

Contrato Interadministrativo Nro. 3021063 de 2021
Suscrito Entre la Empresa de Telecomunicaciones de Bogotá y el
Fondo Financiero Distrital de Salud - Secretaría Distrital de Salud

Fase 3 del Proyecto
Grupo de Entregables E20 – Infraestructura, Soporte, Mantenimiento y Operación

Plan de Recuperación de Desastres

Código:
SISEM-3-E20-1

Bogotá, 22 de noviembre de 2023

FICHA DE IDENTIFICACIÓN DEL DOCUMENTO

Título del Documento	Plan de Recuperación de Desastres	
Resumen	El presente documento describe el plan de recuperación de desastres para el sistema de información SISEM.	
Código	SISEM-3-E20-1	
Autor	ETB	
Estado	V2	22/11/2023
Revisado por		
Aprobado por		

CONTROL DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Fecha del Cambio
V1	Versión inicial	Gustavo Adolfo Beltrán	10/01/2023
V2	Actualización	Juan Pablo Barreto Núñez	22/11/2023

DERECHOS DE AUTOR

Derechos de autor
ETB. Todo el material de este entregable puede ser utilizado libremente por la SDS y las personas a quienes está asigne en el marco del convenio citado.

CRÉDITOS

Créditos
Grupo de Migración de Datos de ETB.

Tabla de Contenido

- 1. INTRODUCCIÓN 6
- 2. OBJETIVO 7
- 3. ALCANCE 8
- 4. AUDIENCIA 9
- 5. DEFINICIONES Y CONCEPTOS 10
- 6. CONFIGURACIÓN INICIAL DE LA PLATAFORMA 11
- 7. IDENTIFICACIÓN DEL RIESGO 12
- 7.1. CALIFICACIÓN DE LA PROBABILIDAD 12
- 7.2. CALIFICACIÓN DEL IMPACTO 13
- 7.2.1. DESCRIPCIÓN DEL IMPACTO 13
- 7.2.2. EVALUACIÓN DEL RIESGO 14
- 8. DESCRIPCIÓN DEL ESCENARIO 14
- 9. DEFINICIÓN TIEMPOS DE RECUPERACIÓN 15
- 10. ESTRATEGIA DE RECUPERACIÓN 16
- 11. ROLES Y RESPONSABILIDADES 18
- 12. RETORNO A LA NORMALIDAD 21
- 12.1. APROVISIONAMIENTO AUTOMÁTICO DE NODOS 21
- 12.2. GENERACIÓN DE ALERTAS 21
- 13. CONCLUSIONES 22

Tabla de Ilustraciones

ILUSTRACIÓN 1 CONFIGURACIÓN INICIAL DE LA PLATAFORMA.....	11
ILUSTRACIÓN 2 CONFIGURACIÓN ZONA	11
ILUSTRACIÓN 3 DISPONIBILIDAD INICIAL DE LA PLATAFORMA.....	12
ILUSTRACIÓN 4 TIEMPOS DE RECUPERACIÓN	15
ILUSTRACIÓN 5 CONFIGURACIÓN PLATAFORMA EN DOS ZONAS.....	16
ILUSTRACIÓN 6 CONFIGURACIÓN NODOS	17
ILUSTRACIÓN 7 NIVEL DE DISPONIBILIDAD CON LA CONFIGURACIÓN REALIZADA	17
ILUSTRACIÓN 8 PLAN COPIA DE SEGURIDAD GKE EN GCP.	18

Tabla de Tablas

TABLA 1.	CALIFICACIÓN PROBABILIDAD	13
TABLA 2.	CATEGORÍAS IMPACTO	13
TABLA 3.	DESCRIPCIÓN DEL IMPACTO	14
TABLA 4.	MAPA DE CALOR RIESGO	14
TABLA 5.	EVALUACIÓN DEL RIESGO	14
TABLA 6.	DESCRIPCIÓN DEL ESCENARIO.....	15
TABLA 7.	TIEMPOS DE RECUPERACIÓN PARA EL ESCENARIO	16
TABLA 8.	ROLES Y ACCIONES EQUIPO RECUPERACIÓN	21

1. Introducción

En el dinámico entorno empresarial actual, la continuidad operativa y la seguridad de la información son fundamentales para garantizar la estabilidad y la confianza. Ante la creciente variedad y sofisticación de las amenazas cibernéticas, así como los posibles desafíos operativos, es imperativo contar con un Plan de Recuperación de Desastres (DRP) eficaz.

