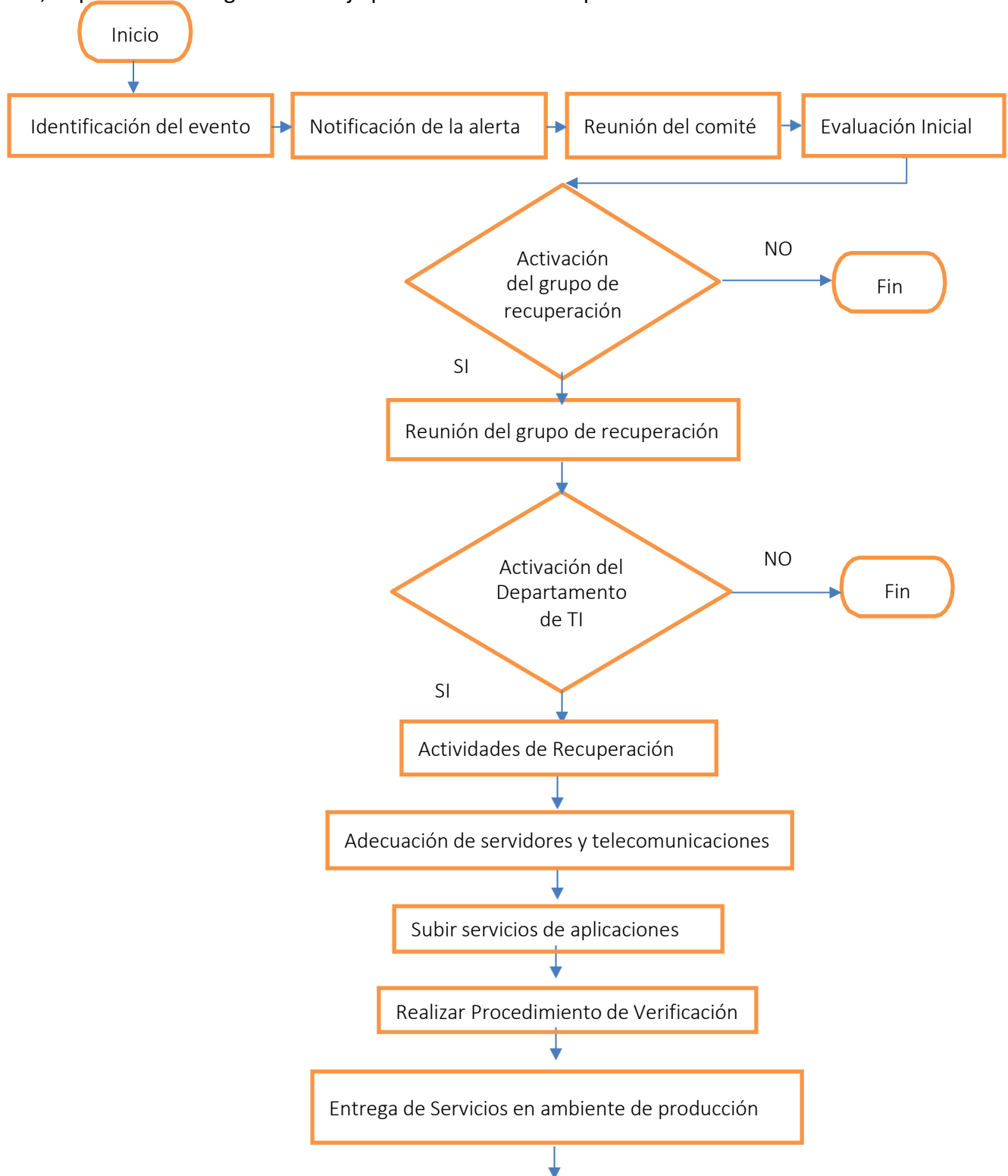
Dentro de los riesgos identificados a nivel de Seguridad de la Informática se Encuentra:

