

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 1 de 53

INDICE

INTRODUCCIÓN	4
1. TERMINOS Y DEFINICIONES	5
2. OBJETIVO	12
3. ALCANCE.....	12
4. GENERALIDADES DEL PLAN DE RECUPERACION DESASTRES - DRP	15
4.1. ESTRATEGIA GENERAL DE RECUPERACIÓN.....	16
4.2. ESTRATEGIA DE ACCIÓN	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	19
4.3.2. PÉRDIDA TOTAL O PARCIAL DE LOS SERVICIOS PACTADOS DENTRO DEL ALCANCE DEL PLAN	20
4.3.3. INTERRUPCIONES AL NEGOCIO O INCIDENTES QUE PODRÍAN AFECTAR EL CUMPLIMIENTO DE LAS LABORES DE LOS FUNCIONARIOS.....	23
4.4. CENTRO DE DATOS ALTERNO.....	23
4.5. CANALES DE COMUNICACIONES	25
4.5.1. CONECTIVIDAD	26
4.6. CENTRO DE OPERACIONES ALTERNO - COA	26
4.6.1. CENTRO DE MONITOREO	27
5. PROCEDIMIENTO DE NOTIFICACIÓN, ACTIVACIÓN Y RETORNO	28
5.1 PROCEDIMIENTO DE NOTIFICACIÓN	30
5.2 DETECCIÓN DEL EVENTO	33
5.4 DEFINICIÓN DE RECURSOS	34
5.4.1 COMITÉ DE EMERGENCIAS.....	35
5.4.2 COMITÉ DE RESPONSABLE DE ACTIVACIÓN DEL DRP	36
5.4.3 EQUIPO DE RECUPERACIÓN DRP.....	39
5.4.3.1 RESPONSABLES OFICINA DE INFORMÁTICA IDEAM PARA LA ACTIVACIÓN DE DRP	46
5.4.4 ÁRBOL DE LLAMADAS	51

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	<p>MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES</p>	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 2 de 53

INDICE DE TABLAS

Tabla 1 - Alcance DRP - IDEAM 13

Tabla 2 - Clasificación de eventos 29

Tabla 3 – Equipo evaluador de daños 36

Tabla 4 – Comité responsable de activación del Plan de recuperación de desastres DRP 38

Tabla 5 – Coordinador DRP – Líder DRP IDEAM 38

Tabla 6 – Equipo recuperación contingencia..... 39

Tabla 7 – Medios de comunicación 52

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:3 de 53

INDICE DE FIGURAS

Figura 1 - RTO - RPO	15
Figura 2 - Alternativas de recuperación	16
Figura 3 - Clasificación escenarios de desastre	19
Figura 4 – Distancia lineal del centro de datos alterno	24
Figura 5 - Diagrama general de conectividad	25
Figura 5 - Centro de monitoreo ROC – CDA	28
Figura 6 - Fases de activación	29
Figura 7 - Procedimiento de notificación.....	31
Figura 8 - Proceso de activación gestión del plan	32
Figura 10 – Definición de recursos	35
Figura 9 – Activación DRP IDEAM	37
Figura 10 – Responsable activación servicios servidores BART – LISTAS – EFA.....	47
Figura 11 – Responsable activación servicios servidores ZASCA – PORTAL SIAC – PRUEBAS JBOSS – AMAKANA – ORFEO - QUEMES.....	48
Figura 12 – Responsable activación servicios servidores TAUSA – BAGUE.	48
Figura 13 – Responsable activación servicios servidores HYDRAS 3.....	49
Figura 14 – Responsable activación servicios servidores SUA – NOREIMAKO – BORFEO.....	49
Figura 15 – Responsable activación servicios servidores FURACHOGUA.	50
Figura 16 – Responsable activación servicios servidores COMUNICACIONES.	50

 IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:4 de 53

INTRODUCCIÓN

La implementación de un proceso de preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por pérdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio) se deberían ser someter a un análisis del impacto del negocio (BIA). Se deben desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales.

La correcta implementación de la gestión de la continuidad del negocio disminuirá el impacto al presentarse incidentes disruptivos y en caso de producirse, la entidad estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de ese incidente.

 <p>Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:5 de 53

1. TERMINOS Y DEFINICIONES

El ítem de términos y definiciones se elabora para lograr entendimiento de forma clara y unificación de la terminología, definiciones y abreviaturas que tengan lugar en el presente documento.