Un desastre se puede considerar como cualquier interrupción a las actividades computacionales que puedan tener impacto sobre las operaciones de la organización. Estos incluyen, pero no están limitados a las siguientes categorías:

- Natural – Ej. Fuego, inundación, epidemias / pandemias
- Humano – Ej. error de operador, sabotaje, virus, ataques terroristas
- Técnico – Ej. falla equipo, error software, corte de telecomunicaciones o suministro eléctrico

Este documento presenta una visión detallada de la estrategia para garantizar la resiliencia y la rápida recuperación en situaciones de interrupción significativa. Nuestra dedicación a la protección de los intereses de todas las partes involucradas impulsa la creación de este plan, el cual busca ser una guía esencial para partes involucradas durante situaciones adversas.

2. Objetivo

El objetivo de este documento es establecer una estrategia integral de recuperación de desastres para la plataforma SISEM en la zona designada. Este Plan de Recuperación de Desastres (DRP) tiene como finalidad primordial garantizar la continuidad operativa y minimizar el impacto ante una posible falla total de la plataforma, asegurando la rápida y efectiva restauración de los servicios esenciales.

3. Alcance

Este entregable presenta la estrategia de recuperación ante un desastre en la plataforma de SISEM en la zona que se encuentra desplegado.

El Plan de Recuperación de Desastres de TI pretende:

- Describir la configuración actual de la plataforma.
- Evaluar el riesgo de caída de la plataforma en la zona establecida.
- Describir el escenario de acuerdo con el riesgo contemplado.
- Determinar la estrategia de recuperación.
- Retorno a la normalidad.

4. Audiencia

Este documento está dirigido a los usuarios técnicos del sistema, más específicamente a aquellos que se desempeñan en la Dirección de Tecnologías de la Información y la Comunicación - TIC - , en su calidad de solicitantes de servicios, procesos, datos, información y demás herramientas funcionales y no funcionales que les debe proveer la solución contratada, en el marco del contrato interadministrativo Nro. 3021063 de 2021 suscrito entre la Empresa de Telecomunicaciones de Bogotá (ETB) y el Fondo Financiero Distrital de Salud - Secretaría Distrital de Salud.

El propósito del entregable es validar la completitud y pertinencia de las actividades realizadas por el contratista respecto del diseño de las arquitecturas del SISEM, para sus componentes de software y de infraestructura.

5. Definiciones y Conceptos

Alta Disponibilidad	Se refiere a la arquitectura de un servicio o componente de un servicio diseñada para minimizar o eliminar los efectos de una falla en el componente de configuración. Las soluciones de alta disponibilidad están diseñadas para lograr un ANS de disponibilidad más alto y hacer uso de técnicas que subsanen una falla total, ofreciendo mayor resiliencia y rápida recuperación para reducir el número de incidentes y el impacto de estos
Análisis de Riesgos	Es la cuantificación de las amenazas y la definición de la probabilidad de que se materialicen
Desastre	Un repentino evento catastrófico que causa un inaceptable daño o pérdida. Evento que compromete la habilidad de la organización de proveer funciones críticas, procesos o servicios por un inaceptable periodo de tiempo
DRP	Disaster Recovery Plan (por sus siglas en inglés). Plan de Recuperación de Desastres. Metodología que formula las actividades asociadas con la planeación de la disponibilidad continua y restauración de la infraestructura de TI
Escenario	Conjunto de condiciones preconcebidas ante la posibilidad de la ocurrencia de eventos que se describen para formular los planes de acción ante interrupciones o pérdidas de los servicios de TI, son necesarios en la formulación de las estrategias de continuidad. Los escenarios no son predicciones o presupuestos
Estrategias de Recuperación	Acciones definidas, administradas, aprobadas y probadas en respuesta de interrupciones operacionales
Falla	Perdida de la habilidad para operar de un componente del servicio de acuerdo con una especificación o la entrega incorrecta de un servicio
Recuperación	Actividades y programas diseñados para retornar a condiciones normales y niveles aceptables para la Entidad
Recuperación de Desastres	Unión de recursos y actividades para restablecer la información contenida en los servicios de tecnología (incluidos los componentes tales como la infraestructura, telecomunicaciones, sistemas, aplicaciones y datos) en una plataforma alterna luego de una interrupción de los servicios de TI. Recuperación de desastres incluye el retorno de las operaciones en la plataforma permanente o principal