LISTA DE RIESGOS IDENTIFICADOS				
No.	¿QUÉ PUEDE SUCEDER? (Consecuencia)	¿POR QUÉ PUEDE SUCEDER? (Fuente de Riesgo)	¿CÓMO PUEDE SUCEDER? (Escenario o Evento Puntual)	DESCRIPCIÓN DEL EVENTO DE RIESGO POTENCIAL IDENTIFICADO
1	Errores de puesta en producción de componentes de pruebas	No se cuenta con ambientes separados para todos los servicios (pruebas y producción)	Se puede presentar implementaciones en producción de componentes que estaban en pruebas y se puede generar errores en el servicio y/o pérdida de servicio	Pérdida de servicio de aplicaciones y/o equipos
2	Falla en sistemas de información	Falta de documentación de planes de recuperación de los sistemas de información	Al presentarse un problema en un sistema de información que no se cuente con la documentación del uso, operación y activación del sistema de información se pueden presentar fallas que no se sabe cómo se pueden solucionar	Dificultad en la recuperación del sistema de información por falta de documentación en las actividades de recuperación
3	Falla de sistema de información	No se cuenta con todos los procedimientos alternos o manuales, cuando no se tiene disponible el sistema de información	Al presentarse un evento de interrupción no se tiene un documento para realizarla recuperación del servicio	Indisponibilidad de servicios, aplicaciones y/o sistemas de información al no poder recuperar su operación
4	Falla en los sistemas de información	Ataque Cibernético por falla en los controles de Seguridad	No se tiene monitoreo constante sobre la plataforma o fallan las herramientas de protección	Falla en los sistemas por actividades ilícitas externas.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

7.2.6. Activación del Plan

A continuación, se presenta el diagrama de flujo para la activación del plan:



Elaborado por: Director de T. I

Fecha: 15/06/2024

Revisado por: Auditor interno

Fecha: 17/06/2024

Aprobado por: Presidente

Fecha: 17/06/2024

Imagen 2 – Diagrama de activación del plan

7.2.7. Estrategia de Recuperación de aplicaciones

Considerando las necesidades de recuperación de RST ASOCIADOS PROJECT SAS y de acuerdo con los resultados del Tiempo objetivo de Recuperación (RTO) definidos por las diversas Unidades de Negocio del Call Center, la estrategia de recuperación definida por RST ASOCIADOS PROJECT SAS es la de Alta Disponibilidad, para aquellas aplicaciones que resultaron con un RTO menor de 8 horas y 3 días que requieren un nivel muy elevado de confiabilidad y disponibilidad. La estrategia es a través de una copia de seguridad de las bases de datos y aplicaciones que puedan entrar en operación en la sede alterna con instalaciones de cómputo disponibles capaces de operar de manera inmediata.

7.2.8. 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 los procesos misionales como del proceso de gestión tecnológica. Los recursos mínimos incluyen todos los registros vitales requeridos para continuar la operación.

7.3. ESTRATEGIA GENERAL

7.3.1. 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.
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 Incidencias utilizados día a día por el Departamento de TI de RST ASOCIADOS PROJECT SAS.
- Contingencia Mayor: Provocada por incidentes que afectan el acceso a los servicios de cómputo y comunicaciones interrumpiendo la operación normal de RST ASOCIADOS PROJECT SAS por un periodo mayor a 24 horas.

De presentarse una contingencia mayor en los equipos y sistemas de las oficinas de RST ASOCIADOS PROJECT SAS, 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

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

el equipo 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: 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.

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

Una vez activado el Plan de Recuperación, el Equipo Coordinador y los líderes de cada Equipose reunirán en el Centro de Control de Crisis para sesionar y tomar decisiones acerca de la recuperación.

7.4. ACTIVIDADES PREVIAS A LA RECUPERACIÓN

Las actividades de los Equipos de Recuperación se dividen en actividades de Preparación y actividades

Contingencia Catastrófica	Interrupción por un tiempo mayor a 15 días. Impacto toda la operación de RST Asociados Project SAS.
Contingencia Mayor	Afecta servicios de telecomunicaciones, Servidores y sistemas de cómputo. Interrumpe la operación normal por un periodo mayor a 24 horas.
Contingencia menor	Eventos que afectan a uno o varios procedimientos, por un periodo menor a 24 horas.

