

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 22/11/2021
		Página: 1 de 58

CONTENIDO

INDICE DE TABLAS	3
INDICE DE FIGURAS	4
4 INTRODUCCIÓN	5
1. TERMINOS Y DEFINICIONES	6
2. OBJETIVO	11
3. ALCANCE	12
4. GENERALIDADES DEL PLAN DE RECUPERACION DE DESASTRES - DRP	15
4.1. ESTRATEGIA GENERAL DE RECUPERACIÓN	16
4.2. ESTRATEGIA DE ACCIÓN	17
4.2.1. SERVICIOS CRÍTICOS	17
4.3. CLASIFICACIÓN DE LOS ESCENARIOS DE DESASTRE	18
4.3.1. PÉRDIDA TOTAL O PARCIAL DE LAS INSTALACIONES DEL CENTRO DE DATOS PRINCIPAL	20
4.3.2. PÉRDIDA TOTAL O PARCIAL DE LOS SERVICIOS PACTADOS DENTRO DEL ALCANCE DEL DRP.	20
4.3.3. INTERRUPCIONES AL NEGOCIO O INCIDENTES QUE PODRÍAN AFECTAR EL CUMPLIMIENTO DE LAS LABORES DE LOS FUNCIONARIOS.	23
4.3.4. PROCEDIMIENTO DE FAILOVER Y FAILBACK	24
4.3.4.1 FASE I: ACTIVIDADES PREVIAS	24

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 2 de 58

4.3.4.2 FASE II: FAILOVER – ACTIVIDADES A EJECUTAR DURANTE LA VENTANA 26

4.3.4.3 FASE III: PRUEBAS FUNCIONALES EN CDA 29

4.3.4.4 FASE IV: FAILBACK – ACTIVIDADES A EJECUTAR REGRESO A CDP 29

5.1. CENTRO DE DATOS ALTERNO - CDA 31

5.2. CANALES DE COMUNICACIONES..... 33

5.2.1. CONECTIVIDAD 34

5.3. CENTRO DE OPERACIONES ALTERNO - COA 34

5.3.1. CENTRO DE MONITOREO 35

6. PROCEDIMIENTO DE NOTIFICACIÓN, ACTIVACIÓN Y RETORNO 36

6.1. PROCEDIMIENTO DE NOTIFICACIÓN 39

6.2. DETECCIÓN DEL EVENTO 41

6.3. ROLES Y RESPONSABILIDADES - DEFINICIÓN DE RECURSOS 41


6.3.1. COMITÉ DE EMERGENCIAS 43

6.3.2. COMITÉ DE RESPONSABLES DE ACTIVACIÓN DEL DRP 44

6.3.3. EQUIPO DE RECUPERACIÓN DEL DRP 46

6.3.3.1. RESPONSABLES OFICINA DE INFORMÁTICA DEL IDEAM PARA LA ACTIVACIÓN DE LOS SERVICIOS DEL DRP. 55

6.3.4. ÁRBOL DE LLAMADAS 56

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:3 de 58

INDICE DE TABLAS

Tabla 1 - Alcance DRP – IDEAM	13
Tabla 2 - Clasificación de eventos	37
Tabla 3 – Equipo evaluador de daños	43
Tabla 4 – Comité responsable de activación del Plan de recuperación de desastres DRP.....	45
Tabla 5 – Coordinador DRP – Líder DRP IDEAM	46
Tabla 6 – Equipo recuperación contingencia	47
Tabla 7 – Medios de comunicación	57

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:4 de 58

INDICE DE FIGURAS

Figura 1 - RTO - RPO	15
Figura 2 - Alternativas de recuperación	16
Figura 3 - Escenarios de falla	19
Figura 4 – Distancia lineal del centro de datos alterno	32
Figura 5 - Diagrama general de conectividad	34
Figura 6 - Centro de monitoreo ROC – CDA	36
Figura 7 - Fases de activación	38
Figura 8 - Procedimiento de notificación	39
Figura 9 - Proceso de activación gestión del plan	40
Figura 10 – Definición de recursos	42
Figura 11 – Activación DRP IDEAM	45
Figura 12 – Responsables activación de servicios del DRP.	55
Figura 13. Árbol de llamadas	56

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:6 de 68

INTRODUCCIÓN

La implementación de estrategias en contribución a la preservación de la información pública ante situaciones disruptivas, permite a la entidad tratar de manera integral los riesgos identificados y amenazas potenciales que puedan comprometer la continuidad de la operación de los servicios críticos esenciales, mediante la combinación de controles preventivos y reactivos como parte de las estrategias para la recuperación de desastres.

Es por esta razón que previamente se deben identificar en la entidad los procesos críticos de operación, por medio de la integración de los requisitos de la Gestión de la Seguridad de la Información y la Gestión de la Continuidad del Negocio teniendo en cuenta los diferentes aspectos y requisitos que pueden relacionarse (Legales, Institucionales, Operacionales y Recursos).

El Análisis de Impacto de Negocio(BIA), permite estimar una posible afectación que la organización obtendría como resultado de alguna incidencia o un desastre, el cual puede orientar a la entidad en cómo podría afectarse en sus objetivos y los procesos de operación, igualmente es de gran importancia en las fases iniciales para el desarrollo de un Plan de Recuperación de Desastres – DRP, el cual es revisado, aprobado e implementado acorde a las necesidades de operación de la entidad, por consiguiente se debe desarrollar e implementar estrategias de continuidad que permitan asegurar la restauración oportuna de las operaciones críticas esenciales.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 7 de 68

La correcta implementación de la gestión de la continuidad del negocio permitirá reducir de manera significativa daños potenciales y sus efectos, en caso de ocurrencia de eventualidades disruptivas, la entidad estará en capacidad para responder de forma oportuna evitando consecuencias negativas (afectación de imagen, pérdidas financieras, sanciones legales e interrupción en la operación de servicios).

1. TERMINOS Y DEFINICIONES

Esta sección es elaborada para lograr dar entendimiento de forma clara y precisa en lo concerniente a la terminología, definiciones y abreviaturas que den lugar en la gestión de continuidad de negocio y en el presente documento.

Actividades prioritarias: Actividades a las que se les debe dar prioridad después de un incidente con el fin de mitigar los impactos.

Nota: Los términos que comúnmente se utilizan para describir las actividades dentro de este grupo son: crítico, esencial, vital, urgente y principal.

Dentro del desarrollo de este documento se utiliza el término *actividades críticas*.
[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.25].

Amenaza: Factor potencial que tiene la capacidad de generar daño ya sea sobre los recursos involucrados en el desarrollo de un proceso (humano, financiero, medio ambiente, información e imagen corporativa) [International Glossary of Resilience].

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 8 de 68

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Nota 1: El análisis de riesgo proporciona las bases para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo.

Nota 2: El análisis del riesgo incluye la estimación del riesgo.

[Norma ISO 31000:2011, Capítulo 2, Términos y definiciones, numeral 2.21].

Árbol de llamadas: Documento que describe gráficamente las responsabilidades y el orden en que deben producirse los enlaces de comunicación a los diferentes niveles de la organización, así como a los clientes y proveedores y otros contactos clave en caso que se produzca una emergencia, catástrofe o situación de indisponibilidad grave.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Centro de Operaciones de Emergencia (COE) (sala de crisis): La ubicación física y / o virtual desde donde se toman las decisiones estratégicas y se dirigen, coordinan y monitorean todas las actividades de un evento / incidente / crisis.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Centro Alterno de Procesamiento de Datos (CAPD) o CDA: Lugar en donde se procesa la información de una entidad cuando no es posible hacerlo en el CPD, independientemente de ser de su propiedad o de un tercero.

Centro de Procesamiento de Datos (CPD): Lugar en donde se concentran los recursos necesarios para el procesamiento de la información de una entidad, independientemente de ser de su propiedad o de un tercero.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:9 de 68

Continuidad del Negocio: Capacidad de la organización para continuar con la entrega de sus productos o servicios a niveles aceptables predefinidos luego de un incidente disruptivo.

[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.3]

Crisis: Situación anormal e inestable que amenaza los objetivos estratégicos, la reputación o la viabilidad de una organización.

[BS 11200:2014 – Crisis Management – Guidance and good practice, Capítulo 2, Términos y definiciones]

Desastre: Un evento repentino, no planeado y/o deseado puede ser catastrófico que causa daño o pérdida en niveles no aceptables a una organización.

- Un evento que pone en peligro la capacidad de una organización para proporcionar funciones críticas, procesos o servicios por un cierto período de tiempo inaceptable.
- Un evento en el que la gestión de una organización invoca sus planes de recuperación.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Directorio activo: Base de datos distribuida que permite almacenar información relativa a los recursos de una red (objetos, dominios, árboles y bosques) con el fin de facilitar su localización y administración, el cual ofrece la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa.

Ejercicio: Proceso para entrenarse, prepararse, practicar y mejorar el desempeño de una organización.

[Norma ISO 22301:2012, Capítulo 3, Términos y definiciones, numeral 3.18]

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:10 de 68

Emergencia: Un evento o incidente imprevisto que sucede repentinamente y demanda acción e intervención inmediata para minimizar pérdidas potenciales de vidas, destrucción de propiedades o la pérdida o interrupción de las operaciones de negocio hasta el punto que pueda representar una amenaza.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Estrategia de continuidad del negocio: Curso de acción definido previamente (y aprobado por el Comité Directivo - Dirección) con el fin de proteger la viabilidad de la empresa y reanudar sus actividades críticas en los plazos establecidos. Las estrategias seleccionadas deben cubrir los RTOs identificados en el BIA.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Evento: Hecho o suceso imprevisto. Es la ocurrencia o cambio de un conjunto particular de circunstancias.

Nota 1: Un evento puede ser una o más ocurrencias, y puede tener varias causas.

Nota 2: Un evento puede consistir en algo que no está sucediendo.

Nota 3: Un evento puede ser algunas veces referido o conocido como incidente o accidente.

Nota 4: Un evento sin consecuencias puede ser referido como “evento fallido”,

“incidente”, “evento cercano”, “evento de aviso”

[Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.14].

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. *Norma ISO 22301:2019, Capítulo 3, Términos y definiciones, numeral 3.16].*

Infraestructura: Sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización. *[Norma ISO 22301:2012, Capítulo 3, Términos y definiciones, numeral 3.20].*

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:11 de 68

Impacto: Efecto, aceptable o no, el resultado de un evento que tiene lugar en una organización. Los tipos de impactos al negocio.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Incidente: Suceso que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe, también suele definirse como la materialización de un riesgo.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 12 de 68

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Mitigación: Implementación de medidas para disminuir o eliminar la ocurrencia o impacto de un evento. *[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]*

MTPD (Maximun Tolerable Period of Disruption): Tiempo para que los impactos adversos, los cuales pueden surgir del resultado de no proveer un producto o servicio o realizar una actividad, sea inaceptable.

[Norma ISO 22301:2012, Capítulo 3, Términos y definiciones; numeral 3.26]

Plan de Recuperación ante Desastres (Disaster Recovery Plan – DRP): Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades establecidas, para la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Plan de Continuidad del Negocio (PCN ó BCP): Conjunto de procedimientos documentados que guían a las entidades para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido aceptable, en caso de interrupciones.

[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia - Capítulo XXIX - CE 026 del 2016 - “Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos”, capítulo 2, numeral 2.6]

Procesos críticos: Son aquellos procesos que debido a su importancia deben estar disponibles y operativos constantemente o lo antes posible, después de un incidente, emergencia o desastre.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:13 de 68

[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia - Capítulo XXIX - CE 026 del 2016 - “Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos”, capítulo 2, numeral 2.7.1]

Proveedor: Persona, natural o jurídica responsable de suministrar bienes y servicios.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Respuesta a incidentes: Conjunto de acciones realizadas por una organización ante un desastre u otro evento importante que pueda afectar significativamente a la organización, a su personal o su capacidad de operación normal. Puede incluir: evacuación, activación de un DRP, evaluación de daños o cualquier otra medida necesaria para llevar a la organización a un estatus más estable.

[Disaster Recovery Institute International - DRI International – International Glossary for Resiliency]

Recovery Time Objective (RTO): Tiempo después de un incidente en el que la operación o el servicio deben ser reanudados.

[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia - Capítulo XXIX - CE 026 del 2016 - “Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos”, capítulo 2, numeral 2.9]

Recovery Point Objective (RPO): Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.