6. Configuración Inicial de la Plataforma

Inicialmente la plataforma se encuentra configurada de la siguiente forma:

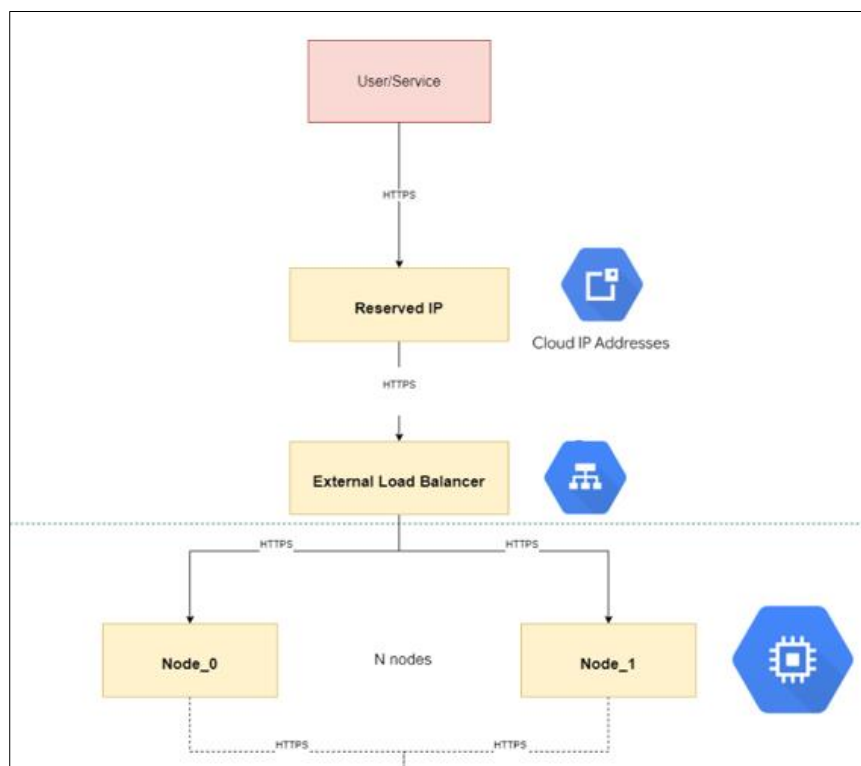


Ilustración 1 Configuración inicial de la plataforma

La plataforma se encuentra configurada bajo un balanceador de carga y distribuida en dos nodos y se encuentra ubicada en la zona US-east-b.

sisem-preprod							
Clústeres de Kubernetes							
DESCRIPCIÓN GENERAL OBSERVABILIDAD OPTIMIZACIÓN DE COSTOS							
Filtro Ingresar el nombre o el valor de la propiedad							
Estado	Nombre	Ubicación	Cantidad de nodos	CPU virtuales totales	Memoria total	Notificaciones	Etiquetas
☒	sisem-pre-prod-cluster-1	us-east1-b	2	16	16 GB		

Ilustración 2 Configuración Zona

Con esta configuración se llega a una disponibilidad de la plataforma del 99.5%.

