PLAN DE CONTINUIDAD DE NEGOCIO DE TECNOLOGIAS DE LA INFORMACIÓN

TC-PL-04

Tecnologías de la Información y las Comunicaciones

30/05/2024

Versión 1

ALCALDÍA MAYOR DE BOGOTÁ D.C.
INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO
BOGOTÁ

Control de Cambios		
Versión	**Fecha**	**Descripción de la Modificación**
1	30/05/2024	Versión inicial del documento

Elaboró	Revisó	Aprobó
Francisco Daza Cardona Contratista Carmenza González Vargas Profesional Universitario	Claudia Marcela Ladino Jefe Oficina TIC	Claudia Marcela Ladino Jefe Oficina TIC Nelson Jairo Rincón Martínez Jefe Oficina Asesora de Planeación

Tabla de contenido

- **Introducción**

La Oficina de Tecnologías y las Comunicaciones en atención a lo dispuesto por el decreto 1078 de 2015 en su artículo 2.2.17.6.6. Seguridad de la información, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, donde se define que los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el Modelo de Seguridad y Privacidad de la Información (MSPI), emitido por el MinTIC o un sistema de gestión de seguridad de la información certificable, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.
La implementación del MSPI requiere definir y aplicar procedimientos para proteger la información de la entidad ante eventos de desastre, que afecten la disponibilidad de los servicios críticos del Instituto Distrital de Gestión de Riesgos y Cambio Climático - IDIGER , definiendo acciones que permitan reducir su impacto negativo, estas acciones permitirán una correcta gestión de la continuidad del negocio orientada a los servicios de tecnologías de la información y comunicación (TIC), por esto, el IDIGER ha decidido acatar los lineamientos que para este sentido contempla la Guía para la preparación de las TIC para la continuidad del negocio (IRBC por sus siglas en inglés ICT Readiness for Business Continuity), emitida por MinTIC.

- **Objetivo**

Establecer las actividades que permitan fortalecer la capacidad de respuesta del IDIGER ante situaciones de desastres, mediante la creación y mejora continua del Plan de recuperación de desastres (DRP por sus siglas en ingles Disaster Recovery Plan).

- **Alcance**

Desde la etapa de planificación y preparación ante la ocurrencia de caída de los servicios hasta la definición de las actividades que permitan disminuir los tiempos para restablecer los servicios críticos de IDIGER.

- **Preparación de las TIC para la continuidad del negocio (IRBC)**

El ciclo de funcionamiento del modelo de operación de continuidad del negocio y su funcionamiento, dentro del modelo de operación de seguridad y privacidad de la información, desarrolla cuatro (4) fases que comprenden el modelo de operación del MSPI definiendo objetivos, metas y herramientas que permiten que

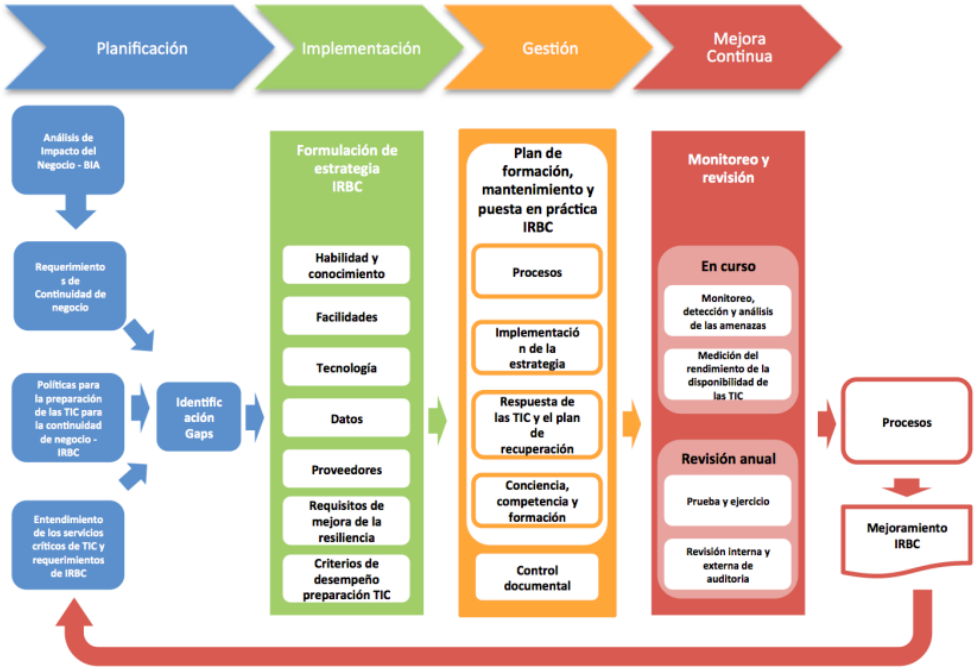
la continuidad del negocio sea un modelo sostenible dentro de IDIGER. En la siguiente ilustración, se aprecian las fases del modelo de operación del MSPI, se debe tener en cuenta que la fase de diagnóstico no se tiene en cuenta en el IRBC.