[Circular Básica Contable Financiera de la Superintendencia Financiera de Colombia - Capítulo XXIX - CE 026 del 2016 - “Reglas relativas para el procesamiento de información en centros de procesamiento de datos, centros alternos de procesamiento de datos y centros de servicios compartidos”, capítulo 2, numeral 2.8]

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 14 de 68

2. OBJETIVO

Describir las acciones necesarias a ejecutar como parte de las estrategias para la activación del plan de recuperación de desastres DRP, en el centro de datos alterno del Instituto de Hidrología, Meteorología y Estudios Ambientales IDEAM, para respaldar y asegurar la disponibilidad y la operación de los servicios críticos de la entidad, ante la ocurrencia de incidencias que puedan generar interrupción.

3. ALCANCE

La necesidad de desarrollar un plan de contingencia está relacionada con el impacto que implicaría la interrupción parcial o total de los sistemas de información críticos de la entidad, es por esta razón que el propósito del proyecto busca mantener la operación de los servicios críticos esenciales y misionales que la entidad provee al estado colombiano.

En el presente documento se incluye el desarrollo de los ejercicios que hacen parte del DRP institucional, describiendo los procedimientos y actividades necesarias (paso a paso) para la activación y recuperación de los servicios contemplados en el presente alcance.

- ☐ Contempla los procesos a seguir durante las pruebas y en caso de un evento adverso que requiera la activación del plan de contingencia.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:15 de 68

Los Servidores que hacen parte integral del DRP se relacionan a continuación:

N°	Servidor	Función y/o servicio	Sistema Operativo	No. Cores	Memoria (GB)	Almacenamiento (GB)	RTO (Horas)	RPO (Horas)	PRUEBAS (anual)
1	BART	Servidor FTP	Red Hat 5.11	8	8	1024	2	2	1
2	BAGUE	SMARTMET	Red Hat Ent 6.9	24	64	1024	0,5	2	1
3	CAGUI	servidor de aplicaciones	Red Hat 6.5	16	32	1024	0,5	2	1
4	jboss6dc-prd	servidor de aplicaciones	Red Hat 7.6	2	8	90	0,5	2	1
5	Jboss7dc -prd	servidor de aplicaciones	Red Hat 7.6	2	8	90	0,5	2	1
6	AQDB-PRD	Servidor BD Oracle Std	Red Hat Ent 7.4 MAIPO	12	32	500	0,5	2	2
7	FURACHOGUA	Directorio Activo, DNS y DHCP	Windows Server 2012 R2 Estándar	16	16	500	0,5	1	1
8	FORFEO	Gestión Documental	Red Hat 5	4	6	600	3	1	1
9	BORFEO	PostgreSQL	Red Hat 5	6	8	320	2	1	1
10	GUAYQUES	Balanceador	Red Hat 7.6	2	4	80	0,5	2	1
11	POLARIS	POLARIS	WS 2008 R2	16	32	1638	0,5	2	1
12	AQDAS - PRD	Aquarius data adquisition	WS2012 R2	4	16	300	1	2	2
13	AQMP-PRD	Modulo Personalizado DHIME	WS2012 R2	8	24	300	1	2	2
14	AQTS- PRD1	Time Series I	WS2012 R2	24	24	600	1	2	2
15	AQWP-PRD	Aquarius Web Portal	WS2012 R2	8	16	600	1	2	2
16	DHIME-PRD	Portal DHIME	WS2012 R2	4	16	100	1	2	2
17	GIS1-WSLS	Server BD postgresQL	RedHat 7.6	4	12	150	1	2	2

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 16 de 68

18	GIS2-WSLS	Server app	RedHat 7.6	4	12	150	1	2	2
19	GIS3-GEOS1	Server app	RedHat 7.6	4	32	100	1	2	2
20	GIS6-GEOEV	server app	RedHat 7.6	4	12	80	1	2	2
21	BD1 (*)	BD Oracle Standard	RedHat 7.6	8	32	2400	0,5	1	1
22	BD2 (*)	BD Oracle Standard	RedHat 7.6	8	32	2300	0,5	1	1
	Total			188	446	13970			

(*) Actualmente BD1 y BD2 están agrupadas en una sola máquina con BD Oracle Enterprise, pero está prevista su separación en los próximos meses.

Tabla 1 - Alcance DRP – IDEAM

- Servicios de conectividad para replicación del Data Center:

Comunicaciones WAN	Link MPLS de 128 Mbps - Renata	< 30 Min
--------------------	--------------------------------	----------

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 17 de 68

Servidor CDP	Servidor CDA	0 MIN	0 MIN - 1 HORA	1 - 2 HORAS
BART	DRP_BART_2			
BAGUE	DRP_BAGUE			
CAGUI	CAGUI-DRP			
JBOSS6DC-PRD	JBOSS6DC-DRP			
JBOSS7DC-PRD	JBOSS7DC-DRP			
AQDB-PRD	AQDB-PRD			
FURACHOGUA	DRP_FURACHIOGUA			
FORFEO	VRA_02			
BORFEO	VRA-01			
GUAYQUES	GUAYQUES-DRP			
POLARIS	POLARIS-DRP			
AQDAS-PRD	AQDAS-PRD_REPLICA			
AQMP-PRD	AQWP-REPLICA			
AQTS-PRD1	AQTS-PPRD_REPLICA			
AQWP-PRD	AQWP-REPLICA			
DHIME-PRD	DHIME-PRD			
GIS1GDB	GIS1-REPLICA			
GIS2WGIS	GIS2-REPLICA			
GIS3GEOS1	GIS3-REPLICA			
GIS6GEOEV	GIS6-REPLICA			
SUA	SUA_REPLICA			

Figura 3. Tiempo Requerido para Recuperación de Sistemas

El cumplimiento del RPO y RTO se verificará en el marco de la ejecución de las pruebas que formalmente son realizadas y/o en ocasiones en que se requiera activar los servicios en el Centro de Datos Alterno.

4. GENERALIDADES DEL PLAN DE RECUPERACION DE DESASTRES - DRP

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 18 de 68

De acuerdo con lo establecido en el alcance el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM definió unos tiempos de RTO y RPO para cada uno de los servidores listados, luego de realizar un análisis de criticidad de las mismas, determinando lo siguiente:

RPO (RECOVERY POINT OBJECTIVE): Se define como el periodo máximo tolerable en el cual la información de un servicio de IT no estaría disponible con motivo de la ocurrencia de un desastre, puede ser especificado en segundos, minutos, horas o días

RTO (RECOVERY TIME OBJECTIVE): Corresponde al tiempo que se toma y el nivel de servicio mediante el cual un proceso de negocio puede ser restablecido después de la ocurrencia de un desastre o una interrupción del servicio, esto en orden de evadir las consecuencias asociadas a la interrupción de un proceso de negocio que debe estar disponible permanentemente.

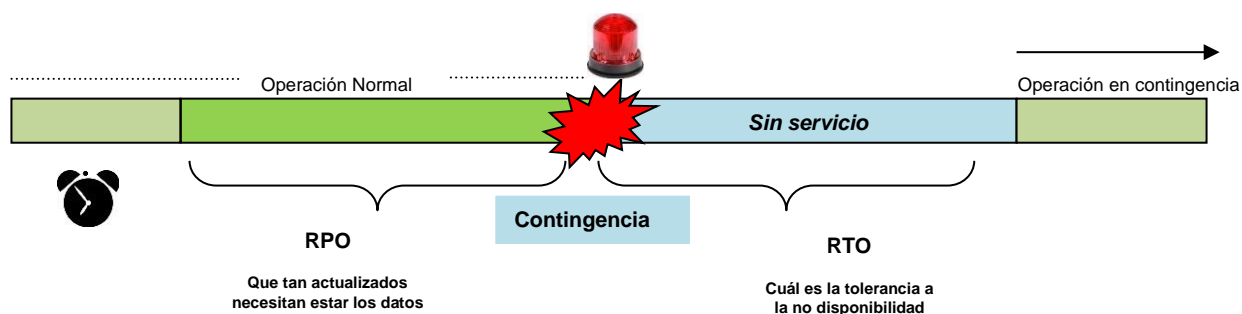


Figura 1 - RTO - RPO

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 19 de 68

4.1. Estrategia general de recuperación

Este plan está basado en el hecho de que por algún factor crítico (interno o externo), se genere indisponibilidad a los servicios de cómputo centrales o las instalaciones donde se ubica el centro de cómputo principal, sea de manera parcial o total (período inaceptable de tiempo).

Las estrategias a realizar serán acordes a la magnitud y duración tentativa del incidente y se deberán tener en cuenta los siguientes aspectos:

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

Este plan solo podrá ser activado únicamente cuando el IDEAM lo apruebe y se considere necesario.

Con base en los resultados obtenidos por el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM en donde se determinó disponer de un Centro de Datos Alternativo, se planteó y estableció la estrategia de recuperación la cual se conforma de elementos tales como:

- La ubicación del Centro de Datos Alternativo y la preparación.
- Puesta en funcionamiento de un Centro de Operaciones Alternativo (COA) y de un Centro de Monitoreo.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:20 de 68

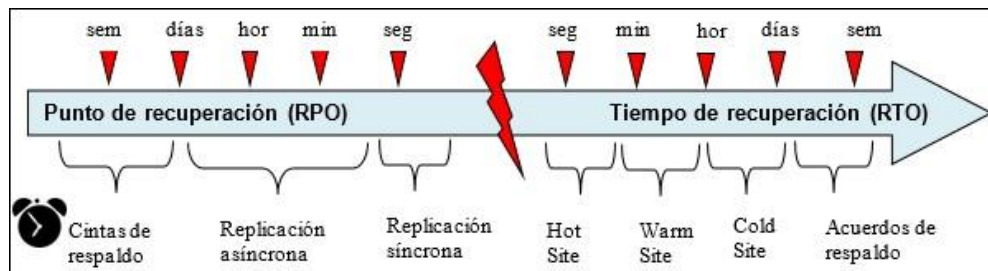


Figura 2 - Alternativas de recuperación

4.2. Estrategia de acción

Las estrategias y planes de acción considerados para la recuperación y restablecimiento de la operación de los servicios críticos del IDEAM, han sido orientados a cubrir cualquier contingencia mayor o catastrófica que inhabilite el acceso del personal al edificio donde se ubica el centro de cómputo o bien a los servicios de cómputo y telecomunicaciones en que se apoyan todas aplicaciones críticas de la entidad, las cuales se definieron como:

4.2.1. Servicios Críticos

1. Servicio de FTP
2. Servicios WEB (SMARMET, SIRH, PRONOSTICOS, PCB, LIFERAY, PORTAL INSTITUCIONAL, GLACIARES ANDINOS y GEOVISOR entre otros)
3. Sistema de recepción de datos de estaciones automáticas - Polaris
4. Servicio de gestión documental
5. Bases de datos Oracle y PostgreSQL
6. Directorio Activo, DNS y DHCP
7. Servicios DHIME

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 21 de 68

La decisión para desarrollar este plan, se basó en las características de la operación actual de la entidad, así como el nivel de dependencia de las tecnologías de la información y las comunicaciones.

Incidencia Menor:

En caso de presentarse una incidencia menor, esta podrá ser subsanada o corregida rápidamente por medio de los mecanismos de detección, diagnóstico y reparación de fallas, activando los procedimientos de atención de problemas dispuestos y utilizados día a día por el personal del IDEAM.

Incidencia Mayor:

De presentarse una incidencia mayor en los equipos y sistemas del Centro de Datos Principal que impida el funcionamiento parcial o total de la entidad, esta deberá ser identificada y corregida a la brevedad. Si el tiempo estimado de reparación que determinen los equipos de recuperación responsables de las aplicaciones o recursos técnicos críticos, es superior al tiempo identificado para que este operativo, el IDEAM tomará la decisión de activar o no el DRP.

Incidencia Catastrófica:

Si se presenta un incidente que provoque una contingencia catastrófica evidente y que por consiguiente interrumpa las operaciones del IDEAM de forma general en sus instalaciones principales ubicadas en el Calle 25D # 96B - 70 de la ciudad de Bogotá, le corresponde al IDEAM la declaración de la contingencia, esta declaración de contingencia es responsabilidad de la entidad.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:22 de 68

4.3. Clasificación de los escenarios de desastre

En esta sección se incluye una clasificación de los posibles escenarios de falla que pueden ocurrir.