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 afinancon los procesos de pruebas.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



En términos generales se deben realizar las siguientes actividades para estar preparados ante cualquier evento contingente:

- Directorio de Equipo de recuperación actualizado y árbol de llamadas.
- Tener actualizado criticidad de Equipos de recuperación.
- Que los cambios realizados sean documentados en los planes de recuperación.
- Definir responsable de actualización de cada plan.
- Establecer política de comunicación para la notificación del desastre.
- Realizar pruebas de los planes de recuperación.
- Tener los planes documentados en un lugar externo a la sede central de RST ASOCIADOS PROJETC SAS.
- Realizar capacitaciones a los integrantes del Plan de recuperación.
- Mantener actualizado el directorio de proveedores, ANS establecidos, vigencia de contratos o convenios establecidos con estos proveedores para atender necesidades inmediatas en casos de desastre.
- Mantener actualizados los requerimientos mínimos de hardware, software y comunicaciones (MARC) para restablecer la operación en el Datacenter Alterno
- Verificar que el procedimiento de respaldo diario y semanal de Bases de Datos y aplicaciones críticas termine exitosamente
- Verificar que se cuente con repositorio NAS como respaldo de datos, sistema operativo, perfiles de usuario, seguridad de acceso a usuarios a la información, configuración física y lógica por triplicado, ubicar una de ellas en el Site productivo, otra en la bóveda externa y la última en el Datacenter Alterno.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



PLAN DE CONTINUIDAD DE NEGOCIO - DRP

Clasificación: 2

Versión: 1.0

Fecha de Actualización:
17-Jun-2024

- Realizar revisión de la carga de volúmenes, subsistemas y rendimiento (performance) del CPU.
- Mantener actualizado la relación de software, equipos y componentes de comunicaciones.
- Recuperar y verificar la copia del software base que deberá ser utilizado para levantarlos enlaces.
- Monitoreo de Equipos Centrales y Alterno y del servicio de antivirus central y alterno.

7.5. ACTIVIDADES DE RESPUESTA Y 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 Equipo 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 Datacenter. 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.

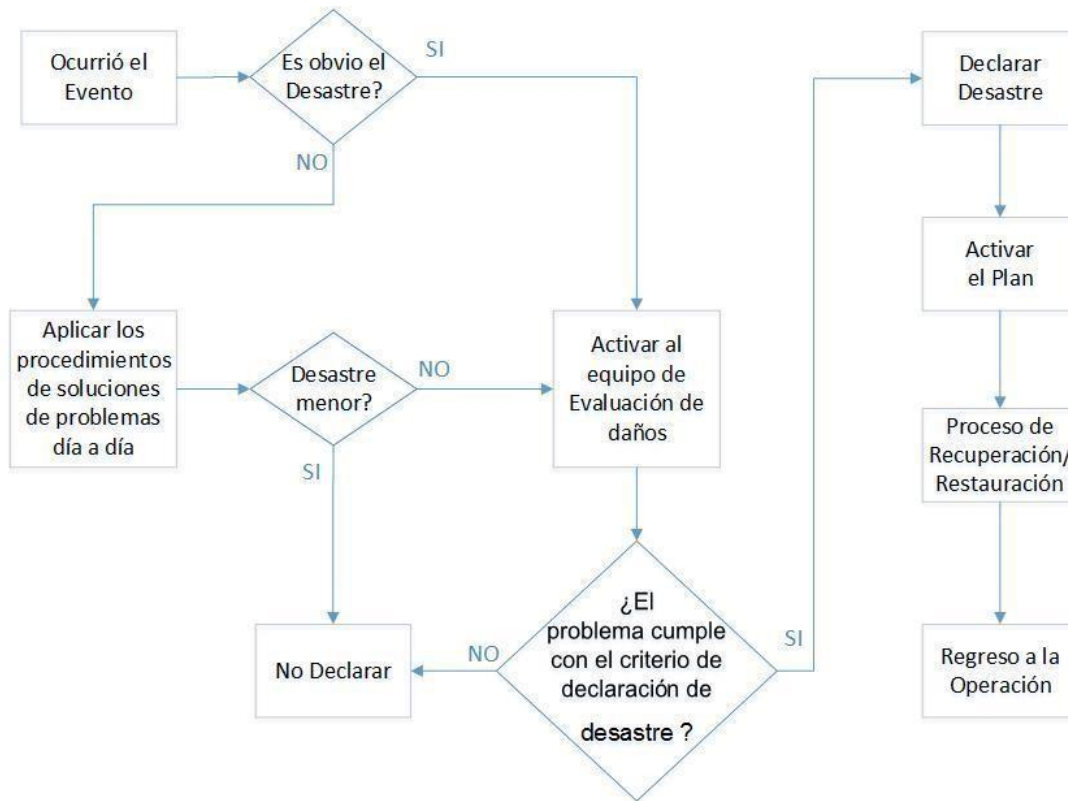
La identificación o reconocimiento de un evento provoca el inicio de las actividades de respuesta a una emergencia y los Procedimientos de Evaluación de Daños. Dependiendo del diagnóstico de la evaluación, se decide la Activación del Plan, y la notificación al Equipo Coordinador.