Ilustración 1. Modelo de operación seguridad y privacidad de la información.

Fuente: Guía para la preparación de las TIC para la continuidad del negocio. MinTIC

En la siguiente ilustración se muestran las actividades claves que se deben desarrollar, en cada una de las fases del modelo de operación del IRBC.

Ilustración 2 Actividades Claves del modelo de operación de continuidad



Fuente: Guía para la preparación de las TIC para la continuidad del negocio. MinTIC

En los siguientes ítems se desarrollan las actividades de cada una de las fases propuestas para la implementación del IRBC.

IDIGER define la estrategia metodológica para establecer las políticas, objetivos, procesos y procedimientos pertinentes del (IRBC), como punto clave se deben establecer los requerimientos de continuidad del negocio, los cuales, deben estar aprobados por la alta dirección.

- **Objetivos específicos del IRBC**

- Asegurar la continuidad de las aplicaciones críticas que son apoyadas por los servicios tecnológicos prestados por el proceso de Gestión Tecnológica e Innovación de IDIGER dentro de los márgenes de tiempo tolerables.
- Minimizar el tiempo de toma de decisiones durante un incidente que amenace la continuidad de las operaciones críticas del negocio.
- Mantener los servicios brindados a los ciudadanos y por ende la confianza en la entidad.
- Cumplir con los requerimientos legales y contractuales que tiene IDIGER con el Distrito, entes reguladores y demás partes interesadas.
- Minimizar la pérdida de información crítica del negocio.
- Diseñar la estrategia del Plan de recuperación de desastres (DRP por sus siglas en ingles Disaster Recovery Plan) acorde a las necesidades de IDIGER, que le permita continuar su operación con el menor impacto posible.
- Desarrollar los procedimientos para la respuesta y recuperación ante incidentes o desastres (planes de contingencia), describiendo las acciones y sus responsables.

- **Manejo de interrupciones**

Se ha definido el manejo de interrupciones por su relación con la severidad y el impacto que las mismas pueden tener sobre los servicios de TI:

Tabla 1 Manejo de interrupciones

Tipo de evento	Características	Ejemplos	Respuesta
Desastre	Evento que inhabilita el Centro de Cómputo Principal (CCP) para prestar sus servicios. No permite seguir laborando en las instalaciones principales.	Terremotos, incendio general, fallo eléctrico en el sector.	DRP
Interrupción	Evento que requiere ser evaluado para ser tratado como desastre o como contingencia. Puede llegar a ser	Incendio localizado, atentado terrorista, huelga	DRP Planes de contingencia

Tipo de evento	Características	Ejemplos	Respuesta
	considerado como un desastre o una contingencia, dependiendo del impacto que se determine en el manejo de incidentes.	interno o externo.	
Contingencia	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática. No impide el acceso al CCP. En ausencia de plan de contingencia, requiere evaluación que puede llevarla a categoría de desastre.	Fallo de sistemas o servicio, ausencia de personal clave.	Planes de contingencia

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER).

Las interrupciones catalogadas como desastre son las menos probables, pero de llegar a ocurrir representan riesgos de afectación a la vida humana, a las instalaciones, a proveedores y a la infraestructura de la entidad o de la ciudad, esta afectación, supone un grado de dificultad mayor para el cumplimiento de los tiempos de recuperación planteados.

- **Fases de una interrupción**

  Dentro del manejo de una interrupción se definen 5 fases que se detallan a continuación.

  - **Prevención**: Tareas de preparación y actividades que garanticen que, ante la necesidad de su activación, el servicio se preste en las condiciones esperadas.
  - **Respuesta**: Actividades encaminadas al manejo del incidente en cuanto a evaluación de daños y proyección de la restauración con el objeto de generar los soportes necesarios para la toma de decisión de activar el DRP. También hacen parte de esta fase la activación del DRP y su procedimiento de notificación.
  - **Recuperación**: Activar sitio alterno y plataformas para prestar servicios.
  - **Reanudación**: Reiniciar la prestación de los servicios de los diferentes aplicativos desde un sitio alterno.
  - **Restauración**: Reparar los daños en el sitio principal en busca de retornar a la normalidad.

- **Lineamientos la preparación de la continuidad de negocio de TI**

- Se debe asegurar que las actividades descritas, sean asignados al personal idóneo para su atención.
- Se debe velar por que se socialice a todos los colaboradores involucrados, tanto titulares como contingencia, los roles y funciones que deben desempeñar en caso de un incidente.
- Se debe mantener contacto permanente con los proveedores de servicios críticos y conocer sus estrategias de continuidad de negocio.
- Se deben aprobar y asegurar los cambios significativos para los servicios de TI.
- Se debe aprobar toda interrupción programada de servicio.
- Se debe asegurar que toda acción preventiva o correctiva propuesta cumpla con las políticas de seguridad de la información.
- Se debe definir el procedimiento para el manejo de incidentes graves que permita: confirmar la naturaleza y grado del incidente, tomar control de la situación, contener el incidente y comunicar a las partes interesadas.