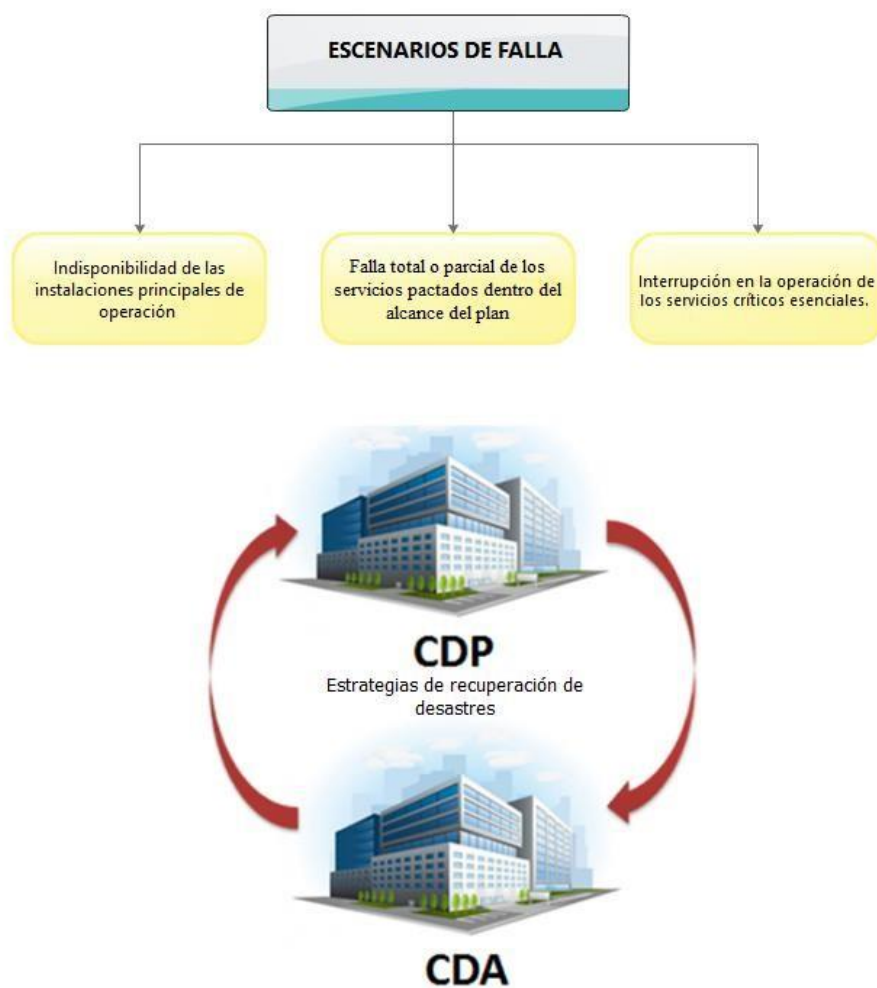


Figura 3 - Escenarios de falla

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:23 de 68

4.3.1. Pérdida total o parcial de las instalaciones del centro de datos principal

La pérdida total o parcial de las instalaciones del Centro de Datos Principal del Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM, puede deberse a diferentes situaciones y/o motivos tales como:

- Guerras internacionales o civiles.
- Actos perpetuados por terroristas y/o grupos armados ilegales.
- Hostilidades u operaciones bélicas ya sea o no declarada una guerra.
- Rebelión, sedición, usurpación o retención ilegal del mando.
- Asonada, motín, o conmoción popular.
- Huelgas, conflictos colectivos de trabajo o suspensión de hecho de labores y por movimientos subversivos y/o acciones terroristas y/o de grupos armados ilegales que conlleven a daños materiales en las instalaciones.
- Deslizamientos de tierra y/o otros elementos, avalanchas, fallas geológicas, terremoto, temblor, asentamientos, inconsistencias del suelo, inundaciones, erupción volcánica, vientos o cualquier otra convulsión de la naturaleza.
- Reacción o radiaciones nucleares o contaminación radioactiva.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:24 de 68

4.3.2. Pérdida total o parcial de los servicios pactados dentro del alcance del DRP.

La pérdida total o parcial de los servicios pactados dentro del alcance del DRP puede originarse por las siguientes causas y/o motivos:

- Daños causados directamente por personas encargadas de la infraestructura de IT, en el curso de la ejecución de las operaciones llevadas a cabo con el propósito de dar cumplimiento a sus obligaciones.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 25 de 68

- Por la pérdida de aquellos bienes cuyo valor excede el de los materiales que los componen tales como planos, modelos, metodologías, documentos de cualquier clase, archivos magnéticos y/o cualquier otro medio de archivo computacional, que traiga como consecuencia que no se pueda efectuar la operación normal de los servicios del negocio.
- Por la reticencia u omisión de los procedimientos establecidos para la prestación de los servicios del negocio.
- Por delitos por computador y/o medios electrónicos que puedan afectar la prestación de los servicios del negocio.
- Por utilización de técnicas como el acceso a los activos de información por medio de una identidad falsa, la alteración de datos en forma no autorizada, la negación de la ocurrencia de un acción o transacción, la visualización de información no autorizada, la negación del servicio y/o operación de la(s) aplicación(es) y la obtención del acceso a la plataforma y/o a los aplicativos con todos los privilegios y/o roles que conlleven a la pérdida total o parcial de los servicios del negocio.
- Por las vulnerabilidades en sistemas operativos y/o en las aplicaciones que estén alojadas en el centro de datos.
- Por la disminución en el rendimiento laboral de las personas a cargo de los procesos de negocio.
- Por exposición de accesos lógicos tales como puertas traseras, ataques asíncronos, fuga de datos, interceptación de líneas (wire-trapping), wardriving, dispositivos adosados (piggybacking), cierre de computadoras (shutdown), ataques de negación de servicio, redondeo hacia abajo,

□

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:26 de 68

técnicas de salami, caballos de troya, virus, gusanos y bombas lógicas que generen la pérdida total o parcial de los servicios de negocio. Por exposición de acceso físico tales como entradas no autorizadas, daño, vandalismo o robo de equipos o documentos, copia o visualización de información privada, alteración de equipos e información sensible, revelación al público de información privada, abuso de los recursos de procesamiento de datos que conlleven a la pérdida total o parcial de los servicios de negocio.

- Por problemas y exposiciones ambientales tales como falla eléctrica, voltaje severamente reducido, depresiones, picos y sobre voltajes, interferencia magnética, caída de la Intranet del Estado, caída de backbones que alteren y/o interrumpan el normal funcionamiento de los equipos que se utilicen para los procesos de negocio.
- Por problemas y exposiciones en bases de datos tales como procesamiento interno erróneo, actividad errónea de administración de base de datos, corrupción de la base de datos, acceso indebido a la base de datos para modificarla, errores en puesta en producción / regresión con impacto en base de datos y errores en generación y restauración de respaldos que conlleven a la pérdida total o parcial de los servicios de negocio.
- Por problemas y exposiciones en aplicación y componentes del sistema tales como código malicioso en el software, fuga de información de claves de usuarios, ataques externos para obtención indebida de claves, suplantación de usuarios externos al pedir cambio de clave, ataques

□

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 27 de 68

externos para obtención/modificación indebida de información, y la inestabilidad del rendimiento del hardware y/o software que conlleve a la pérdida total o parcial de los servicios del negocio.

- Por acciones tomadas por personas que terminen en el sabotaje de los procesos de negocio a causa de chantaje, fraude, descontentos, huelgas, amenazas (acción disciplinaria o con despido), adictos y/o experimentación de problemas financieros o emocionales.

Dolo y/o imprudencia manifiesta por parte de personas directa y/o indirectamente involucrada en los procesos de negocios que conlleven a la suspensión total o parcial de los servicios.

- Pérdida del hardware, software y data de propiedad y/o tenida a cargo, en custodia y/o control del IDEAM.
- Pérdida o daño debido al cálculo o diseño erróneo del hardware y software.
- Falla y/o daño eléctrico interno o desarreglo de los equipos y dispositivos del centro de datos.
- Daños y/o fallas atribuibles a la falta y/o carencia de diligencia en los mantenimientos predictivos, preventivos y correctivos a los equipos y dispositivos del centro de datos.
- Daño total o parcial del hardware debido a los deterioros causados por el calor, el humo, el vapor, y/o los medios empleados para extinguir y/o contener un incendio ya sea por acción directa e inmediata del mismo, y las demoliciones que sean necesarias a consecuencia del incendio y que sean ordenadas en tal carácter por la autoridad competente.

□

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:28 de 68

- Por la combustión espontánea de algún elemento que forme parte de algún equipo y/o dispositivo del centro de datos.

4.3.3. Interrupciones al negocio o incidentes que podrían afectar el cumplimiento de las labores de los funcionarios.

Las interrupciones al negocio o incidentes que podrían afectar el cumplimiento de las labores de los funcionarios puede deberse a diferentes situaciones y/o motivos tales como:

- Pérdidas de personal (cesación, muerte, accidentes laborales, enfermedades)
- Cortes de servicio de transporte
- Fallas en los proveedores

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 29 de 68

4.3.4. Procedimiento de Failover y Failback

En el siguiente procedimiento se detalla de forma general el Failover o activación de los 21 servidores que forman parte de los servicios definidos como críticos por el IDEAM en CDA y el Failback de los mismos al CDP cuando se haya recuperado la operatividad del mismo.

De igual forma se confirma que durante la actual vigencia se han realizado pruebas y contingencias unitarias y totales de los servidores y servicios en el CDA, con resultados satisfactorios, los informes de los resultados de las pruebas se han entregado a la OI.

El procedimiento está definido en cuatro fases y se puede ejecutar para una prueba o contingencia real parcial o total de acuerdo a las necesidades del IDEAM:

4.3.4.1 Fase I: Actividades previas

1. Enviar comunicado por correo electrónico al Cliente IDEAM informando el inicio del cambio.
2. Solicitar al Command Center (Monitoreo) de IMPRETICS - SONDA poner en mantenimiento los servidores del servicio de DRP del IDEAM (DRP_BART_2, DRP_BAGUE, CAGUI-DRP, JBOSS6DC-DRP, JBOSS7DC-DRP, FORFEODRP, BORFEO-DRP, GUAYQUES-DRP, POLARIS-DRP, SUA_REPLICA, AQDAS-REPLICA, AQMP-REPLICA, AQTS-REPLICA, AQWP-REPLICA, DHIME-REPLICA, GIS1-REPLICA, GIS2-REPLICA, GIS3-REPLICA, GIS6REPLICA, AQDB-REPLICA, GUATQUYCA, BART, BAGUE, CAGUI, JBOSS6DC-PRD, JBOSS7DC-PRD, FORFEO, BORFEO, GUAYQUES,

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:30 de 68

POLARIS, SUA, AQDB-PRD, AQDAS-PRD, AQMP-PRD, AQTS-PRD1, AQWPPRD, DHIME-PRD, GIS1GDB, GIS2WGIS, GIS3GEOS1, GIS4GEOS2, GIS5IMGS y GIS6GEOEV)

3. Verificar en la consola de Carbonite Double-Take el estado de replicación de los servidores de DHIME (AQDAS-REPLICA, AQMP-REPLICA, AQTS-REPLICA, AQWP-REPLICA, DHIME-REPLICA, GIS1-REPLICA, GIS2-REPLICA, GIS3REPLICA, GIS6-REPLICA), es necesario que el Failover este configurado para que los servidores suban en CDA con el hostname y dirección IP del servidor origen y revisar que el servidor AQDB-REPLICA con replicación por Files & Folders no presente encolamiento.

4. Verificar en la consola de Carbonite Double-Take el estado de replicación de los servidores (CAGUI-DRP, JBOSS6DC-DRP, JBOSS7DC-DRP, FORFEO-DRP, BORFEO-DRP y POLARIS-DRP), es necesario que el Failover este configurado para que los servidores suban en CDA con el hostname y dirección IP del servidor destino y revisar que el servidor DRP_BAGUE con replicación por Files & Folders no presente encolamiento.

5. Detener la replicación de los servidores (DRP_BAGUE, CAGUI-DRP, JBOSS6DC-DRP, JBOSS7DC-DRP, FORFEO-DRP, BORFEO-DRP y POLARIS-DRP, AQDAS-REPLICA, AQMP-REPLICA, AQTS-REPLICA, AQWP-REPLICA, DHIME-REPLICA, GIS1-REPLICA, GIS2-REPLICA, GIS3-REPLICA, GIS6-REPLICA y AQDB-REPLICA).