Los procedimientos de recuperación documentan la evaluación inicial, la decisión y las actividades de inicio del Equipo Coordinador. Como se ha mencionado, este Equipo 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 Equipo 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 RST ASOCIADOS PROJECT SAS.

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.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



Declaración de desastre

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

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 Datacenter 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 Datacenter o instalaciones Alternas de Trabajo.
- Preparar equipos e instalar los clientes de las aplicaciones en el Datacenter o instalaciones Alternas de Trabajo.
- Restablecer el acceso a la red local y a los sistemas de cómputo centralizados.
- Obtener los datos protegidos (Backup) conservados fuera de RST ASOCIADOS PROJETC SAS.
- Contactar a los proveedores de bienes y servicios de Infraestructura Tecnológica que sean necesarios para apoyar la recuperación.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

- Coordinar todas las actividades de soporte para la restauración del Datacenter afectado.
- Coordinar la reinstalación del Datacenter afectado una vez que ha sido restaurado.
- Coordinar con todos los Equipos de Recuperación una reunión de evaluación del proceso del Plan.
- Generar un reporte de evaluación a la Dirección General.

7.5.1. Procedimientos de Respuesta Inmediata

Implementar los procedimientos de respuesta inmediata basados en las circunstancias específicas del evento; 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

¿Qué hacer en caso de falla del equipo de Cómputo?

Responsables:

DEPARTAMENTO DE TI.

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 Equipo Coordinador de inmediato.
- Contactar de inmediato, al (los) proveedor(s) del equipo que presentó problema, consultando la relación de Proveedores.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

¿Qué hacer en caso de falla del equipo de apoyo?

Responsables:

DEPARTAMENTO DE TI.

- Si fallan los equipos de Aire Acondicionado, intente restaurar los dispositivos que fallan accionandolos switches de arranque.
- Notificar de inmediato al área de Mantenimiento y soporte de RST ASOCIADOS PROJECT SAS
- Notificar al Equipo Coordinador de inmediato.
- Apague las lámparas no indispensables en la sala de Cómputo.
- Siga las instrucciones del Departamento de TI 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.

¿Qué hacer en caso de falla de Software base?

Responsables:

DEPARTAMENTO DE TI.

Solución de Problemas

- Identifique el Problema para ser reportado al Equipo de Operación del Datacenter de inmediato.
- Contacte al Equipo de Mesa de Ayuda.

¿Qué hacer en caso de falla de Software Aplicativo?

Responsables:

- DEPARTAMENTO DE TI.
- Proveedor Responsable de Sistemas de la Aplicación.

Solución de Problemas

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

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

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 Datacenter Alterno 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 diferentes destinos, en donde están habilitadas estaciones de trabajo en el caso de una interrupción por mayor tiempo.