- **Roles y responsabilidades**

En la siguiente tabla se detallan las características de los roles definidos.

Tabla 2 Roles y responsabilidades IRBC

Rol	Responsabilidades
Comité Institucional de Gestión y Desempeño	Aprobar el PCN de TI y realizar el seguimiento a las acciones propuestas. Proponer acciones de mejora al PCN de TI.
Oficina de Tecnologías de la Información y las Comunicaciones	Definir las políticas que debe cumplir el PCN para garantizar que este alineado a la implementación del MSPI. Garantizar que las acciones de mejora son implementadas, verificar la correcta actualización y mantenimiento del IRBC. Velar porque los documentos y procedimientos asociados al IRBC sean actualizados, publicados y socializados por cada una de las áreas responsables. Gestionar el análisis BIA y los riesgos para garantizar que el IRBC responde a las necesidades de IDIGER. Verificar que los DRP definidos en la entidad se mantengan actualizados y sean probados periódicamente. Gestionar diagnósticos y auditorias para presentarlos al CIGD y, garantizar que sean implementadas las acciones de mejora en el Plan de Continuidad de Negocio de TI.

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

- **Plan de requerimientos**

Los requerimientos de continuidad deben estar en función del tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO), en la siguiente tabla se definen los tiempos que son parte de los requerimientos de continuidad.

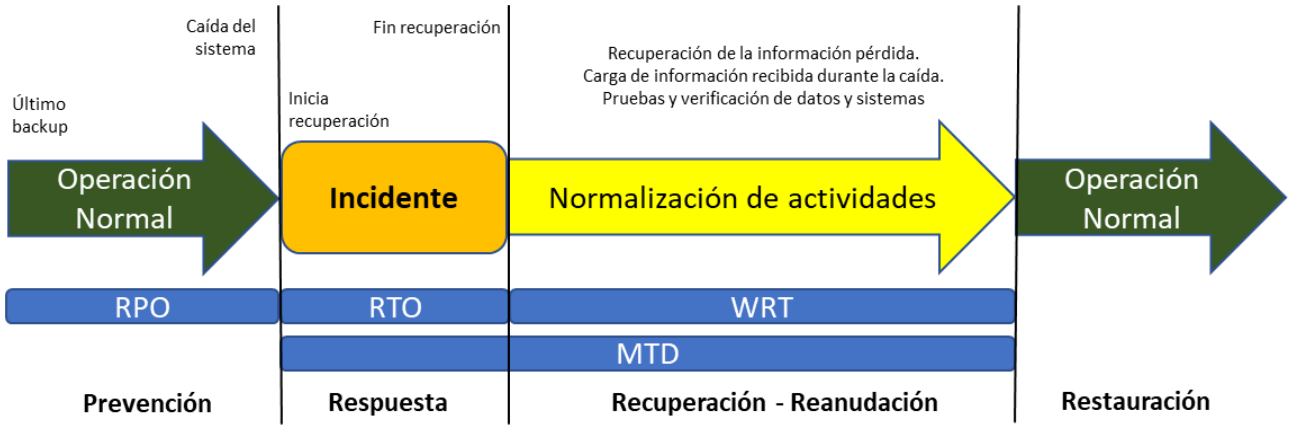
Tabla 3 Tiempo de Recuperación que se deben establecer

TIEMPO	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo de Recuperación de Trabajo. Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados.
MTD	Tiempo máximo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Fuente: ISO 22301:2019

IDIGER debe tener en cuenta el momento de establecer sus objetivos mínimos de continuidad del negocio (MBCO), para lograr su cumplimiento, tal como se aprecia en la siguiente ilustración.

Ilustración 3 Tiempos de recuperación



Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

Con base el análisis de Impacto (**BIA**), que debemos realizar en el **segundo trimestre de 2024**, se obtuvo por de la Oficina de Tecnologías de la Información y las Comunicaciones algunos objetivos mínimos de continuidad del negocio (MBCO) para los servicios más críticos de IDIGER.

Para cumplir estos MBCO se debe contar con un plan de requerimientos categorizando las actividades para la continuidad definiendo el nivel con el cual, cada actividad critica, podrá reanudar su operación. Estas actividades deberán contar con un tiempo objetivo de recuperación (RTO), y un punto objetivo de recuperación (RPO), por cada objetivo mínimo de continuidad del negocio (MBCO) definido por producto, servicio o procedimiento.

Después de tener los tiempos RTO y RPO para cada producto, servicio o procedimiento de TI crítico se deben comparar con la duración de las actividades actuales de preparación, tales como prevención, monitoreo, detección, respuesta y recuperación, y las brechas encontradas deben ser informadas e incluir estas actividades en el plan.