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:31 de 68

6. Revisar el servidor de BD SUA-REPLICA del CDA y verificar la replicación por Data Guard entre los servidores de BD: SUA y SUA_REPLICA (instancias ideam11pr, ideam9pr, geodata y bdideam).
7. Revisar el servidor GUATQUYCA (DA, DNS y DHCP) del CDA y verificar la replicación este sincronizada entre los servidores de DA, DNS y DHCP: FURACHOGUA y GUATQUYCA.
8. En el CDA del IDEAM es necesario realizar un snapshot de los siguientes servidores: DRP_BAGUE, CAGUI-DRP, JBOSS6DC-DRP, JBOSS7DC-DRP, FORFEO-DRP, BORFEO-DRP, POLARIS-DRP, SUA_REPLICA, AQDAS-REPLICA, AQMP-REPLICA, AQTS-REPLICA, AQWP-REPLICA, DHIMEREPLICA, GIS1-REPLICA, GIS2-REPLICA, GIS3-REPLICA, GIS6-REPLICA, AQDB-REPLICA y GUATQUYCA:

4.3.4.2 Fase II: Failover – Actividades a ejecutar durante la ventana

1. En CDP se deben finalizar y apagar los siguientes servidores (BAGUE, CAGUI, JBOSS6DC-PRD, JBOSS7DC-PRD, FORFEO, BORFEO, GUAYQUES, POLARIS, AQDB-PRD, AQDAS-PRD, AQMP-PRD, AQTS-PRD1, AQWP-PRD, DHIME-PRD, GIS1GDB, GIS2WGIS, GIS3GEOS1, GIS4GEOS2, GIS5IMGS y GIS6GEOEV).
2. Crear el enrutamiento en el CPE de Renata - MC para las direcciones IP correspondientes a los servidores del servicio Dhime en CDP.
3. En el vCenter del CDA habilitar el enrutamiento para las direcciones IP correspondientes a los servidores del servicio Dhime en CDP

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:32 de 68

4. Para el servidor AQDB-REPLICA con método de replicación Files and Folders es necesario cambiar el hostname por AQDB-PRD, garantizar el direccionamiento IP del CDP y des comentar los filesystem.

5. Para el servidor DRP_BAGUE con método de replicación Files and Folders es necesario cambiar el hostname por BAGUE, conserva la dirección IP y el Gateway del CDA, des comentar los filesystem.

6. Para el servidor GUATQUYCA en CDA:

Verificación de roles por línea de comandos (netdom, query y fsmo)
 Se ingresa al controlador de dominio alterno en usuario y equipos se da click derecho sobre el dominio de en maestro de operaciones se cambian los roles RID, CONTROLADOR PRINCIPAL DE DOMINIO e INFRAESTRUCTURA.
 En seguida por línea de comandos se traen los dos roles restantes Maestro de Esquema y Maestro de Nomenclatura, de la siguiente forma: C:\ntdsutil
 ntdsutil:roles
 fsmo maintenace: transfer "el nombre del rol"
 * Una vez configurado el servidor para DHCP, se debe subir el servicio de servidor DHCP
 Realizar el cambio de contraseña para un usuario de directorio activo, luego de esto en la máquina cliente, configurar como DNS principal el AD de DRP y luego de esto reiniciar la máquina y hacer login con las nuevas credenciales:

7. Para la activación de SUA en CDA:

Conectarse con la utilidad de data guard broker dgmgrl utilizando password de sys.
 Ejecutar switchover de las 4 bases de datos
 Verificar que el proceso se ejecute correctamente para cada BD
 Validación de la aplicación de secuencias de archives en las nuevas bases de datos PRIMARIAS.
 Pruebas con cliente de BD

8. Para los servidores con replicación Full Server: CAGUI-DRP, JBOSS6DC-DRP,

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:33 de 68

JBOSS7DC-DRP, FORFEO-DRP, BORFEO-DRP, POLARIS-DRP, AQDASREPLICA, AQMP-REPLICA, AQTS-REPLICA, AQWP-REPLICA, DHIMEREPLICA, GIS1-REPLICA, GIS2-REPLICA, GIS3-REPLICA, GIS6-REPLICA, se debe seleccionar el Job y ejecutar el Failover.

9. Al finalizar el proceso, aparecerá la confirmación que se ejecutó el Failover, iniciando el servidor del ambiente de Contingencia, se verifica que los servidores (DHIME) se encuentren con el mismo hostname y direccionamiento IP del CDP
-

AUTOMATICO, revisar que los filesystem de los servidores CAGUI (GUETA-CONSOLA_DRP), GIS2WGIS, GIS3GEOS1 y GIS6GEOEV (GIS5IMGS) estén bien presentados (replicación F&F) y copiar /u01/Dhime de GIS2WGIS a GIS3GEOS1.

* Presentar la Biblioteca documental del Portal Web desde la CONSOLA-DRP (N:\Shares\) a CAGUI.

* Extraer /u01/Data/Servicios del .dtstaging de GIS2WGIS, GIS3GEOS1 y GIS6GEOEV

Los servidores CAGUI-DRP, JBOSS6DC-DRP, JBOSS7DC-DRP, FORFEO-DRP, BORFEO-DRP, POLARIS-DRP suben con el direccionamiento IP del CDP."

10. Mover los servidores del Servicio Dhime de la VLAN de replicación a la VLAN de activación de contingencia.
11. Poner la MAC del Servidor del CDP Nodo1W2008Oraculo en el servidor POLARIS-DRP del CDA.
12. Subir las instancias de la BD AQDB en CDA.
13. Subir las instancias de la BD Postgres del servidor GIS1GDB en CDA.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:34 de 68

14. Subir la BD BORFEO.

15. Verificar que los servicios en los servidores del CDA suban correctamente y realizar los apuntamientos necesarios.

*Inhabilitar los formularios de ORFEO

*Revisar en ORFEO el ultimo PQR ingresado, en radicados y tabla auditoria

*Garantizar el banner de indisponibilidad del Portal Web

4.3.4.3. Fase III: Pruebas funcionales en CDA

1. Activación y prueba funcional del servicio DHIME en contingencia, se adjunta la lista de servidores del servicio Dhime en CDA (AQDB-PRD, AQDAS-PRD, AQMP-PRD, AQTS-PRD1, AQWP-PRD, DHIME-PRD, GIS1GDB, GIS2WGIS, GIS3GEOS1 y GIS6GEOEV).

2. Activación y prueba funcional del servicio POLARIS en contingencia, se adjunta la lista de servidores del servicio en CDA (POLARIS).

3. Activación y prueba funcional del Portal Web(SMARMET, SIRH, PRONOSTICOS, PCB, LIFERAY -FULL PORTAL, GLACIARES ANDINOS y GEOVISOR) en contingencia, se adjunta la lista de servidores del servicio en CDA (BART, BAGUE, CAGUI, JBOSS6DC-PRD, JBOSS7DC-PRD, GUAYQUES, CONSOLA-DRP y SUA).

4. Activación y prueba funcional del Gestor Documental en contingencia, se adjunta la lista de servidores del servicio en CDA (ORFEO y BORFEO).

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:35 de 68

4.3.4.4. Fase IV: Failback – Actividades a ejecutar regreso a CDP

1. Restaurar los snapshot de los servidores a los que se les tomo en actividades preliminares: DRP_BAGUE, CAGUI-DRP, JBOSS6DC-DRP, JBOSS7DC-DRP, FORFEO-DRP, BORFEO-DRP, POLARIS-DRP, SUA_REPLICA, AQDAS-REPLICA, AQMP-REPLICA, AQTS-REPLICA, AQWP-REPLICA, DHIMEREPLICA, GIS1-REPLICA, GIS2-REPLICA, GIS3-REPLICA, GIS6-REPLICA, AQDB-REPLICA y GUATQUYCA.
2. Reversar el enrutamiento en el CPE de Renata - MC para los servidores del servicio DHIME.
3. Reversar en el vCenter del CDA el enrutamiento creado para el grupo de servidores del servicio DHIME y mover este grupo de servidores de la VLAN de contingencia a la VLAN de replicación.
4. Revisar que todos los servidores en el CDA (DRP_BART_2, DRP_BAGUE, CAGUI_DRP, JBOSS6DC-DRP, JBOSS7DC-DRP, FORFEO-DRP, BORFEODRP, GUAYQUES-DRP, POLARIS-DRP, SUAREPLICA, DRP_FURACHOGUA (GUATQUYCA), AQDB-RELICA, AQDAS-REPLICA, AQMP-REPLICA, AQTSREPLICA, AQWP-REPLICA, DHIME-REPLICA, GIS1-REPLICA, GIS2REPLICA, GIS3-REPLICA y GIS6-REPLICA) se encuentren con su hostname y direccionamiento IP de forma correcta.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	<p align="center">PLAN DE RECUPERACIÓN DE DESASTRES IDEAM</p>	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:36 de 68

5. En CDP se deben iniciar los siguientes servidores: BART, BAGUE, CAGUI, JBOSS6DC-PRD, JBOSS7DC-PRD, FORFEO, BORFEO, GUAYQUES, POLARIS, SUA, FURACHOGUA, AQDB-PRD, AQDAS-PRD, AQMP-PRD, AQTS-PRD1, AQWP-PRD, DHIME-PRD, GIS1GDB, GIS2WGIS, GIS3GEOS1, GIS4GEOS2, GIS5IMGS y GIS6GEOEV.

6. Para el servidor el servidor FURACHOGUA en CDP:

Verificación de roles por línea de comandos (netdom, query y fsmo)

Se ingresa al controlador de dominio alterno en usuario y equipos se da click derecho sobre el dominio de en maestro de operaciones se cambian los roles RID, CONTROLADOR PRINCIPAL DE DOMINIO e INFRAESTRUCTURA.

En seguida por línea de comandos se traen los dos roles restantes Maestro de Esquema y Maestro de Nomenclatura, de la siguiente forma: C:\ntdsutil ntdsutil:roles

fsmo maintenace: transfer ""el nombre del rol""

* Una vez configurado el servidor para DHCP, se debe subir el servicio de servidor
DHCP"

7. Realizar retorno de la BD SUA a CDP:

Conectarse con la utilidad de data guard broker dgmgrl utilizando password de sys

Ejecutar switchover de las 4 bases de datos

Verificar que el proceso se ejecute correctamente

Validación de la aplicación de secuencias de archivos en las nuevas bases de datos PRIMARIAS

Pruebas con cliente de BD

8. Realizar pruebas de funcionalidad de SUA en CDP. se debe probar que todos los aplicativos productivos que consumen las instancias de la BD SUA logren hacerlo.

9. Verificar que los servicios en los servidores del CDP suban correctamente.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:37 de 68

10. Realizar pruebas funcionales de los servicios en CDP: Portal Web, Dhime, Polaris, Gestor Documental y BDs.
11. Iniciar los jobs de replicación y validar que inicien sincronización de forma correcta, revisar la replicación F&F de los servidores BART, BAGUE, CAGUI, GIS2-REPLICA, GIS3-REPLICA y GIS6-REPLICA.
12. Declarar el fin de la prueba parcial o total de contingencia del Servicio DRP del IDEAM.

5.1. Centro de Datos Alterno - CDA

El centro de datos alternativo para el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM está ubicado en Colombia XV CenturyLink (Level 3) ubicado en la ciudad de Bogotá – Carrera 68 No. 169^a-27 y 169^a-45.