Actividades prioritarias: Actividades a las que se les debe dar prioridad después de un incidente a 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 22301:2012, Capítulo 3, Términos y definiciones, numeral 3.42].

Amenaza: Percepción de la posibilidad de ocurrencia de algún hecho dañino sobre los recursos involucrados en el desarrollo de un proceso (humano, financiero, medio ambiente, información e imagen corporativa), representando pérdidas para el sistema o la organización. (International Glossary of Resilience).

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 las llamadas 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.

 <p> IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales </p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:6 de 53

[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): 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.

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 22301:2012, 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 catastrófico que causa daño o pérdida no aceptable a una organización.

 <p> IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales </p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:7 de 53

- 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]

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.

 <p> IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales </p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:8 de 53

[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 22301:2012, Capítulo 3, Términos y definiciones, numeral 3.17].

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Norma ISO 22301:2012, Capítulo 3, Términos y definiciones, numeral 3.51].

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].

Impacto: Efecto, aceptable o no, que un evento tiene en una organización. Los tipos de impactos al negocio son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos, dependiendo del sector.

[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.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:9 de 53

[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, Capitulo 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 claramente 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): 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”, capitulo 2, numeral 2.6]

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 10 de 53

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.

[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 gente 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]

 <p> IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales </p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 11 de 53

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]

 <p>Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 12 de 53

2. OBJETIVO

Describir las acciones necesarias a ejecutar 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 las aplicaciones críticas bajo la modalidad de hosting cloud con el fin de asegurar la continuidad de la operación ante un desastre o contingencia e iniciar con el correcto funcionamiento de los servicios identificados como críticos por la entidad.

3. ALCANCE

La necesidad de desarrollar un plan de contingencia está relacionada con el impacto potencial que provoca la interrupción parcial o total de los servicios de aplicaciones críticas de la información de la entidad, sobre el normal desarrollo de las actividades; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos. Buscando mantener funcionando a los sistemas de misión críticos y a los servicios esenciales que la entidad ofrece.

Como parte de la construcción del presente documento se incluye el desarrollo de los ejercicios DRP, fundamental en el procedimiento paso a paso para la activación y recuperación de los servicios contemplados en el presente alcance.

El documento preliminar contempla los procesos a seguir durante las pruebas y en caso de un evento adverso en que se requiera la activación del plan.

Servidores que hacen parte integral del DRP:

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 13 de 53

MAQUINA	FUNCIÓN O SERVICIO ASOCIADO	RPO	RTO
BART	Servidor FTP	2 Horas	2 Horas
ZASCA	JBOSS EAP - 6,2,1	25 min	25 min
QUEMES	JBOSS EAP - 6,2,1	1 Hora	1 Hora
TAUSA	Servidor WEB	25 min	25 min
HYDRAS	Sistema de recepción de datos de estaciones automáticas	25 min	25 min
SUA	BD Oracle Enterprise 11GR2	25 min	25 min
CONA		2 Horas	2 Horas
FURACHOGUA	Directorio activo	2 Horas	2 Horas
MAIL	Servidor de correo	2 Horas	2 Horas
NOREIMAKO	N/A	2 Horas	2 Horas
PRUEBAS JBOSS	N/A	2 Horas	2 Horas
AMAKANA	N/A	2 Horas	2 Horas
ORFEO	N/A	3 Horas	3 Horas
BORFEO	POSGRESS SQL	2 Horas	2 Horas
LISTAS	Grupos de correo	2 Horas	2 Horas
EFA	Seguridad de correo	2 Horas	2 Horas
BAGUE		25 min	25 min

Se anexa al presente alcance la maquina BAGUE y CONA en reemplazo de los servidores CAGUI Y PORTAL SIAC.

Tabla 1 - Alcance DRP - IDEAM

- Servicios de conectividad para replicación del Data center:

Comunicaciones WAN	N/A	< 30 Min	-
--------------------	-----	----------	---

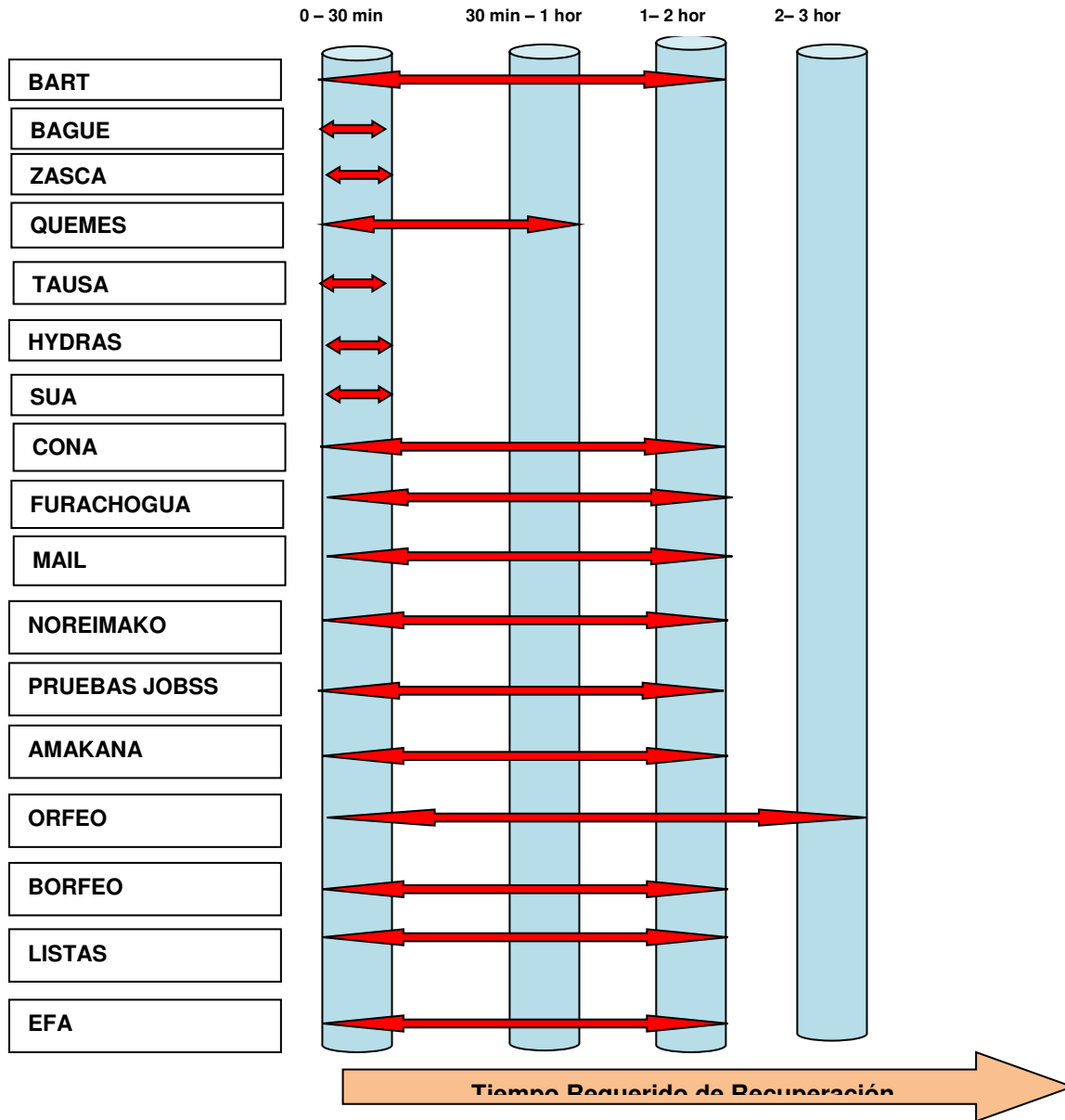


Figura 3. Tiempo Requerido para Recuperación de Sistemas

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

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 15 de 53

4. GENERALIDADES DEL PLAN DE RECUPERACION DESASTRES - DRP

De acuerdo con la descripción del alcance el Instituto de hidrología, meteorología y estudios ambientales - IDEAM definió unos tiempos de RTO y RPO para cada una de las máquinas, luego de realizar un análisis de criticidad de las mismas, mediante:

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, es especial, los procesos de carácter sempiterno.