- **Análisis de Impacto de Negocio**

El análisis del impacto sobre el negocio (BIA) es uno de los aspectos más importantes a considerar en el desarrollo de un plan de recuperación ante desastres o DRP, que permite identificar los diversos eventos que pueden afectar la continuidad de sistemas críticos de la información, este proceso será necesario realizarlo cada año o cuando ocurran cambios que impacten fuertemente a IDIGER.

- **Evaluación de riesgos**

La gestión de riesgo es el punto central de la definición de una estrategia de continuidad perfectamente alineada con la visión del MSPI, dentro de su entorno de operación. Esta metodología es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo a la operación y continuidad de los procesos. Se usará la metodología de valoración de riesgos de seguridad de la información, contemplada en la guía para la administración del riesgo y oportunidades del DAFP y el que se haya definido en IDIGER.

- **Desarrollo de estrategias de recuperación de desastres (DRP)**

Las estrategias de recuperación estarán basadas obviamente en los resultados obtenidos luego de la realización del BIA, en donde también se consideran los valores de los tiempos máximos permitidos de no disponibilidad (MTD). Realizando también un análisis de la toda la información obtenida de las entrevistas, entendimiento de los procesos de negocio, BIA, MTD se procede a organizar esta información en una tabla ordenada de prioridades de recuperación de los diferentes sistemas considerados como críticos.

Se deben considerar elementos como:

- Sistemas telefónicos
- Redes Locales
- Redes WAN
- Internet
- Personas
- Infraestructura física
- Aplicaciones
- Hardware
- Bases de datos
- Sistemas operativos
- Firewalls
- IDS-IPS
- Switches
- Routers

Una de las principales estrategias a definir son las características del sitio alterno que se usará para un sistema o servicio. A continuación, se enumeran los tipos de sitios alternos que se pueden definir.

1. Sitio frio (Cold sites): En esta opción sólo se tiene aire acondicionado, potencia, enlaces de telecomunicaciones, y otros.
2. Sitio semipreparado (Hot site): Normalmente está configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad.
3. Sitio preparado (Warm sites): En esta opción no se incluyen servidores específicos de alta capacidad.
4. Sitios móviles: Tener proveedores en varias partes para usar su infraestructura y operar en ella el servicio.
5. Sitio espejo (Mirror site): Se procesa cada transacción en paralelo con el sitio principal.
6. Sitio reciproco: Acuerdos recíprocos con otras organizaciones para utilizar sus recursos y poder atender en ellos la crisis.

Se debe tener en cuenta los criterios de la siguiente tabla para evaluar el tipo de sitio alterno a implementar:

Tabla 4 Criterios para seleccionar estrategias DRP

Estrategia	Costo	Hardware	Telecomunicaciones	Tiempo	Localización
Sitio en frio	Bajo	No	Ninguno	Largo	Fijo
Sitio semipreparado	Medio	Parcial	Parcial	Medio	Fijo
Sitio preparado	Alto	Completo	Parcial	Corto	Fijo
Sitio móvil	Alto	Variable	Variable	Variable	No Fijo
Sitio Espejo (mirror)	Muy Alto	Completo	Completo	Mínimo	Fijo
Sitio reciproco	Bajo	Parcial	Parcial	Medio	Fijo

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

- **Pruebas del Plan de Recuperación de Desastres (DRP)**

La efectividad de los planes de recuperación de desastre se puede valorar si existe un plan de prueba que se lleve a cabo en condiciones reales, garantizando que durante estas pruebas se consideran las actividades más importantes que requieran comprobación y certeza en su funcionamiento futuro.
Se debe probar dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera. Es también importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una crisis.

En la tabla que aparece a continuación se muestran los tipos de prueba que se pueden ejecutar.

Tabla 5 Tipos de Pruebas

Tipo de prueba	Uso / planificación/tiempo
Prueba de orientación	Presenta a los participantes los planes y tareas a realizar. Introducir un nuevo DRP o revisar otros. No requiere experiencia previa Ayuda a orientar al nuevo personal al liderazgo No afecta los servicios de producción. Ciclo de planificación: un mes Tiempo de prueba: 60-90 minutos.
Simulacro	Prueba de respuesta a un evento de crisis. Implica la respuesta de campo real, practica o prueba en condiciones realistas. Involucrar a todos los niveles de personal de respuesta. Ciclo de planificación: un mes Tiempo de prueba: 10-60 minutos. Ejemplos: Simulacro de incendio, Prueba de radio, Prueba de tornado y Prueba de terremoto, entre otros.
Prueba de escritorio	La versión básica busca resolver problemas en un entorno grupal a través de una lluvia de ideas. Los tableros de escritorio avanzados presentarán mensajes y asistentes de prueba que puedan responder preguntas Una experiencia más "basada en la realidad" No afecta los servicios de producción. Ciclo de planificación: 2-3 meses Tiempo de prueba: 90-120 minutos. Tiempo de debate: 30 minutos.
Prueba funcional	Evalúa la asignación de recursos. Evalúa la comunicación a través de diferentes grupos