Google Kubernetes Engine Service Level Agreement (SLA)

During the Term of the agreement under which Google has agreed to provide Google Cloud Platform to Customer (as applicable, the "Agreement"), the Covered Service will provide a Monthly Uptime Percentage to Customer as follows (the "Service Level Objective" or "SLO"):

Covered Service	Monthly Uptime Percentage
Zonal Cluster (control plane)	99.5%
Regional Cluster (control plane)	99.95%
Autopilot Cluster (control plane)	99.95%
Autopilot Pods in Multiple Zones	99.9%

Ilustración 3 Disponibilidad Inicial de la Plataforma

Para acceder a información detallada sobre la arquitectura de la plataforma, consulte el documento denominado "SISEM-3-E16-3 Plataforma de Interoperabilidad". Este documento proporciona una visión exhaustiva de la estructura y diseño de la plataforma para una comprensión completa de su funcionamiento.

Ahora se procederá a identificar el riesgo de tener esta configuración.

7. Identificación del Riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de estos, y el impacto de sus consecuencias, lo que se denomina riesgo inherente, calificándolos y evaluándolos, con el fin de obtener información para establecer el nivel de criticidad del riesgo y las acciones que se van a implementar.

Se han establecido dos (2) aspectos para tener en cuenta en el análisis de los riesgos identificados:

- **Probabilidad:** La cual se entiende como la posibilidad de ocurrencia del riesgo
- **Impacto:** El cual se entiende como las consecuencias que puede ocasionar a la entidad la materialización del riesgo

7.1. Calificación de la Probabilidad

Para calificar la probabilidad de los riesgos se deben tener en cuenta los siguientes criterios:

Concepto	Frecuencia de la Actividad
Casi seguro	La actividad se realiza de forma Diaria
Probable	La actividad se realiza de forma Semanal
Posible	La actividad se realiza de forma Mensual
Improbable	La actividad se realiza de forma Semestral
Rara vez	La actividad se realiza una vez al año

Tabla 1. Calificación Probabilidad

7.2. Calificación del Impacto

El impacto sobre los riesgos se mide según el efecto que puede causar el evento frente al cumplimiento de los objetivos estratégicos y de los procesos. Para calificar el impacto de los riesgos, se deben tener en cuenta los siguientes criterios:

Categorías de Impacto si se materializara el riesgo:

Categoría
Afecta el objetivo estratégico o del proceso.
Afecta la imagen y/o credibilidad.
Afecta recursos económicos.
Genera una intervención y/o sanción
Genera pérdida de la información

Tabla 2. Categorías Impacto

7.2.1. Descripción del Impacto

Impacto	Descripción	Afectación Económica
Catastrófico	- No se lograría el objetivo estratégico o del proceso. - Se afectaría la imagen y credibilidad de la compañía. - Se produciría una sanción - Se generaría un paro total del proceso. - Pérdida de información estratégica.	Afectación mayor a 500 SMLMV.
Mayor	- Impactaría en alto grado el objetivo. - Se generaría intermitencia del servicio.	Afectación entre 100 y 500 SMLMV.

Impacto	Descripción	Afectación Económica
	Pérdida de información del proceso.	
Moderado	- Impactaría moderadamente el logro del objetivo. - Se generaría afectación en la interacción de procesos.	Afectación entre 100 y 500 SMLMV.
Menor	- Impactaría de manera mínima en el logro del objetivo. - Se generaría cambio en los procedimientos.	Afectación entre 10 y 50 SMLMV.
Insignificante	- Sería imperceptible el impacto en el logro del objetivo. - Se generaría ajustes de una actividad.	Afectación menor a 10 SMLMV.

Tabla 3. Descripción del Impacto

A través del análisis de la información anterior se establece la zona de riesgo. El análisis del riesgo se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que pueda causar la materialización de este. La siguiente imagen muestra el cruce de las dos (2) variables y el resultado indica el nivel de riesgo.