Este Data Center tiene clasificación TIER III de acuerdo con las especificaciones requeridas por la norma NFPA75 y norma EIA/TIA 942. El Data Center está ubicado a una distancia lineal de 12,61 km respecto al Centro de Datos Principal del Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:38 de 68

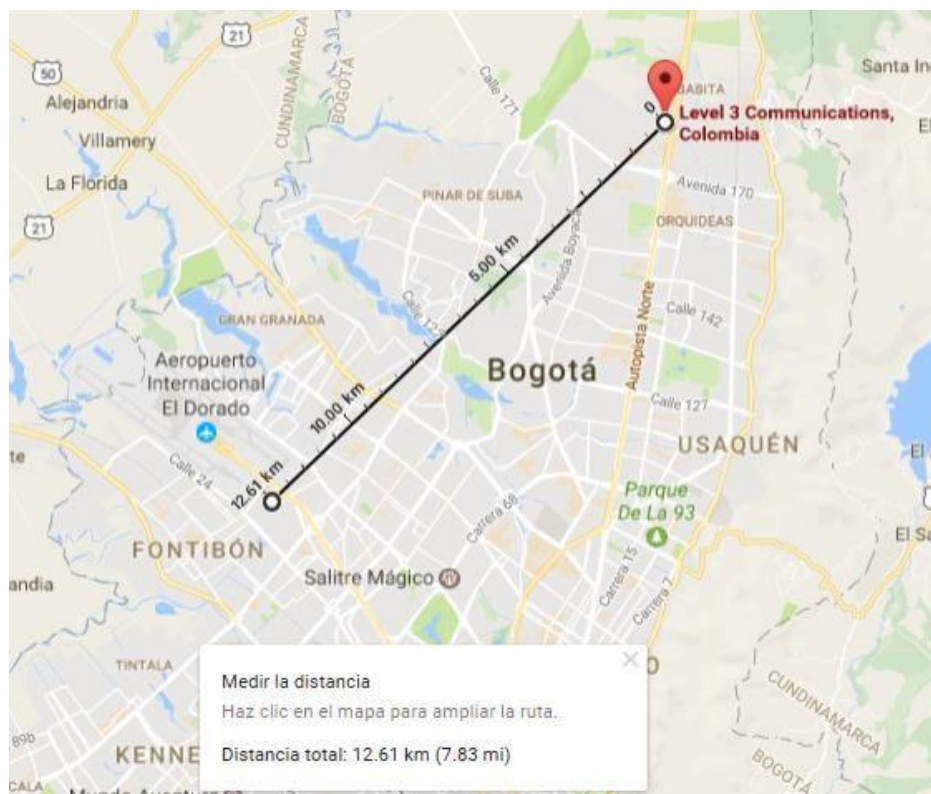



Figura 4 – Distancia lineal del centro de datos alternativo

La infraestructura del centro de datos alternativo provista por Colombia XV CenturyLink (Level 3) para el alojamiento de los componentes de hardware que hacen parte de la solución de DRP para el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM, es la siguiente:

- Suministrar toda la infraestructura tecnológica de servidores.
- Suministrar mínimo 15,6 TB de almacenamiento.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021

Página:39 de 68

- Monitoreo y administración en contingencia.
- Replicación en línea mediante una canal de datos MPLS de 128 Mbps provisto por el IDEAM.
- Replicación de todos los servicios contemplados en el alcance del DRP.
- Pruebas reales de todos los servicios por lo menos una vez durante la vigencia del contrato.

5.2. Canales de comunicaciones

Se dispondrán de los siguientes canales de comunicación:

Enlace de replicación MPLS de 128 Mbps con redundancia entre el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM y Colombia XV modalidad MPLS, asegurando que los servicios del sitio principal o CDP se puedan avisar y usar en el Data Center de contingencia o CDA.

	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:40 de 68

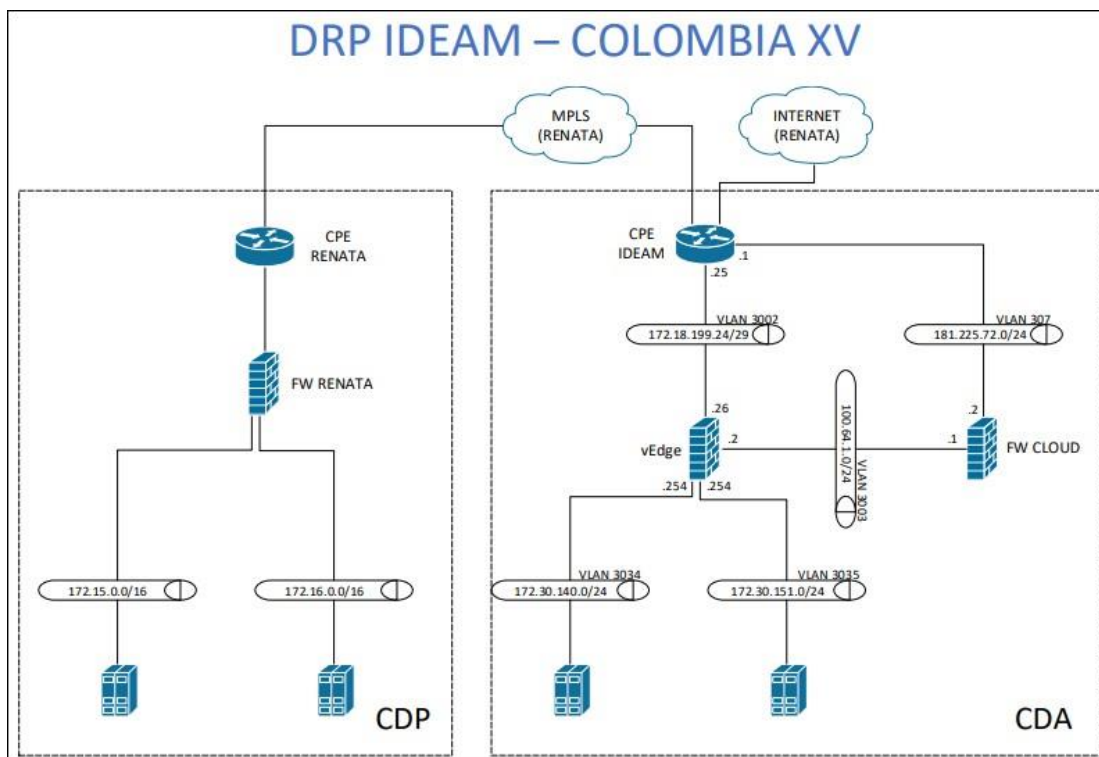


Figura 5 - Diagrama general de conectividad

5.2.1. Conectividad

Los diferentes componentes físicos instalados en los racks, se encuentran conectados a través de los FW que hacen parte de la solución, permitiendo la gestión y comunicación adecuada. Toda la conectividad de management se centralizará en el FW EDGE (NAT POLICYS) y FW CLOUD (IPS), generando separación lógica de tráfico y garantizando optimizar el tráfico productivo.

5.3. Centro de Operaciones Alternativo - COA

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	<p align="center">PLAN DE RECUPERACIÓN DE DESASTRES IDEAM</p>	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:41 de 68

El Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM contrató de manera exclusiva cinco (5) puestos de trabajo en el sitio alternativo para ser utilizados por personal de la entidad. Estos deben disponer de área física de trabajo, equipo de cómputo con capacidad para atender las necesidades mínimas de oficina y aplicaciones, conexión segura al sitio alternativo, instructivo detallado para el acceso a las aplicaciones.

IMPRETIC'S E.I.C.E. tiene a disposición en sus instalaciones ubicadas en la Autopista Norte No. 118-68 el Centro de Operaciones Alterno (COA), el cual se encuentra a más de 12,5 Km medidos en línea recta del Centro de Datos Principal ubicado en el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM en la Calle 25 D # 96B -70 en la ciudad de Bogotá.

Las principales características y servicios que presta el Centro de Operaciones Alterno (COA) se describen a continuación:

- Conexión con el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM y con el Centro de Datos Alterno (CDA).
- Cinco (5) puestos de trabajo dotados de una (1) silla, un (1) computador y Acceso controlado.
- Los equipos cuentan con salida a Internet y conexión al Centro de Datos Alterno y al Centro de Datos Principal en el Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM

5.3.1. Centro de monitoreo

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	<p align="center">PLAN DE RECUPERACIÓN DE DESASTRES IDEAM</p>	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 42 de 68

El Centro de Monitoreo está ubicado en las instalaciones de IMPRETIC´S E.I.C.E. - SONDA DE COLOMBIA S.A. a más de 12,5 Km medidos en línea recta del Centro de Datos Principal ubicado en Instituto de Hidrología, Meteorología y Estudios Ambientales - IDEAM

A continuación, se enuncian las principales características y servicios que presta el Centro de Monitoreo:

- Operadores 7x24.
- Verificación de la operatividad de los equipos y componentes.
- Notificación en caso de alarmas o de alteraciones en los sistemas.

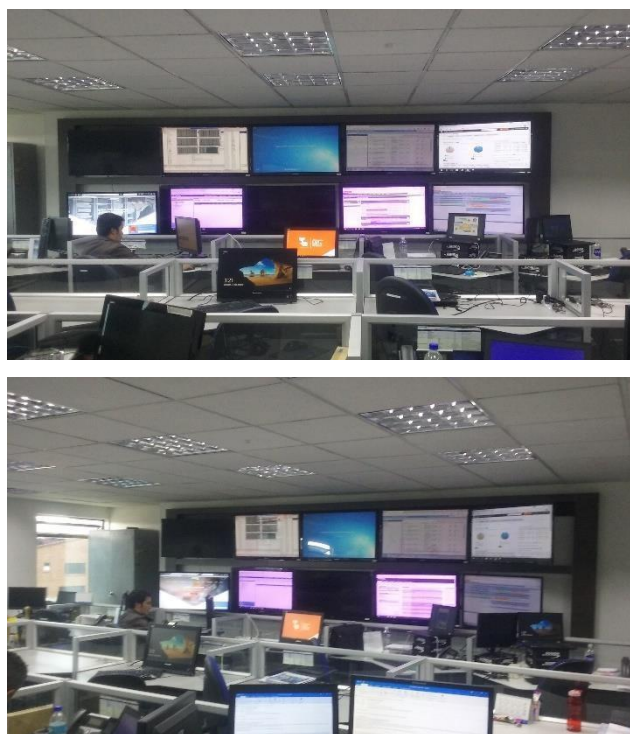


Figura 6 - Centro de monitoreo ROC – CDA

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 43 de 68

6. PROCEDIMIENTO DE NOTIFICACIÓN, ACTIVACIÓN Y RETORNO

Como parte de las estrategias inmediatas ante una posible eventualidad y/o crisis, se contemplan las tareas que deben efectuarse de manera oportuna, tan pronto se identifique un evento que comprometa la prestación de alguno de los servicios críticos, para reducir posibles impactos. En muchos casos, estos procedimientos contemplan la comunicación inicial con clientes y otros contactos externos.

A continuación, se listan las actividades a ejecutar cuando se active la contingencia, de acuerdo con la presentación de cualquier tipo de evento adverso:

Tipo de evento	Características	Ejemplos	Respuesta
DESASTRE	Evento que inhabilita el Centro de Datos Principal para prestar sus servicios. No permite seguir laborando en las instalaciones principales del Instituto.	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 considerado como un desastre o una contingencia, dependiendo del impacto que se determine en el manejo de incidentes.	Incendio localizado, atentado terrorista, huelga interno o externo.	DRP Planes contingencia
CONTINGENCIA	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática. No impide el acceso al CDP. 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 contingencia

Tabla 2 - Clasificación de eventos

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:44 de 68



Figura 7 - Fases de activación

Así mismo se listan algunas actividades anexas a las fases definidas anteriormente:

1. Registro de Incidentes.
2. Evaluación inicial del alcance del incidente y fallos.
3. Validar la criticidad de la falla (contingencia menor, mayor o catastrófica).
4. Comunicar al comité.
5. Activar alertas.
6. Activar mitigación desastre.
7. Activación del plan de recuperación de desastres.
8. Ejecución procedimientos de contingencia.
9. Notificación contingencia.
10. Monitoreo y seguimiento periodo de contingencia.
11. Comunicación continua interna/externa a involucrados.
12. Activación de plan de retorno de contingencia.
13. Declaración de fin de contingencia.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:45 de 68

14. Retorno al modo normal de operación.
15. Notificación formal de fin de contingencia.
16. Actualización del plan de recuperación de desastres.
17. Documentación de lecciones aprendidas.
18. Actualización planes de prueba.
19. Fin de contingencia.

6.1. Procedimiento de notificación

Cuando se presenta una emergencia, hay que tener en cuenta que se debe gestionar la notificación de la misma, con el propósito de iniciar con el proceso de activación del Plan de Recuperación de Desastres (DRP). Esta notificación corresponde a una gestión de activación del plan la cual se describe a continuación:

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:46 de 68



Figura 8 - Procedimiento de notificación

La notificación de la indisponibilidad de los sistemas de información o servicios de TI puede llegar por diferentes fuentes, esto va a depender de la naturaleza del evento, del momento en el cual éste suceda y de la fuente que lo causa. El procedimiento de notificación debe estar acorde a los procedimientos de Emergencia definidos y establecidos por el IDEAM.