Tipo de prueba	Uso / planificación/tiempo
	Evalúa la adecuación de los procedimientos y políticas que están activos. Se busca que los participantes realicen actividades reales. Involucra a simuladores, evaluadores, implica tener un equipo de diseño más grande. Introduce mensajes más avanzados transmitidos por varios medios Tiempo de prueba: 90 min - 4 horas Ciclo de planificación: 3-6 meses
Prueba a escala completa	Evalúa la capacidad operativa de sistemas de forma interactiva sobre un período de tiempo sustancial Presenta eventos complejos y detallados en tiempo real Moviliza personal y recursos y movimiento de equipos de respuesta a emergencias. Equipos y recursos. Puede ser costoso; puede ser perjudicial para operaciones normales Tiempo de prueba: 2-8 horas. Ciclo de planificación: mínimo 4 meses

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

- **Notificación de la prueba a los equipos de trabajo**

Notificar a los equipos participantes la realización de la prueba y verificar que todos ellos estén enterados.

Tabla 6 Notificación de la prueba

Descripción	Responsables
Identificar y notificar al personal participante en la prueba, cada colaborador (a) debe conocer y comprender los objetivos y las responsabilidades que debe desempeñar durante la prueba.	Equipo coordinador
Suministrar los números de teléfono, mapa y dirección del sitio de operación alterno si aplica.	Equipo coordinador
Verificar y confirmar la disponibilidad de los registros críticos.	Líderes tecnológicos
Verificar y confirmar que la red de comunicación está habilitada y disponible para la prueba.	Equipo coordinador
Coordinar reuniones con los diferentes equipos que participaran en la prueba para coordinar el trabajo y definir las responsabilidades de cada uno de estos.	Equipo coordinador

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

- **Ejecutar la prueba**

Incluye contar con todos los elementos necesarios para iniciar el proceso de prueba en el(los) centro(s) alterno(s).

Tabla 7 Ejecutar la prueba

Descripción	Responsables
Actividades antes de la prueba - Verificar y aseguraras el correcto estado de los componentes tecnológicos que van a soportar el servicio (verificar las alertas y monitoreo que se realiza sobre estos).	Líderes tecnológicos
Actividades durante la prueba - Identificar las tareas o transacciones que se deben ejecutar en los sistemas a probar, además de hacer un análisis de riesgos (probabilidad de que algún evento ocurra vs el impacto que puede originar a la prueba), detallando las medidas que se usaran para mitigarlo y el responsable de aplicarlas. Activar los grupos del equipo DRP que acompañará la prueba. Registrar el tiempo de inicio y terminación del ejercicio y sus actividades. Identificar tareas de rollback (para volver a producción), en caso de que alguna de las tareas de la prueba falle. Documentar los problemas y desempeño general. Definir las actividades de comunicación que se van a enviar a los interesados, tenido en cuenta el medio, el mensaje y el vocero entre otros.	Líderes tecnológicos Grupo de comunicaciones
Actividades después de la prueba. Comunicar a los proveedores críticos la finalización de la prueba. Borrar todos los datos en la localidad alterna de recuperación que no sea parte de la solución permanente de contingencia. Enviar archivos vitales a la bóveda de archivos vitales, si aplica.	Líderes tecnológicos

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

- **Evaluación de la prueba**

Una vez se haya realizado la prueba y como actividad final, es necesario efectuar una evaluación o revisión de su desarrollo en la cual estén analizados los objetivos, los parámetros, los criterios establecidos, las fallas y fortalezas. Se deben hacer reuniones con el personal que participó en la prueba para identificar problemas y bondades del plan de recuperación.

- **Entrenamiento y mantenimiento**

Para lograr el éxito del DRP es fundamental contar con la participación y el compromiso de los usuarios de IDIGER involucrados en el mismo, quienes deben recibir la capacitación sobre cómo proceder en caso de alguna situación

contingente que pueda afectar de manera parcial o total las operaciones, la infraestructura donde se llevan a cabo sus operaciones y/o la manera de proceder en caso de un desastre natural o cualquier otro tipo de amenaza.

Las capacitaciones se deben realizar de acuerdo con la demanda o cada vez que se generen cambios en el DRP y al ingreso de nuevos colaboradores para de esta manera asegurar que conozcan la forma de proceder y sus responsabilidades dentro del este.

Se debe realizar un monitoreo de la efectividad de las actividades de concientización y entrenamiento de DRP a través de evaluaciones y registros de estas en concordancia con los procedimientos de IDIGER.