Probabilidad/ Impacto	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro	Moderado	Alto	Alto	Extremo	Extremo
Probable	Moderado	Moderado	Alto	Alto	Extremo
Posible	Moderado	Moderado	Moderado	Alto	Alto
Improbable	Bajo	Bajo	Bajo	Moderado	Moderado
Rara	Bajo	Bajo	Bajo	Bajo	Moderado

Tabla 4. Mapa de Calor Riesgo

7.2.2. Evaluación del Riesgo

Se identificó el riesgo de Indisponibilidad de la información por caída de la plataforma en la zona definida y se valoró de la siguiente forma:

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Indisponibilidad de la información por caída de la plataforma	Raro	Catastrófico	Moderado

Tabla 5. Evaluación del Riesgo

8. Descripción del Escenario

De acuerdo con el riesgo identificado, se define el escenario para el DRP de falla total de la plataforma de Google.

Ítem	Escenarios Definidos
1	Falla total de la plataforma de Google: Este escenario cubre la caída total de la plataforma en la zona establecida.

Tabla 6. Descripción del Escenario

Este escenario se replicará o simulara anualmente, ya que la programación anual de ejercicios de replicación del escenario del DRP no solo es una práctica recomendada, sino que también es esencial para mantener la preparación y resiliencia de la organización frente a posibles desastres y situaciones de emergencia.

9. Definición Tiempos de Recuperación

Para la continuidad de la operación se definen los siguientes tiempos:

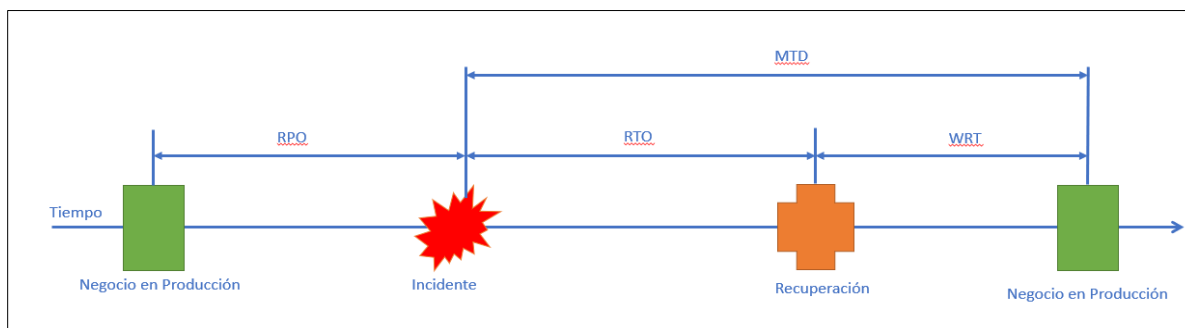


Ilustración 4 Tiempos de Recuperación

- RPO: Determina la cantidad máxima aceptable de pérdida de datos (en minutos u horas) que la empresa está lista / se puede permitir. Es el tiempo entre la última copia de seguridad creada y el momento del desastre.
- RTO: Determina la cantidad máxima de tiempo tolerable necesario para que todos los sistemas críticos vuelvan a estar en línea.
- WRT: Determina la cantidad máxima de tiempo tolerable que se necesita para verificar el sistema y / o la integridad de los datos.
- MTD: Define la cantidad total de tiempo que un proceso de negocio puede interrumpirse sin causar consecuencias inaceptables y es la suma del RTO y WRT.
- El RPO de acuerdo con los requerimientos iniciales de disponibilidad del 99.95%, es de 4 horas.
- De acuerdo con el RPO, se configuran los siguientes tiempos de recuperación:

- El RTO que se define será de 2 horas, para que la plataforma esté en línea nuevamente.
- El WRT que se define es de 1 horas para hacer la verificación del sistema, operación, funcionalidad, integridad de los datos etc.
- El MTD es de 3 horas en el que el proceso puede interrumpirse.

Ítem	Escenario	RPO (Recover y Point Objective)	RTO (Recover y Time Objective)	WRT (Work Recover y Time)	MTD (Maximum Tolerable Downtime)
1	Falla total de la plataforma de Google	4	2	1	3

Tabla 7. Tiempos de Recuperación para el Escenario

10. Estrategia de Recuperación

La estrategia de recuperación ante el riesgo de indisponibilidad de la información debido a la caída de la plataforma por una falla total de Google Cloud Platform (GCP) o en la zona donde está configurado el clúster debe abordarse de manera integral para garantizar la continuidad operativa. Para dar cumplimiento del RPO, se configuró la plataforma en dos zonas generando alta disponibilidad a nivel del recurso.