Así mismo se describe el proceso mediante el cual se activa la gestión del plan, previa notificación del desastre, y hasta el momento en que el servicio es restaurado en el Sitio Principal en producción:

	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:47 de 68

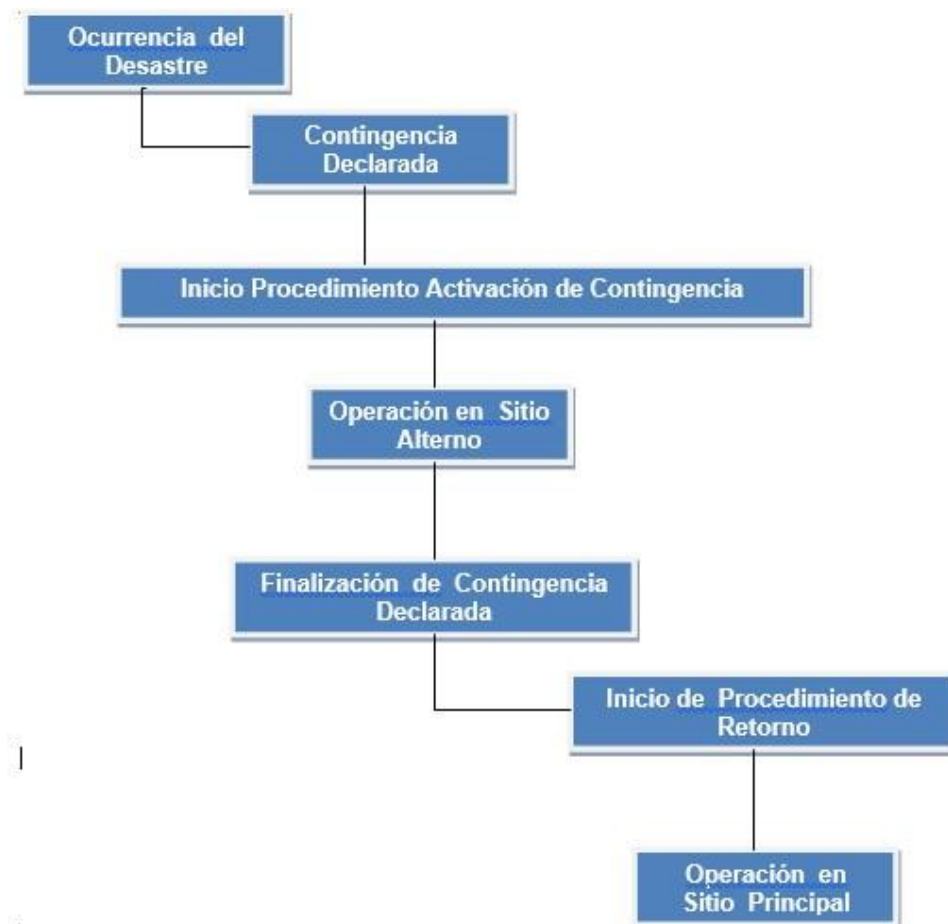


Figura 9 - Proceso de activación gestión del plan

6.2. Detección del evento

Los eventos que afectan la continuidad de las operaciones de los servicios críticos esenciales (listado de servidores y servicios) identificados por el IDEAM, podrán ser reportados una vez identificados con el fin de iniciar a trabajar en una pronta atención y garantizar el cumplimiento de los tiempos de atención, los RTO's y RPO's definidos.

Esta detección de eventos se realizará una vez se presenten interrupciones de los servicios:

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:48 de 68

1. Servicio de FTP
2. Servicios WEB (SMARMET, SIRH, PRONOSTICOS, PCB, LIFERAY, PORTAL INSTITUCIONAL, GLACIARES ANDINOS y GEOVISOR)
3. Sistema de recepción de datos de estaciones automáticas - Polaris
4. Servicio de gestión documental
5. Bases de datos Oracle y PostgreSQL
6. Directorio Activo, DNS y DHCP
7. Servicio DHIME

Los anteriores servicios descritos, fueron definidos por la entidad como críticos, y en ellos se relacionan la totalidad de los servidores que se encuentran en el alcance del DRP y para los cuales se debe garantizar su correcto funcionamiento.

6.3. Roles y Responsabilidades - Definición de recursos

Como parte del Plan de Recuperación de Desastres (DRP), se realizó la definición de los siguientes recursos, cuyos miembros de los equipos de trabajo atenderán las solicitudes realizadas por el IDEAM, teniendo en cuenta las responsabilidades específicas que les han sido asignadas.

- **Comité de Emergencias:** Hace parte de la contingencia en la presentación de un evento adverso, este equipo de emergencias debe ser definido internamente en la entidad y en él se debe mantener informado al responsable de la activación de la contingencia.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:49 de 68

- **Comité responsable de activación del DRP:** se encuentra conformado por los responsables de la activación del plan de recuperación de desastres - DRP.
- **Equipo de Recuperación del DRP:** Incluye todo el personal técnico de la oficina de informática de la entidad, encargados de realizar la activación de los servicios definidos como críticos y la puesta en funcionamiento de los servidores contemplados dentro del alcance.

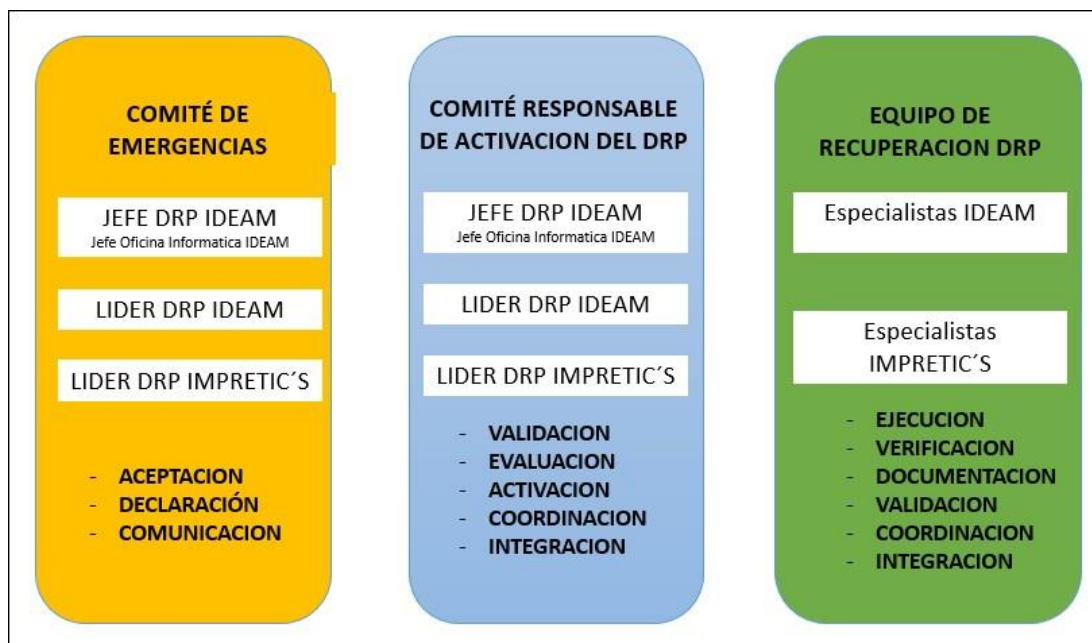


Figura 10 – Definición de recursos

6.3.1. Comité de emergencias

Realiza la evaluación de los daños y la magnitud del suceso, trabaja conjuntamente con el equipo del DRP, su principal función es salvaguardar las vidas humanas, este comité es informado de manera inmediata ante cualquier incidencia para la toma de decisiones efectivas para la superación de eventos y dar alcance a la comunicación oportuna al

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:50 de 68

jefe del DRP para iniciar la activación de los servicios definidos en el alcance. La intervención de este grupo durante una situación de contingencia está determinada por el tipo de daño, siendo necesaria su gestión en la ocurrencia de algún evento.

Hace parte del Comité de Emergencias el equipo evaluador de daños quienes validan los daños a la infraestructura de IT con el fin de determinar la afectación y poder informar con el Comité de Emergencias al comité de activación del DRP si se debe declarar una contingencia.

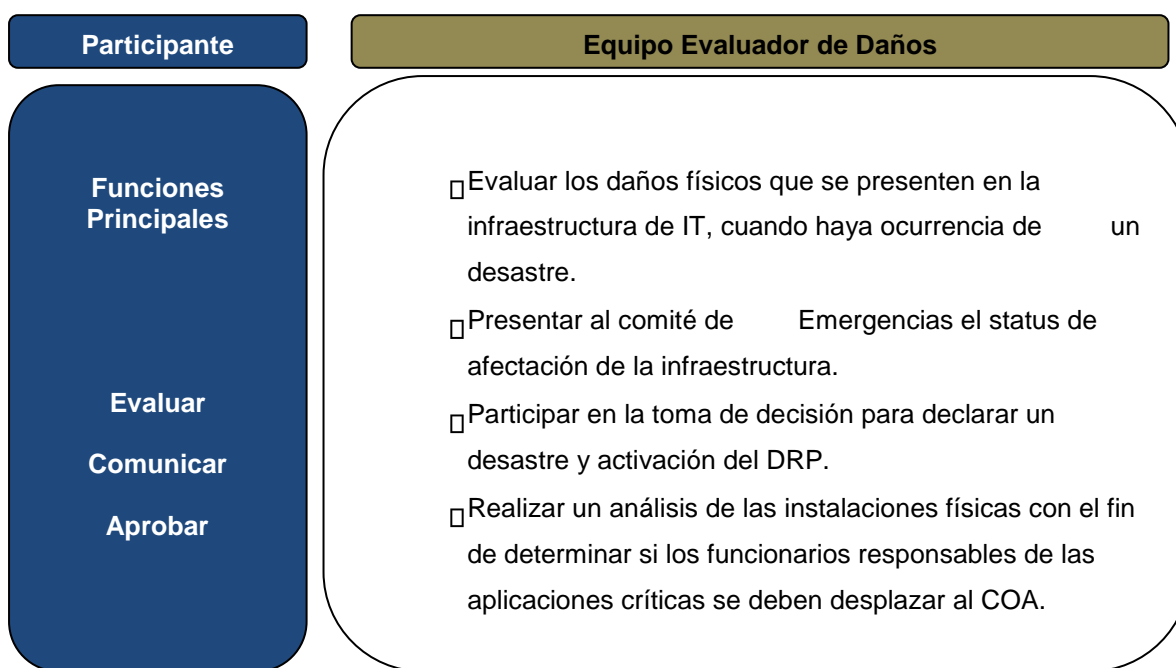


Tabla 3 – Equipo evaluador de daños

6.3.2. Comité de responsables de activación del DRP

Está conformado por el Jefe de la Oficina de Informática. Esto no es una limitante en caso que se decida invitar a participar dentro de este equipo a algunos funcionarios del nivel ejecutivo del Instituto como el mismo Director General, Subdirectores o Jefes de

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:51 de 68

Oficina. No se debe perder de vista el carácter técnico del DRP y por tanto el nivel de especialización del equipo.

Se debe asegurar la comunicación permanente con las altas directivas del Instituto en cada momento (antes, durante y después) por la naturaleza de las decisiones que se deban tomar. El Coordinador del DRP y el Líder DRP también integran este equipo a nivel de apoyo para la toma de decisiones.

Algunas de las responsabilidades de este equipo son:

- Establecer las directrices y políticas del DRP enmarcadas en un Plan de Continuidad de Negocios alineadas con el Sistema de Gestión de Continuidad de Negocio.
- Mantener contacto con la alta dirección, proveedores y entidades interesadas, sobre la situación del IDEAM.
- 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 institucional.
- Supervisión de la efectividad de las actividades de recuperación.