- **Estrategias de Recuperación de Desastres DRP**

Las recuperaciones de los servicios de TI críticos se basan en la definición de una estrategia que incluye una infraestructura física y tecnológica que permita activación de las aplicaciones críticas y procesamiento de datos desde servidores alternos, IDIGER ha definido estrategias de continuidad ante desastres para cada uno de sus servicios más críticos. En la siguiente tabla se muestran los servicios críticos y la estrategia definida para cada uno de ellos.

Tabla 8 Estrategias DRP

Servicio	Estrategia
1	Sitio preparado CCP: Data center nube privada CCA: Data center en sitio COA: no aplica, se puede operar de manera remota
2	Sitio semipreparado CCP: Data center en sitio CCA: Data center nube privada COA: no aplica, se puede operar de manera remota
3	Sitio preparado CCP: Nube Oracle CCA: Nube Oracle – otra localización COA: no aplica, se puede operar de manera remota

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

- **Gestión para la recuperación de desastres**

Para que el Plan de Recuperación de Desastres tenga éxito es crucial el compromiso de todos los colaboradores de IDIGER para el desarrollo y mantenimiento de un Plan de Recuperación de Desastres que garantice la sobrevivencia de la organización en el evento de un desastre, en este sentido

deberán asignar el personal que mantenga, direccione y actúe para coordinar la continuidad de las operaciones frente a eventos que impacten los servicios.

A continuación, se definen los equipos de trabajo y sus responsabilidades durante una situación de desastre. En cada equipo se debe establecer un plan de sucesión para que en caso de no estar disponible el funcionario principal, pueda su reemplazo actuar con la misma autoridad y responsabilidad.

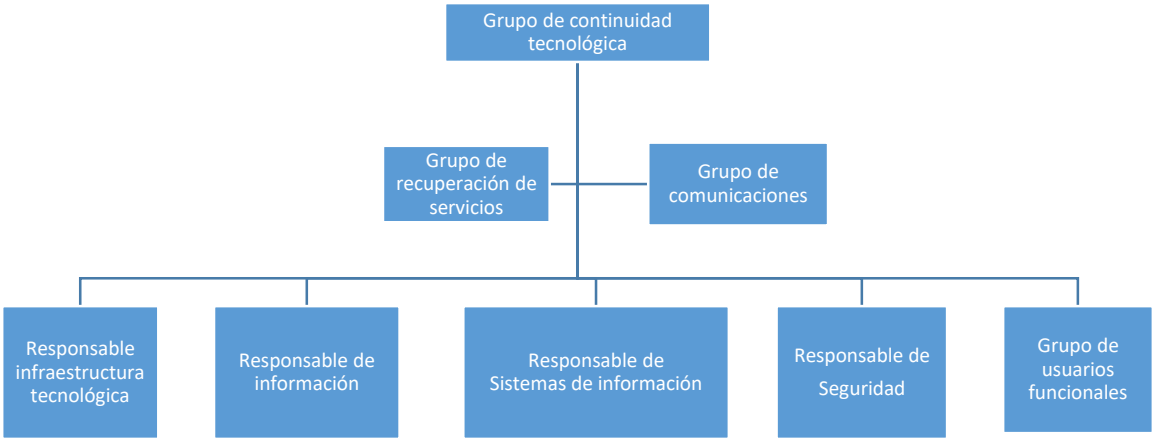
Este plan está compuesto por los planes individuales de cada equipo, los cuales consideran las actividades que deben ser ejecutadas en cada una de las fases definidas para el manejo de desastres, según el siguiente esquema de responsabilidades.

- **Roles y responsabilidades del DRP**

Para que el Plan de Recuperación de Desastres tenga éxito es crucial el compromiso de todas las personas de la Entidad, mientras no exista el gobierno específico de Continuidad de Negocios definido al interior de IDIGER, la OGTI será el encargado del desarrollo y mantenimiento de un Plan de Recuperación de Desastres que garantice la sobrevivencia de los servicios de tecnología de la Entidad en el evento de un desastre, en este sentido, deberán asignar el personal que mantenga, direccione y actúe para coordinar la continuidad de las operaciones frente a eventos que impacten los servicios.
A continuación, se definen los equipos de trabajo y sus responsabilidades durante una situación de desastre. En cada equipo se debe establecer un plan de sucesión para que en caso de no estar disponible el colaborador principal designado, pueda su reemplazo actuar con la misma autoridad y responsabilidad.

Este plan está compuesto por los planes individuales de cada equipo, los cuales consideran las actividades que deben ser ejecutadas en cada una de las fases definidas para el manejo de desastres, según el siguiente esquema de responsabilidades.

Figura 1: Ilustración 4 Equipo DRP



Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)

Las responsabilidades de cada equipo se detallan en los siguientes ítems.