The screenshot shows the Google Cloud console interface for a Kubernetes Engine cluster named 'cluster-1'. The 'Clústeres' (Clusters) page is active, and the 'DETALLES' (Details) tab is selected. The 'Aspectos básicos del clúster' (Basic cluster aspects) section is visible, showing the following configuration:

- Nombre** (Name): cluster-1
- Tipo de ubicación** (Location type): Regional
- Región** (Region): us-east1
- Zonas predeterminadas de los nodos** (Default node zones): us-east1-b, us-east1-c
- Canal de versiones** (Version channel): Canal regular
- Versión** (Version): 1.24.7-gke.900
- Tamaño total** (Total size): 5
- Extremo externo** (External endpoint): 34.73.209.215
- Extremo interno** (Internal endpoint): 172.20.0.15

The 'Región' and 'Zonas predeterminadas de los nodos' fields are highlighted with a red box, indicating the multi-zone configuration for high availability.

Ilustración 5 Configuración Plataforma en dos Zonas

Los recursos se alojan en varias ubicaciones. Estas ubicaciones se encuentran en us-east1-b y us-east1-c. Corresponde a una región en el este oeste de Estados Unidos. A su vez, se configuran 5 nodos en total:

Migrate to Containers	Nodos												
Copia de seguridad para GKE													
Postura de seguridad													
Configuración y política ^													
Configuración	Filtro Filtra los nodos												
Política	<table><tr><th>Nombre ↑</th><th>Estado</th></tr><tr><td>gke-cluster-1-default-pool-7bb1d7d4-spp4</td><td>✓ Ready</td></tr><tr><td>gke-cluster-1-default-pool-7bb1d7d4-tbgz</td><td>✓ Ready</td></tr><tr><td>gke-cluster-1-default-pool-b5070023-5lgc</td><td>✓ Ready</td></tr><tr><td>gke-cluster-1-default-pool-b5070023-d6xc</td><td>✓ Ready</td></tr><tr><td>gke-cluster-1-pool-1-84fdc43b-vvk4</td><td>✓ Ready</td></tr></table>	Nombre ↑	Estado	gke-cluster-1-default-pool-7bb1d7d4-spp4	✓ Ready	gke-cluster-1-default-pool-7bb1d7d4-tbgz	✓ Ready	gke-cluster-1-default-pool-b5070023-5lgc	✓ Ready	gke-cluster-1-default-pool-b5070023-d6xc	✓ Ready	gke-cluster-1-pool-1-84fdc43b-vvk4	✓ Ready
Nombre ↑	Estado												
gke-cluster-1-default-pool-7bb1d7d4-spp4	✓ Ready												
gke-cluster-1-default-pool-7bb1d7d4-tbgz	✓ Ready												
gke-cluster-1-default-pool-b5070023-5lgc	✓ Ready												
gke-cluster-1-default-pool-b5070023-d6xc	✓ Ready												
gke-cluster-1-pool-1-84fdc43b-vvk4	✓ Ready												

Ilustración 6 Configuración nodos

Con esta configuración se llega un nivel de disponibilidad del 99.99%, permitiendo demostrar que es una arquitectura de alta disponibilidad que permite la conmutación automática a zonas o regiones alternas en caso de falla en la zona primaria.

Covered Service	Monthly Uptime Percentage
Instances in Multiple Zones	>= 99.99%
A Single Instance	>= 99.5%
Load balancing	>= 99.99%

Ilustración 7 Nivel de disponibilidad con la configuración realizada

Además de la alta disponibilidad implementada, el sistema cuenta con copias de seguridad diaria a 7 días, a nivel de clúster completo. En caso de cualquier fallo o incidente, se llevará a cabo la restauración utilizando la copia más reciente del clúster, asegurando así la integridad y continuidad de los datos.