	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 52 de 68



Figura 11 – Activación DRP IDEAM

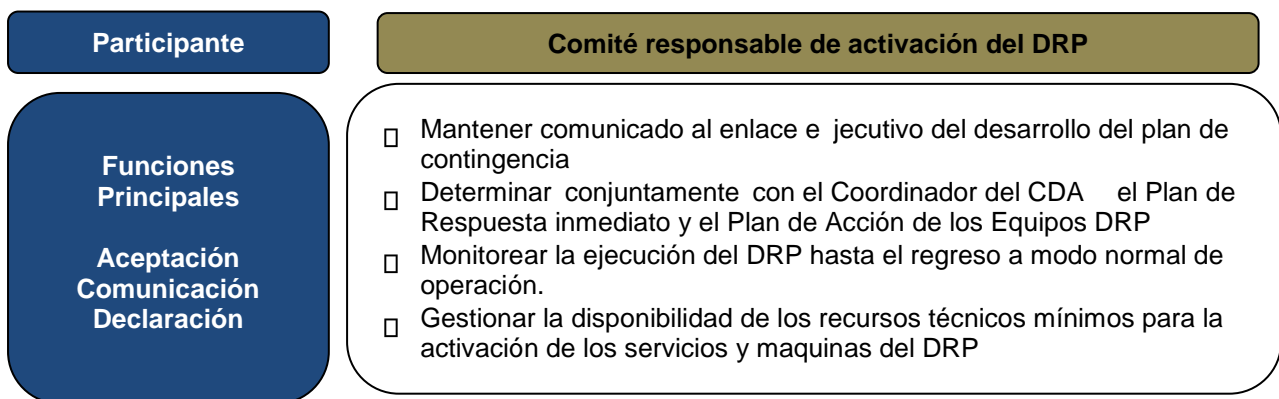


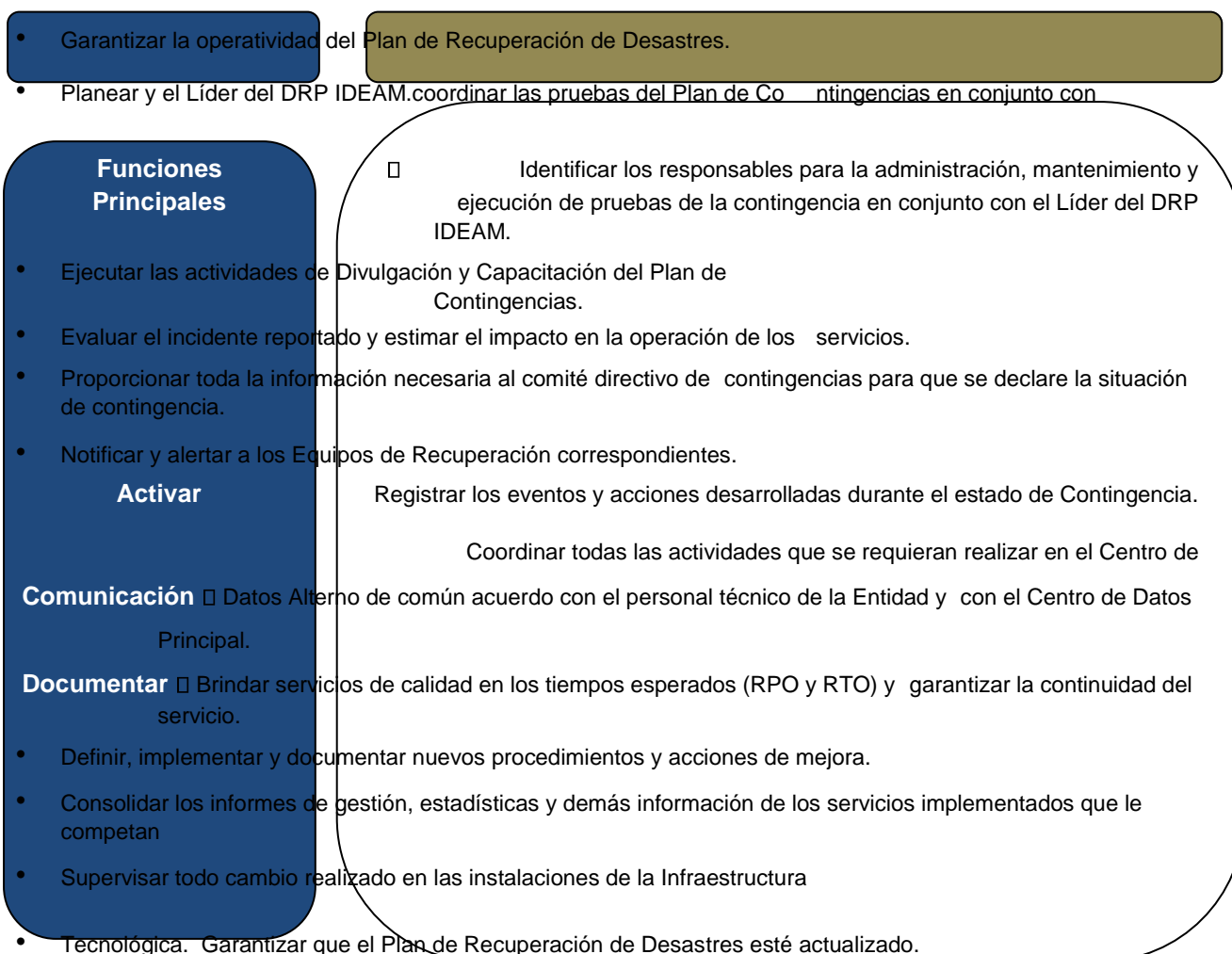
Tabla 4 – Comité responsable de activación del Plan de recuperación de desastres DRP

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 53 de 68

En conjunto como parte del equipo de trabajo se encuentran:

- Líder DRP IDEAM y el Coordinador del DRP, quienes tienen a su cargo:

Coordinador DRP – Líder DRP IDEAM



 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 54 de 68

Tabla 5 – Coordinador DRP – Líder DRP IDEAM

6.3.3. Equipo de recuperación del DRP

Está compuesto por: Equipo evaluador de daños del (IDEAM), Coordinador del CDA, Especialistas y el Equipo de Soporte a Usuarios.

Recibe la confirmación de activación del Plan de Recuperación de Desastres DRP del comité responsable de activación del DRP y se encarga de restablecer la operación de los servicios de hardware, software, telecomunicaciones, energía y seguridad física que dificulten la continuidad de la operación en el sitio principal.

Participante

Equipo Recuperación de Contingencia

- Llevar a cabo los procedimientos de recuperación de la operación cuando se declare la contingencia, en coordinación con los responsables designados de cada proceso.

Principales ☐ Ejecutar el Plan de Pruebas para los pasos a seguir en el retorno a producción.

- Mantener un inventario y registro actualizado de los equipos, componentes y aplicaciones que integran la infraestructura tecnológica a recuperar.
- Mantener actualizados las copias de respaldo y documentos necesarios para la recuperación en caso de eventos o contingencias. Identificar y documentar los requerimientos mínimos para la operación de las aplicaciones.
- Identificar las debilidades de la Infraestructura frente al escenario de contingencia.

EJECUCIÓN

VERIFICACIÓN

DOCUMENTACION

VALIDACIÓN

COORDINACIÓN

INTEGRACIÓN

- ☐ Mantener actualizados los listados de contactos técnicos, proveedores y equipos de contingencia con datos de ubicación (teléfono, Celular, Dirección, email) para emergencias.
- ☐ Evaluar el tipo de daño ocurrido sobre el o los servicios reportados. Informar al Equipo Coordinador de Contingencias sobre el evento.
- Ejecutar los procedimientos de activación del Plan de Contingencias establecidos previamente.
- Contactar a los proveedores o personas responsables para superar la contingencia.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	<p align="center">PLAN DE RECUPERACIÓN DE DESASTRES IDEAM</p>	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:55 de 68

- Informar al Equipo Coordinador de Contingencias sobre el avance y el tiempo de recuperación estimados.
- Ejecutar las acciones de recuperación pertinentes a cada acción desarrollada.
- Evaluar la efectividad del Plan de Contingencias para su área de responsabilidad.

Tabla 6 – Equipo recuperación contingencia

Dentro del equipo de Recuperación de Contingencias se encuentran los diferentes roles de especialistas en cada una de las áreas junto con sus responsabilidades así:

Equipo de la plataforma Linux.

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios específicos de la plataforma Linux sobre los cuales funcionan las aplicaciones identificadas como muy críticas y los servicios que las apoyan, desde un Centro de Datos Alterno. 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, y las que conduzcan al restablecimiento de los servicios desde el Centro de Cómputo Principal.

Algunas de las responsabilidades de este equipo 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 contingencia.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:56 de 68

- Mantener iguales las configuraciones de los equipos del sitio principal y del sitio alternativo, en hardware y software.
- 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 sitio alternativo.
- Asistir la recuperación de la plataforma en el sitio principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 57 de 68

- Restaurar el servicio en el centro de datos principal.
- Alistar el sitio alternativo para usarlo nuevamente después de un retorno a la normalidad.

Equipo de la plataforma Windows.

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios específicos de la plataforma Windows sobre los cuales funcionan las aplicaciones identificadas como muy críticas y los servicios que las apoyan, desde un Centro de Datos Alterno. 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, y las que conduzcan al restablecimiento de los servicios desde el Centro de Cómputo Principal.

Algunas de las responsabilidades de este equipo 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 Centro de Datos Principal y del Centro de Datos Alterno, en Hardware y Software.
- 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 Centro de Datos Alterno.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:58 de 68

-
- Asistir la recuperación de la plataforma en el Centro de Datos Principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
Restaurar el servicio en el Centro de Datos Principal.
- Alistar el Centro de Datos Alterno para usarlo nuevamente después de un retorno a la normalidad.

Equipo de Base de Datos.

Es el responsable de planear y ejecutar las actividades que permitan la activación de los servicios específicos sobre los cuales funcionan las bases de datos de las aplicaciones identificadas como muy críticas y los servicios que las apoyan, desde un Centro de Datos Alterno. Igualmente es responsable de todas las actividades que garanticen la adecuada disponibilidad del servicio de respaldo en cuanto la actualización de datos y documentación, y las que conduzcan al restablecimiento de los servicios desde el Centro de Datos Principal.

Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y arranque de los servidores de base de datos y los planes recuperación.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Verificar la realización de las copias de seguridad.
- Verificar el estado de la actualización, se debe procurar que los datos del centro de datos principal y el del centro de datos alternativo, esté al mismo nivel de

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:59 de 68

- actualización (toda mejora, cambio y demás debe estar documentada y validar que en el sitio alterno hayan sido implementadas).
- Tener disponibilidad de los medios de instalación de los gestores de Bases de Datos.
- 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 periódicamente o cuando se tenga contemplado con el proveedor.
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el Centro de Datos Alterno.
- Asistir la recuperación de la plataforma en el Centro de Computo Principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el Centro de Datos Principal.
- Alistar el Centro de Datos Alterno para usarlo nuevamente después de un retorno a la normalidad.

Equipo de Conectividad.

Es el responsable de planear y coordinar las actividades que permitan la activación de los servicios específicos de conectividad sobre los cuales se apoya la entrega de los servicios de TI en un Centro de Datos Alterno. 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, y las que conduzcan al restablecimiento de los servicios desde el Centro de Datos Principal o desde el COA - Centro de Operación Alterna.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:60 de 68

-

Algunas de las responsabilidades de este equipo son:

- Mantener actualizados los procedimientos de instalación y arranque de los Equipos de conectividad.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Mantener iguales las configuraciones de los equipos del CDP y del CDA, en HW y SW.

Definir y ejecutar pruebas del DRP cuando se tenga establecido con el proveedor.

- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el CDA.
- Asistir la recuperación de la plataforma en el CDP.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el CDP.
- Alistar el CDA para usarlo nuevamente después de un retorno a la normalidad.

Equipo de Administradores de la Aplicación.

Es el responsable de planear y ejecutar las actividades que permitan la activación de las aplicaciones en los respectivos servidores de tal forma que se restablezcan los servicios de TI en un Centro de Datos Alterno.

- Mantener actualizados los procedimientos de instalación y arranque de las aplicaciones.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:61 de 68

-
- Mantener actualizado los requerimientos para la operación de las aplicaciones.
- Conocer y divulgar a los miembros de los equipos los procedimientos de notificación de contingencia.
- Velar porque las configuraciones de los equipos del CDP y del CDA, en HW y SW sean apropiadas para el correcto funcionamiento de las aplicaciones.
- Velar porque las versiones de las aplicaciones disponibles en el CDP y el CDA sean las mismas.
- Definir y ejecutar pruebas del DRP en lo referente a las aplicaciones.
- Definir y apoyar la ejecución de las pruebas del DRP.
- Velar porque se realicen los respaldos a la aplicación de acuerdo con las necesidades.
- Mantener los medios de instalación disponibles.
Mantener los contratos de soporte de acuerdo a lo requerido por el Instituto.
- Atender los requerimientos de auditoria
- Determinar el impacto en caso de falla y emitir concepto para toma de decisiones.
- Activar servicios de la plataforma en el CDA.
- Proveer soporte técnico según requerimientos del momento.
- Documentar fallas y su solución.
- Asistir la recuperación de las aplicaciones en el CDP.
- Restaurar el servicio en el CDP.
- Alistar el CDA para usarlo nuevamente después de un retorno a la normalidad.