- **Grupo de continuidad tecnológica (Equipo ejecutivo)**

Dado el alcance que por definición tiene un DRP, el equipo ejecutivo debe estar conformado por el jefe de la oficina de tecnología de la información de IDIGER, es muy importante que no se pierda de vista el carácter técnico del DRP y por tanto el nivel de

especialización del equipo, lo anterior se debe tener en cuenta, si a futuro, se desea tener como invitados a este equipo algunos funcionarios del nivel ejecutivo de la empresa.
Por la naturaleza de las decisiones que se deban tomar, el equipo debe asegurar la comunicación permanente con las altas directivas de la empresa en cada momento (antes, durante y después).

Algunas de las responsabilidades de este equipo son:

- Establecer las directrices y políticas de los DRPs de IDIGER, enmarcadas en un Plan de Continuidad de Negocio.
- Mantener contacto con la alta dirección, proveedores y entidades interesadas, sobre la situación de la empresa.
- Toma de decisiones estratégicas durante la crisis o incidente.
- Declarar la activación del DRP.
- Comunicación efectiva con los medios de comunicación, en caso de no existir un equipo a nivel corporativo.

- Supervisión de la efectividad de las actividades de recuperación, asegurar el retorno de la información a la plataforma principal.

- **Grupo de recuperación de servicios**

Liderado por el responsable del DRP (líder del dominio de servicios tecnológico), estará conformado además por su equipo de trabajo líderes Infraestructura de almacenamiento y procesamiento, redes y comunicaciones, gestión de servicios y de seguridad lógica y física quienes tendrán asignados roles para el manejo de incidentes en las fases de: recuperación, reanudación y restauración.

Algunas de las responsabilidades de este grupo son:

- Organizar la elaboración y actualización de los DRPs de IDIGER.
- Programar, coordinar y evaluar las pruebas y ejercicios del DRP (al menos una vez al año para cada DRP).
- Apoyar al Equipo Ejecutivo para decidir sobre la activación del Plan de Recuperación de Desastres.
- Coordinar las actividades del DRP cuando se active, siguiendo su plan específico.
- Mantener informado al equipo ejecutivo sobre las acciones y la situación ante un evento de crisis.
- Dar seguimiento a la situación durante y después de la activación del DRP.
- El Equipo Coordinador del DRP debe tener el apoyo de los otros equipos de trabajo definidos.

Conformado por profesionales de los dominios de Seguridad, Información, Sistemas de información y Servicios tecnológicos.

- **Grupo de comunicaciones**

Se debe alinear a las políticas y formatos utilizados por IDIGER para definir los canales y tipos de comunicados que se deben utilizar en el momento de una crisis.

Algunas de las responsabilidades de este grupo son:

- Tener conocimiento de la forma que se deben usar las plataformas habilitadas por IDIGER para usar ante una situación de crisis.
- Capacitar y entrenar a los colaboradores que puedan tomar el rol de voceros de la entidad en una situación de crisis.
- Crear y poner a disposición de los voceros y del grupo de continuidad tecnológica, un set de comunicados que se pueda usar ante situaciones de crisis.
- Durante la crisis, determinar cuáles deben son los interesados que deben recibir comunicaciones, elegir el vocero, mantener comunicación constante con el grupo de continuidad tecnológica.
- Informar el inicio y finalización de la crisis.

- **Infraestructura tecnológica**

Es el responsable de planear y ejecutar las actividades que permitan la activación de las plataformas específicas sobre los cuales funcionan los servicios críticos. Igualmente, es responsable de todas las actividades que garanticen la adecuada disponibilidad del servicio de respaldo en cuanto la actualización de los sistemas, aplicativos, datos y documentación, así como, las que conduzcan al restablecimiento de los servicios desde el Centro de Cómputo Principal del (los) servicio(s) afectado(s).

Es el responsable de gestionar y monitorear todos los recursos de red que hacen posible la conectividad, la gestión, las operaciones comerciales y la comunicación de la red o Internet, comprende hardware y software, sistemas y dispositivos que permiten la comunicación entre usuarios, servicios, aplicaciones y procesos desde servidores hasta enrutadores inalámbricos.

Algunas de las responsabilidades de este grupo son:

- Mantener actualizados los procedimientos de instalación y arranque de los servidores y los planes recuperación.
- Conocer y divulgar a los miembros de los equipos, los procedimientos de notificación de desastre.
- Mantener iguales las configuraciones de los equipos del CCP y del CCA, en HW y SW.
- Apoyar las labores que garanticen la disponibilidad del esquema de respaldo de datos.
- Definir y ejecutar pruebas del DRP en lo referente a esta plataforma.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el CCA.
- Asistir la recuperación de la plataforma en el CCP.
- Documentar fallas y su solución.
- Proveer Soporte técnico según requerimientos del momento.
- Restaurar el servicio en el CCP.
- Alistar el CCA para usarlo nuevamente después de un retorno a la normalidad.
- Mantener y monitorear la infraestructura garantizando su confidencialidad.
- Garantizar el personal calificado para la gestión de la red.
- Mantener una visibilidad total en toda su infraestructura de red para la supervisión del rendimiento como para la detección de amenazas.
- Mejorar constantemente la eficiencia y las herramientas de seguridad
- Realizan filtrado de tráfico inteligente para que solo se envíe el tráfico adecuado a las herramientas adecuadas.