7.5.2. 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 Datacenter como una guía. Después, coordinar el regreso a las instalaciones permanentes (nuevas o reconstruidas) al concluir la operación de 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.

- Probar que el Datacenter Principal (afectado inicialmente) esté listo para ser utilizado.
- Coordinar la fecha de regreso a las actividades normales.
- Comunicar a la Dirección General la terminación del desastre.
- Notificar al personal de Sistemas el regreso a la operación normal.
- Verificar que obtengan los respaldos de los archivos modificados del Datacenter Alterno.
- Verificar que las comunicaciones estén enrutadas al Datacenter nuevo.
- Suspender los servicios contratados durante el desastre, ya sea temporal o de forma permanente.
- Coordinar la reinstalación de las actividades en las Oficinas administrativas.
- Coordinar que cada Equipo revise que los documentos, manuales, catálogos, directorios, etc. utilizados en el Datacenter de Trabajo Alterno estén de nuevo en las Oficinas Administrativas.
- Evaluar el Plan de Contingencia y el desempeño del personal durante el desastre.
- Solicitar retroalimentación de los participantes del Plan.

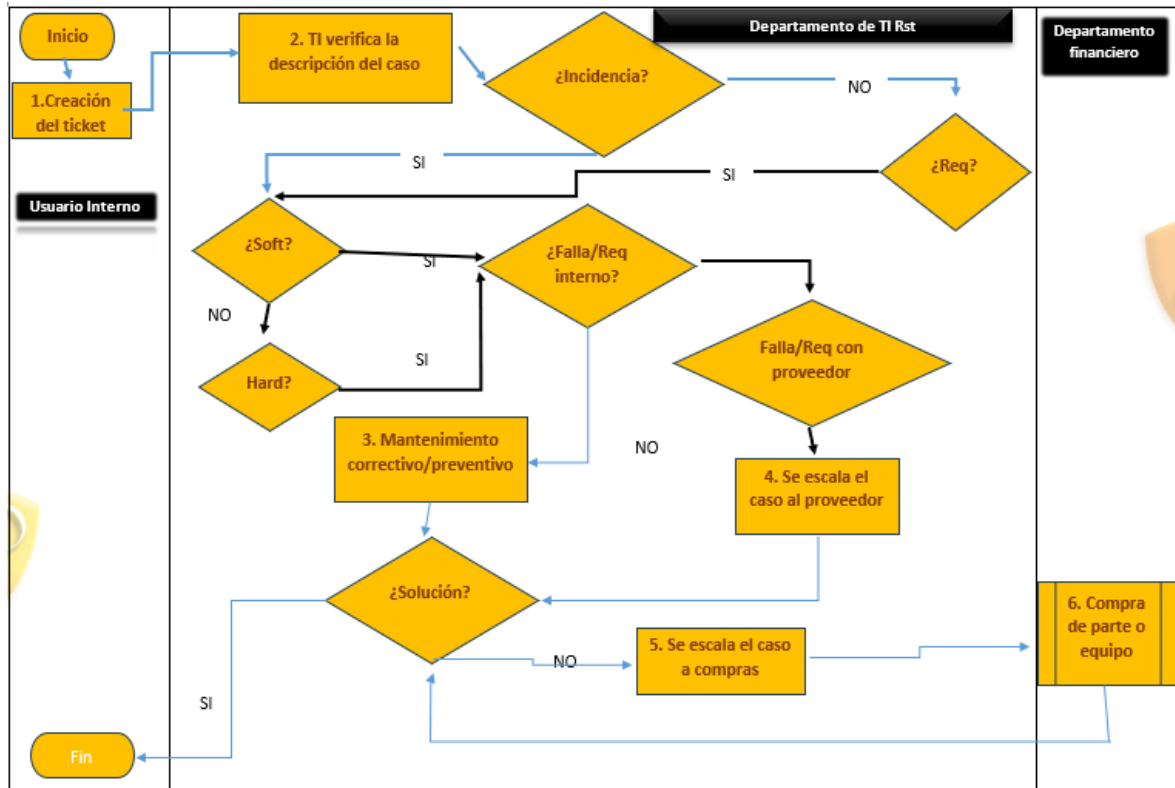
7.5.3. Gestión de Incidentes

En el proceso de DRP se debe enlazar con la Gestión de Incidentes de RST ASOCIADOS PROJECT SAS, dado que un incidente se puede convertir en un problema o en un incidente que genere una indisponibilidad en la infraestructura tecnológica o afectar a una o varias aplicaciones; por ende, el procedimiento de Gestión de Incidentes se encuentra articulado con el Plan de Recuperación de Desastres y se identifica el momento en que por un incidente es necesario activar el plan de recuperación. RST ASOCIADOS PROJECT SAS cuenta con un procedimiento Documentado para la

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

Gestión de Incidentes:

“Anexo Procedimiento de Gestión de incidencias”



Fuente: Procedimiento de Incidentes de RST ASOCIADOS PROJECT SAS de la Mesa de Ayuda.

7.5.4. Actualización de cambios realizados en la Infraestructura

Con el fin de mantener la infraestructura, comunicaciones, aplicaciones y diferentes componentes del Datacenter Principal y Alterno, dentro del proceso de gestión de incidencias, se tiene contemplado que los cambios que se realice en el Datacenter principal deben ser realizados también en el alterno con el fin de asegurar la infraestructura tecnológica de RST ASOCIADOS PROJECT SAS.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



7.5.5. Distribución y Disponibilidad del Plan

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

- Mantener una copia actualizada de su Plan de Recuperación (DRP) para los Servicios de Cómputoen Datacenter alternativo y la oficina administrativa.
- Asegurar que todos los miembros del equipo y sus suplentes mantengan una copia actual de este Plan.