Plan/Nombre de la copia de seguridad	Estado	Clúster	Ubicación	Pods	Tipo de copia de seguridad	Hora de inicio	Duración	Tamaño
cluster-1-backup-diario	Correcto	cluster-1	us-east1	99	Programada	15 de noviembre de 2023, 23:22:00 GMT-5	2 min 3 s	5.54 GiB

Ilustración 8 Plan copia de seguridad GKE en GCP

La creación de un checklist para la replicación o simulación del escenario y la activación del Plan de Recuperación de Desastres (DRP) es una excelente práctica para asegurar una ejecución precisa y completa del proceso. A continuación, se proporcionan las actividades como checklist para dar la atención correcta:

- **Simulación de la Caída de un Nodo:** Iniciar la simulación de la caída de uno de los nodos configurados o que componen el clúster.
- **Activación del Plan de Recuperación:** Activar formalmente el Plan de Recuperación de Desastres como se haría en una situación de emergencia real.
- **Restauración del nodo:** Iniciar el proceso de restauración del nodo demostrando que se ejecuta automáticamente mantenimiento operatividad y alta disponibilidad del clúster.
- **Comunicación Interna y Externa:** Practicar la comunicación interna dentro del equipo de recuperación. Simular la comunicación externa, informando a las partes interesadas sobre la situación y el progreso.
- **Monitoreo Continuo:** Monitorear continuamente la evolución del ejercicio para identificar cualquier problema o actualización del plan.

11. Roles y Responsabilidades

A continuación, se detallan los roles y responsabilidades (tanto antes como después de un desastre) para cada miembro del equipo de recuperación. Es importante anotar que un miembro del equipo puede tener más de un rol descrito.

Mesa de Ayuda

mesadeayuda@skgtecnologia.com

Antes de un Desastre:

- Entiende el papel y la responsabilidad dentro del plan de recuperación de desastres
- Recibe las incidencias que se reporten
- Realiza monitoreo constante

- Participar en el plan de recuperación de desastres como sea requerido

Durante un Desastre:

- Ayuda en la recuperación donde sea necesario
- Monitorea las incidencias y verifica que se respondan

Coordinador De Recuperación – Director de TI

Herman Ricardo Pinzón Pinzón - hpinzon@skgtecnologia.com

Antes de un Desastre:

- Aprueba el Plan de Recuperación de Desastres
- Lidera el equipo de Recuperación
- Designa a los miembros del equipo y los roles que participan en el proceso de recuperación
- Define junto con el negocio el orden de prioridad de la recuperación de las aplicaciones
- Hay que asegurar que el Plan de Recuperación de Desastre se mantenga actualizado
- Autoriza las pruebas periódicas del Plan de Recuperación de Desastre

Durante un Desastre:

- Declara que un desastre ha ocurrido y el Plan de Recuperación de Desastre es activado
- Determina con el responsable del plan de recuperación de desastre, la estrategia de plan para ser implementada
- Determina con el responsable de Plan de Recuperación, los miembros de equipo alternos y otros miembros de apoyo al proceso de recuperación en casos de ser requeridos
- Autoriza el gasto local hasta límites operacionales definidos
- Dirige y supervisa el proceso de recuperación total de TI

Equipo Infraestructura TI

Yoel Lombana Castro - ylombana@skgtecnologia.com

Antes de un Desastre:

- Entiende el papel y la responsabilidad dentro del plan de recuperación de desastres
- Asegura que a todos los sistemas se les realice las copias de seguridad periódicamente y sean aseguradas de acuerdo con los procedimientos existentes
- Hay que asegurar que los servidores tengan apropiados niveles de tolerancia a fallas
- Hay que asegurar que la documentación de los sistemas, bases de datos y servidores se mantenga actualizada
- Participar en el plan de recuperación de desastres como sea requerido

Durante un Desastre:

- Ayuda en la evaluación del grado de daño ocurrido
- Arregla y recibe la entrega de los medios con las copias de seguridad
- Instala o configura la plataforma de ser necesario
- Se comunica con proveedores y/o prestadores de servicios en caso de ser necesario
- Restaura sistemas operativos, aplicaciones y datos
- Prueba y verifica los sistemas operativos, aplicaciones y los datos que están en operación
- Reportar el progreso al equipo del plan de recuperación de desastres

Equipo de Aplicaciones y Desarrollo

Vanessa Carolina Gutiérrez Mendoza - vgutierrez@skgtecnologia.com

Antes de un Desastre:

- Entiende el papel y la responsabilidad dentro del plan de recuperación de desastres
- Hay que asegurar que todas las aplicaciones clave tengan su documentación y las copias de seguridad verificadas, así como las estrategias de recuperación
- Participa en el plan de recuperación de desastres como requerido

Durante un Desastre:

- Ayuda en la instalación y reconfiguración de software de aplicaciones y datos donde sea necesario, de acuerdo con el orden de prioridad acordado
- Ayuda en la recuperación de software de aplicaciones donde sea necesario
- Trabaja con los usuarios líderes en las pruebas y verificación del software de aplicaciones y los datos que han sido restaurados
- Reporta el progreso al equipo del plan de recuperación de desastres

Gerente de Proyecto

Carlos Humberto Caicedo Espitia - ccaicedo@skgtecnologia.com

Antes de un Desastre:

- Entiende el papel y la responsabilidad dentro del plan de recuperación de desastres
- Asegurar las comunicaciones entre la SDS y la ETB
- Participa en el plan de recuperación de desastres como sea requerido

Durante un Desastre:

- Ayuda en la comunicación constante ante la SDS sobre la activación y

recuperación del desastre

- Trabaja y articula con los demás integrantes del DRP

Rol	Acción
Mesa de Ayuda	Recibe las incidencias, las analiza y en caso de ser necesario notifica al coordinador de recuperación para que verifique si es necesario activar el DRP.
Coordinador de Recuperación	Notifica a todos los equipos relevantes (Gerente Proyecto, usuarios, etc.) que un desastre de TI ha ocurrido.
Coordinador de Infraestructura	Notifica al equipo de recuperación, de la ocurrencia de un desastre posterior al análisis.
Coordinador de Recuperación – Equipo de Recuperación	Realizan una evaluación preliminar para determinar el escenario de desastre y procedimiento a realizar consultando la documentación correspondiente.
Coordinador de Recuperación – Equipo de Recuperación	De acuerdo con el escenario de desastre aplicable, coordina con el equipo de recuperación y personal adicional una evaluación del daño.
Coordinador de Proyecto	Comunicación entre SDS y ETB

Tabla 8. Roles y Acciones Equipo Recuperación

12. Retorno a la Normalidad

Esta configuración que se propone se realiza en el momento del despliegue y queda de manera automática, de forma tal que es transparente para el usuario cuando la plataforma haga el cambio de zona, de igual manera al hacer el retorno a la zona original.

12.1. Aprovisionamiento Automático de Nodos

El aprovisionamiento de nodos se realiza de forma automática y administra los nodos del clúster mediante la creación y eliminación de grupos de nodos según se requiera en función de las necesidades de carga de trabajo.

12.2. Generación de Alertas

La plataforma está configurada con la generación de logs automáticos de cada uno de los eventos asociados a los servicios y éstos son monitoreados por la mesa de servicios. En estos logs se registran entre otros, las alertas de uso de los recursos de la infraestructura y procesos.

13. Conclusiones

El DRP que se propone es una configuración automática en la cual no hay necesidad de la interacción humana para su activación.

Con la configuración del DRP propuesto se logra una disponibilidad de la plataforma del 99.99%.

El coordinador de recuperación junto con el gerente de proyecto establecerá el mejor canal, que garantice una comunicación abierta y frecuente, que deberá ser mantenida durante todo el periodo de recuperación, en esta comunicación deberán estar incluidos los miembros del equipo de recuperación, cliente, usuarios claves y proveedores de ser necesario.