- **Información**

Es el responsable de definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la misma.

Algunas de las responsabilidades de este grupo son:

- Liderar la recuperación de los componentes de información.
- Aplicar las actividades correctivas para garantizar la calidad de los componentes de información.
- Verificar la correcta restauración de la información que aseguran el servicio, conforme a lo relacionado en el directorio de los componentes de información.
- Asegurar los mecanismos que permiten el acceso a los servicios de información por parte de los diferentes grupos de interés, garantizando las características de accesibilidad, seguridad y usabilidad.
- He de asegurar que se cumplan los acuerdos de nivel de servicio con las dependencias o instituciones con las que se realice intercambio de información con las características de oportunidad, disponibilidad y seguridad.
- Verificar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información.

- **Sistemas de información**

Responsable de planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en IDIGER.

Algunas de las responsabilidades de este grupo son:

- Asegurar la extracción de datos para la generación y publicación de datos abiertos.
- Suministrar la documentación técnica y funcional debidamente actualizada.
- Garantizar que se ejecuten los mecanismos para preservar los registros históricos de las acciones que realizan los usuarios sobre los sistemas de información, manteniendo la trazabilidad y apoyando los procesos de auditoría.
- Garantizar que los sistemas referenciados en el catálogo de actualizado de los sistemas de información tengan la información relevante para su correcto funcionamiento.

- **Seguridad**

Encargado de mantener la seguridad perimetral de IDIGER, además, se encarga de custodiar la información de respaldo de los sistemas críticos.

Algunas de las responsabilidades de este grupo son:

- Monitorear el estado de los certificados digitales que soportan los servicios publicados por IDIGER.
- Verificar el estado de los equipos que controlan las comunicaciones entrantes o salientes de la entidad tanto a nivel centra como territorial.
- Verificar la disponibilidad de equipos de respaldo que pueden ser usados para atender una crisis.
- Monitorear y verificar el correcto funcionamiento de los dispositivos utilizados para la generación y restauración de copias de seguridad de los procesos críticos.

- **Grupo de Usuarios funcionales**

Grupo de colaboradores responsables funcionales de los servicios prestados por el área de informática, donde ejecutan funciones propias de su proceso y otras complementarias al trabajo diario. También puede hacer parte de este equipo de colaboradores del dominio de sistemas de información para garantizar que el sistema que se utilice en eventos de crisis cumpla todas las funcionalidades entregadas.

Algunas de las responsabilidades de este grupo son:

- Información y notificación de eventos identificados a nivel de sus procesos que puedan afectar las operaciones.
- Participar en las actividades de continuidad (Capacitaciones, divulgación, pruebas y auditorias)
- Actualizar la información de continuidad de las operaciones internas de su proceso y divulgarlos al interior de este.
- Participar en los ajustes a las actividades de entrevista de valoración de impacto de negocio y evaluación de riesgos a nivel de proceso.
- Apoyar al interior de su proceso los aspectos de continuidad, indicando acciones de mejora, cambios al interior del proceso y otros factores que deban ser revisados a nivel de comité para su aprobación.

- **Hoja de Ruta (Actividades del Plan de Continuidad de Negocio de TI)**

En la siguiente tabla se plantean las actividades que son necesarias para continuar con la implementación y mejora continua del IRBC.

Tabla 9 Hoja de ruta

Actividad	Detalle	Trim 2024
Realizar el BIA en los Procesos	Establecer el impacto de negocio para los procesos contra los servicios críticos que presta la Oficina de Tecnologías y las Comunicaciones.	2do TRIM

Actividad	Detalle	Trim 2024
Realizar Análisis de Riesgo.	Definir, ejecutar y hacer seguimiento al plan de acción producto del análisis de riesgo de continuidad de negocio realizado.	3er TRIM
Entregar los Roles y responsabilidades del DRP	Determinar los responsables y sus suplentes para la gestión del DRP. Se debe garantizar que las personas que administren el procedimiento estén plenamente capacitadas.	3er TRIM
Generar Plan de Pruebas	Crear, ejecutar y hacer seguimiento al plan de pruebas de los diferentes DRP definidos en IDIGER. Acompañar las pruebas del ejercicio de continuidad de negocio para el sistema de registro con la prueba del DRP.	3er TRIM
Medición de resultados de las pruebas	Despues de las pruebas determinar si los resultados se ajustan a los objetivos propuestos y las necesidades de los procesos en materia de RTO y RPO.	3er TRIM
Programar sesiones de Entrenamiento y mantenimiento de documentos.	Se deben programar sesiones de trabajo con los responsables de mantener y ejecutar los DRP durante el presente año. Es necesario registrar y mantener actualizados todos los documentos que hacen parte del DRP conforme a lo estipulado.	4to TRIM

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones (IDIGER)