- Asegurar que todo el personal de los Equipos de recuperación considere la preparación de recuperación como parte de sus deberes normales.
- Asegurar que los respaldos y actividades de rotación externas para registros vitales incluyendo aquellos de PC’s están siendo efectuados.
- 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:

- Cambios en el personal del departamento que forman parte de los Equipos.
- Cambios significativos a los requerimientos de recuperación del Datacenter que reflejen cambios en el marco de Recuperación o en la Configuración de Recuperación Mínima

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024



PLAN DE CONTINUIDAD DE NEGOCIO - DRP

Clasificación: 2

Versión: 1.0

Fecha de Actualización:
17-Jun-2024

Aceptable.

- 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*.
- Participar sobre todo en el programa de pruebas del Plan de Recuperación (DRP) para los Servicios de Cómputo tan frecuente como sea requerido

7.6. 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 Equipos 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.

7.6.1. Mantenimiento del Plan

Para asegurar que el plan puede utilizarse de manera eficaz en una emergencia, debe ser preciso y completo, por esta razón es necesario que 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 Equipo 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 Equipo responsable enviará los cambios requeridos al Plan al líder del Equipo de Recuperación para su revisión. Será la responsabilidad del líder de este Equipo 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 Equipo de Recuperación, el líder del Equipo de Recuperación enviará la propuesta a todos los Equipos afectados para su notificación y/o aprobación, si se justifica tal aprobación. Subsecuentemente, el líder del Equipo distribuirá copias de la sección(es) mejorada a todos los Equipos afectados.

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

7.6.2. Distribución del Plan

El Plan de Recuperación ante desastres está disponible en los recursos compartidos de RST ASOCIADOS PROJECT SAS, para ser consultado en la sección de planes de atención de Incidencias.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	<div>PLAN DE CONTINUIDAD DE NEGOCIO -</div> <div>DRP</div>	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

Las guías e instructivos técnicos que se generen como parte del Plan serán documentados dentro del

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

Sistema Integrado de gestión y serán entregados al personal que hace parte del equipo de recuperación, con el fin de que sea almacenado en un lugar que permita su accesibilidad en cado de una activación del Plan de Recuperación.

7.7. CRONOGRAMA

A continuación, se presenta el cronograma de actividades para realizar las pruebas del Plan de Recuperación de Desastres (DRP) y efectuar su implementación y evaluación.