Equipo de Usuarios.

Corresponde al grupo de personas que han sido identificadas como responsables funcionales de los aplicativos que utilizan los servicios prestados por la Oficina de

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:62 de 68

-
Informática para ejecutar las funciones propias de su proceso y otras complementarias al trabajo diario.

Algunas de las responsabilidades de los usuarios 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 auditorías)
- Actualizar la información de continuidad de las operaciones internas de su proceso y divulgarlos al interior del mismo. En este proceso se deberá seguir los lineamientos de control documental y de versiones del Instituto.
- 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

El equipo de Soporte a Usuarios debe brindar el soporte a los usuarios finales de la entidad para el desarrollo de sus actividades tareas durante el tiempo que esté operativa la contingencia.

El equipo está conformado por:

- Coordinador de la Mesa de Ayuda del IDEAM
- Soporte Nivel I y II de la Mesa de Ayuda
- Operadores del Centro de Datos Alterno

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:63 de 68

-

Responsabilidades:

- Conocer y entender el Plan de Contingencia.
- Verificar con los usuarios finales del IDEAM la estabilidad de las aplicaciones y reportar anomalías.
- Cooperar con el Equipo de Recuperación de Contingencias en la puesta en marcha del Plan de Contingencia.
- Verificar con los usuarios finales del IDEAM la estabilidad de las aplicaciones y reportar anomalías.
- Actualizar los procedimientos existentes en el Manual de Contingencias que esté relacionado con su trabajo.

	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:64 de 68


6.3.3.1. Responsables oficina de informática del IDEAM para la activación de los servicios del DRP.

Una vez declarada la activación del DRP del IDEAM, se procede a dirigirse al personal de la oficina de informática para habilitar los servicios y las comunicaciones según corresponda:

Responsables OI del IDEAM para la activación de los servicios del DRP							
Servidor CDP	Servidor CDA	PRINCIPAL	CORREO	TELEFONO	SUPLENTE	CORREO	TELEFONO
BART	DRP_BART_2	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
BAGUE	DRP_BAGUE	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
CAGUI	CAGUI-DRP	FABIO ROJAS	macarrillo@ideam.gov.co	3005298687	NO ESTABLECIDO		
JBOSS6DC-PRD	JBOSS6DC-DRP	FABIO ROJAS	macarrillo@ideam.gov.co	3005298687	NO ESTABLECIDO		
JBOSS7DC-PRD	JBOSS7DC-DRP	FABIO ROJAS	macarrillo@ideam.gov.co	3005298687	NO ESTABLECIDO		
AQDB-PRD (HV-SO)	AQDB-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
AQDB-PRD (BD)	AQDB-REPLICA	MAURICIO DAZA	emdaza@ideam.gov.co	316 2690451	SANDRO LLANOS	sandro.llanos@sonda.com	312 5123131
FURACHOGUA	DRP_FURACHOGUA	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127	A. FELIPE ARIAS	afarias@ideam.gov.co	312 2890963
FORFEO	FORFEO-DRP	FABIO ROJAS	macarrillo@ideam.gov.co	3005298687	NO ESTABLECIDO		
BORFEO (HV-SO)	BORFEO-DRP	FABIO ROJAS	macarrillo@ideam.gov.co	3005298687	NO ESTABLECIDO		
BORFEO (BD)	BORFEO-DRP	MAURICIO DAZA	emdaza@ideam.gov.co	316 2690451	SANDRO LLANOS	sandro.llanos@sonda.com	312 5123131
GUAYQUES	GUAYQUES-DRP	FABIO ROJAS	macarrillo@ideam.gov.co	3005298687	NO ESTABLECIDO		
POLARIS	POLARIS-DRP	ANDRES BRAVO	abravo@ideam.gov.co	3017548303	NO ESTABLECIDO		
AQDAS-PRD	AQDAS-PRD-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
AQMP-PRD	AQMP-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
AQTS-PRD1	AQTS-PPRD-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
AQVP-PRD	AQVP-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
DHIME-PRD	DHIME-PRD	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
GIS1GDB (HV-SO)	GIS1-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
GIS1GDB(BD)	GIS1-REPLICA	MAURICIO DAZA	emdaza@ideam.gov.co	316 2690451	SANDRO LLANOS	sandro.llanos@sonda.com	312 5123131
GIS2VGIS	GIS2-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
GIS3GEOSI	GIS3-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
GIS6GE0EY	GIS6-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
SUA (HV-SO)	SUA-REPLICA	A. FELIPE ARIAS	afarias@ideam.gov.co	3122890963	JAVIER H. GARCIA	jhgarciag@ideam.gov.co	321 4656127
SUA(BD)	SUA-REPLICA	MAURICIO DAZA	emdaza@ideam.gov.co	316 2690451	SANDRO LLANOS	sandro.llanos@sonda.com	312 5123131

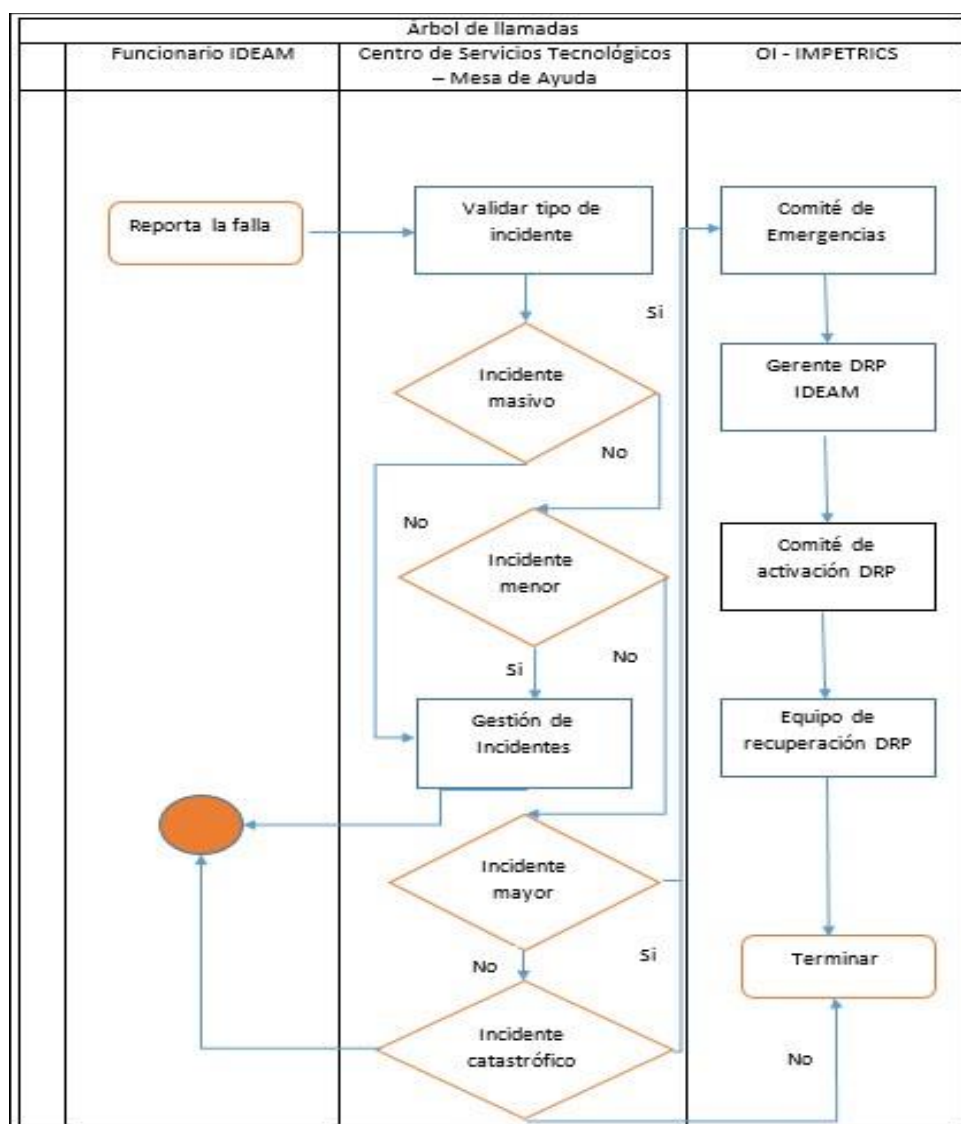
Figura 12 – Responsables activación de servicios del DRP.

NOTA: Es importante destacar que el personal relacionado anteriormente es el que se encuentra actualmente disponible en la Oficina de Informática del IDEAM, varios

	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:65 de 68

servicios no cuentan con la definición de personal especialista suplente, esto representa un riesgo al momento de realizar la activación del DRP.

6.3.4. Árbol de llamadas



Figura

13. Árbol de llamadas

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:66 de 68

El árbol de llamadas representa la cadena de llamadas que se debe seguir y cumplir para comunicar a los integrantes del DRP la activación del plan, esta se ejecuta después de la declaración de contingencia realizada por el Gerente del DRP.

El árbol de llamadas está dividido en equipos o grupos para permitir llamar a los integrantes requeridos según el tipo de contingencia que se haya declarado.

Cada nivel está encargado de llamar al nivel inferior según la estructura del plan y el llamado a cada integrante debe ser verificado por el nivel superior. Jefe de la Oficina de Informática y el Líder DRP son los encargados de efectuar las llamadas y son los responsables de la intercomunicación con el primer nivel de llamadas.

El llamado a los integrantes del plan se debe realizar siguiendo el procedimiento de comunicación necesario y utilizando los medios de comunicación disponibles para realizarlo.


A continuación, se relacionan algunos medios de comunicación a ser utilizados al momento de un evento adverso, así como su prioridad en usabilidad:

MEDIOS DE COMUNICACIÓN		
Prioridad	Tipos de Medio	Descripción
1	Persona a Persona	La forma más fácil y efectiva de comunicar el evento es hacerlo persona a persona. Este medio permite ser más explícito y detallar lo sucedido con el evento. La comunicación depende de factores socio-ambientales y/o factores de riesgo (catástrofes) que afecten este tipo de comunicación.
2	Telefonía Celular	La comunicación telefónica es un medio facilitador para acortar distancias y tener una conversación interpersonal. Con él se puede al igual que en la comunicación persona a persona ser más explícito y ahondar dentro de la comunicación del evento.

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	PLAN DE RECUPERACIÓN DE DESASTRES IDEAM	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página:67 de 68




3	Mensajería Instantánea – Link (requiere Computador Personal e internet WhatsApp (requiere Smartphone e internet)	La mensajería instantánea como un tipo de correo permite interactuar de forma más rápida y efectiva entre una o varias personas, depende de los medios y restricciones impuestos por el Instituto y de la disposición de los intercomunicadores.
4	Correo Electrónico	El correo electrónico se ha establecido como un medio efectivo para comunicarse a cualquier distancia y en el menor tiempo. Este tipo de comunicación depende del grado de consulta de los intercomunicadores.

Tabla 7 – Medios de comunicación

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	<p align="center">PLAN DE RECUPERACIÓN DE DESASTRES IDEAM</p>	Código: E-SGI-SI-M004
		Versión: 007
		Fecha: 20/09/2021
		Página: 58 de 58

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
001	01/06/2017	Creación del documento.
002	21/06/2017	Actualización del documento.
003	20/06/2018	Actualización documento para SGI
004	12/08/2019	Actualización documento para SGI
005	06/07/2020	Actualización documento para SGI
006	10/12/2020	Actualización documento para SGI
007	22/11/2021	Actualización documento para SGI

ELABORÓ:	REVISÓ:	APROBÓ:
 <p>Adilio Pardo Hernández Líder CDA</p>	 <p>Andrés Felipe Arias Coordinador Grupo de Tecnología</p>	 <p>Alicia Barón Leguizamón Jefe OI</p>