ACTIVIDADES	RESPONSABLE	PREREQUISITOS	MES
Realizar análisis de Impactos del Negocio a nivel Táctico y Operativo de procesos en nueva definición por la oficina de Planeación	Responsable DRP	Definición de procedimientos que hacen parte del proceso que se encuentran en nueva definición.	Mayo de cada vigencia anual
Secuencia de recuperación de cada aplicativo (sistema)	Líder de infraestructura y Responsable DRP	Inventario de hardware y software. Estrategias de DRP.	Noviembre de cada vigencia anual
Roles y responsabilidades en la recuperación (incluyendo proveedores - SLA's y contratos, proveedores alternos)	Líder de infraestructura, líder de contratos, Responsable DRP	Orden de recuperación, contratos.	Julio de cada vigencia anual
Plan de comunicación equipos DRP	Líder continuidad, líder de infraestructura, líder de seguridad y Responsable DRP	Roles y responsabilidades, Plan DRP y Estrategias DRP	Julio de cada vigencia anual
Pruebas DRP y documentación planes de recuperación	Líder de infraestructura, equipo técnico de recuperación, proveedores, Responsable DRP	En conjunto con la implementación del DRP.	Agosto de cada vigencia anual
Capacitación DRP	Responsable DRP	Roles y responsabilidades, Plan DRP y Estrategias DRP	Julio de cada vigencia anual

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

8. RECURSOS

Si la implementación implica la adquisición de herramientas o servicios tecnológicos bajo la responsabilidad del Departamento de TI, los recursos se tomarán del proyecto de inversión “Fortalecimiento de las tecnologías de la información y la comunicación en RST ASOCIADOS PROJECT SAS a nivel nacional.” Para la vigencia 2024 y 2025 se cuenta con el proyecto “Fortalecimiento de la infraestructura física y tecnológica de la RST ASOCIADOS PROJECT SAS”.

9. SEGUIMIENTO Y MEDICIÓN DEL PLAN

El plan de Recuperación de Desastres se encuentra a cargo del Departamento de TI, y realizará las actualizaciones que corresponda en el momento de identificar cambios en el Plan de Recuperación deDesastres por parte del Líder del Área.

9.1. Indicadores

A continuación, se relacionan los indicadores de gestión del DRP:

Nombre del indicador	Porcentaje de recuperación de infraestructura crítica	Valor del indicador	>=90%
Objetivo del Indicador	Medir el incremento porcentual de la capacidad derecuperación	Responsable de la medición de los resultados	Líder Oficina de Tecnologías de la Información y las Comunicaciones
Responsable del análisis de los resultados	Líder de Oficina de Departamento de TI	Tendencia	Aumentar
Tipo de indicador	Eficiencia	Frecuencia de Medición	Semestralmente

VARIABLES DEL INDICADOR						
Fórmula del indicador	Unidad de medida	Variable	Nombre de la variable	Unidad de medida	Fuente de la información	Periodicidad de recolección de la información
(CCA/CCP)	Porcentaje	CCA (Datacenter Alterno)	Capacidad de recuperación actual del Datacenter Alterno	Cantidad	Medición de capacidad de recuperación de la infraestructura crítica respaldada en Datacenter Alterno	Semestralmente
		CCP (Datacenter Principal)	Capacidad de recuperación del Datacenter Principal	Cantidad	Medición de capacidad de recuperación de la infraestructura de Datacenter Principal de las aplicaciones críticas	Semestralmente

Nombre del indicador	Porcentaje de planes de recuperación documentados	Valor del indicador	>=90%
Objetivo del Indicador	Medir el incremento porcentual de planes de recuperación documentados de la infraestructura Tecnológica de RST ASOCIADOS PROJECT SAS	Responsable de la medición de los resultados	Líder Departamento de TI
Responsable del análisis de los resultados	Líder Departamento de TI	Tendencia	Aumentar
Tipo de indicador	Eficiencia	Frecuencia de Medición	Semestralmente

VARIABLES DEL INDICADOR						
Fórmula del indicador	Unidad de medida	Variab le	Nombre de la variable	Unidad de medida	Fuente de la información	Periodicidad de recolección de la información
PD/TIR	No. Planes documentados	PD	Planes documentados	Número	Repositoriode planes documenta dos	Semestralmente
	Cantidad de Infraestructura respaldada	TIR	Total, de infraestructura respaldada	Número	Inventario de infraestructura respaldada	

ANEXO I: PERSONAL TÉCNICO EQUIPO DRP

No.	Rol/Cargo	Nombre	Correo
1	Líder de equipo de recuperación / Líder Departamento de TI	Hugo Andrés Bustos Restrepo	soporte1@rstasociados.com.co
2	Equipo Datacenter / Líder de Infraestructura de Servicios Tecnológicos y líder DRP	Jean Carlos Iglesias- Hugo Andrez Bustos Restrepo	soporte@rstasociados.com.co soporte1@rstasociados.com.co
3	Equipo de Recuperación Telecomunicaciones	Jean Carlos Iglesias- Hugo Andrez Bustos Restrepo	soporte1@rstasociados.com.co soporte@rstasociados.com.co
4	Equipo de Recuperación Seguridad y Privacidad de la Información	Christian Felipe Carrillo	soporte2@rstasociados.com.co
5	Equipo de Recuperación Desarrollo de Sistemas	Iván Quintero	developer@rstasociados.com.co
6	Equipo de Recuperación Mesade Ayuda	Daniel Acosta	soporte3@rstasociados.com.co
7	Equipo de recuperación de Bases de Datos	Jorge Alonso	analytics@rstasociados.com.co

ANEXO II: MIEMBROS DEL COMITÉ DE CRISIS

No.	Rol/Cargo	Nombre	Correo
1	Líder de equipo de recuperación / Líder Departamento de TI	Hugo Andrés Bustos Restrepo	soporte1@rstasociados.com.co
2	Equipo Datacenter / Líder de Infraestructura de Servicios Tecnológicos y líder DRP	Jean Carlos Iglesias Hugo Andrés Bustos Restrepo	soporte@rstasociados.com.co soporte1@rstasociados.com.co
3	Equipo de Recuperación Telecomunicaciones	Jean Carlos Iglesias Hugo Andrés Bustos Restrepo	soporte1@rstasociados.com.co soporte@rstasociados.com.co
4	Equipo de Recuperación Seguridad y Privacidad de la Información	Christian Felipe Carrillo	soporte2@rstasociados.com.co
5	Equipo de Recuperación Desarrollo de Sistemas	Iván Quintero	developer@rstasociados.com.co
6	Equipo de Recuperación Mesa de Ayuda	Daniel Acosta	soporteti@rstasociados.com.co
7	Gerente	Sergio Riaño	Sergio.riaño@rstasociados.com.co
8	Team Líder Coordinador Campaña	Catterine Guerra Will Marin	team.callcenter3@rstasociados.com.co coordinadorbanagrario@rstasociados.com.co

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

		PLAN DE CONTINUIDAD DE NEGOCIO - DRP		Clasificación: 2
				Versión: 1.0
				Fecha de Actualización: 17-Jun-2024
9	Coordinación Call Center	Lizeth Marín	coordinación.callcenter@rstasociados.com.co	
10	Supervisor	Fredy García	supervisor3.icetex@rstasociados.com.co	

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024

	PLAN DE CONTINUIDAD DE NEGOCIO - DRP	Clasificación: 2
		Versión: 1.0
		Fecha de Actualización: 17-Jun-2024

CONTROL DE CAMBIOS		
Versión	Fecha de la Actualización	DESCRIPCIÓN DE LA MODIFICACIÓN
01	17/Junio/2024	Documentación del Plan de Recuperación de Desastres 2024-2025 por segregación del Plan de Continuidad del Negocio.

Elaborado por: Director de T. I	Revisado por: Auditor interno	Aprobado por: Presidente
Fecha: 15/06/2024	Fecha: 17/06/2024	Fecha: 17/06/2024