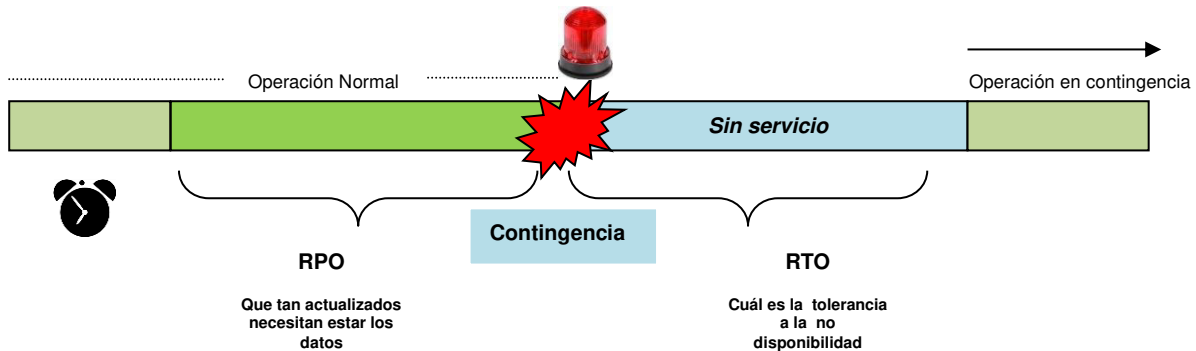


Figura 1 - RTO - RPO

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 16 de 53

4.1. Estrategia general de recuperación

Este plan está basado en el hecho de que por alguna situación crítica interna o externa, no haya acceso a los servicios de cómputo centrales o las instalaciones donde se ubica el centro de cómputo o son inaccesibles por completo por un período inaceptable de tiempo.

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

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

Este plan solo podrá ser activado únicamente cuando el IDEAM lo apruebe.

Con base en los resultados obtenidos por Instituto de hidrología, meteorología y estudios ambientales - IDEAM en donde se determinó contar con un Centro de Datos Alterno se planteó y estableció la estrategia de recuperación la cual se conforma de elementos tales como la ubicación del centro de datos alternativo, la preparación y puesta en funcionamiento de un Centro de Operaciones Alterno (COA) y de un Centro de Monitoreo.

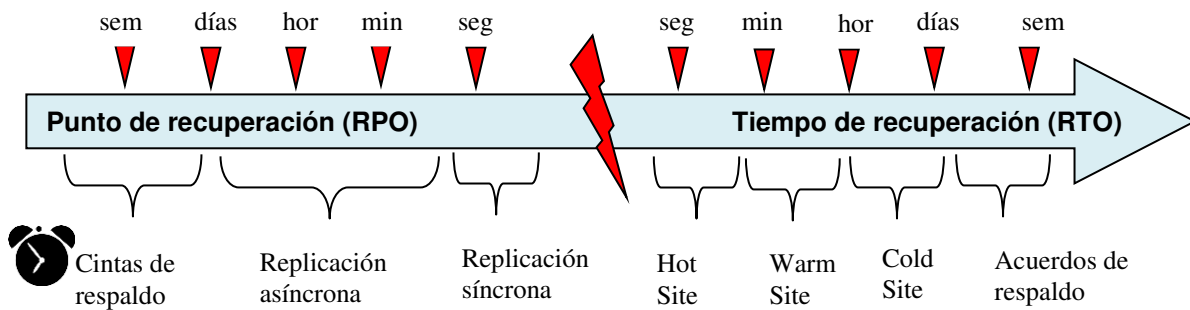


Figura 2 - Alternativas de recuperación

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:17 de 53

4.2. Estrategia de acción

Las estrategias y planes de acción considerados para la recuperación 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 las todas aplicaciones críticas de la entidad, las cuales se definieron como:

1. Servidor FTP
2. JBOSS EAP
3. Servidor WEB
4. Sistema de recepción de datos de estaciones automáticas
5. BD Oracle Enterprise 11 GR2
6. Servidor Portal SIAC y aplicativo SISAIRE Moodle
7. Servidor de Correo
8. Directorio Activo
9. POSTGRESS SQL
10. Grupos de Correo
11. Seguridad de Correo

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 tecnología de información y 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

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 18 de 53

fallas, activando los procedimientos de atención de problemas utilizados día a día por el personal del IDEAM.

Incidencia Mayor:

De presentarse una incidencia mayor en los equipos y sistemas del centro de cómputo principal que impida la función general 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 Plan DRP.

Incidencia Catastrófica:

Si se presenta un incidente que provoque una contingencia catastrófica evidente y que por consiguiente interrumpa las operaciones del IDEAM en sus instalaciones ubicadas en el Calle 25D # 96B - 70 de la ciudad de Bogotá. Siendo importante recalcar que la declaración de contingencia es responsabilidad del IDEAM.

4.3. Clasificación de los escenarios de desastre

En esta sección se incluye una clasificación de los posibles escenarios de desastre que pueden Ocurrir.

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 19 de 53

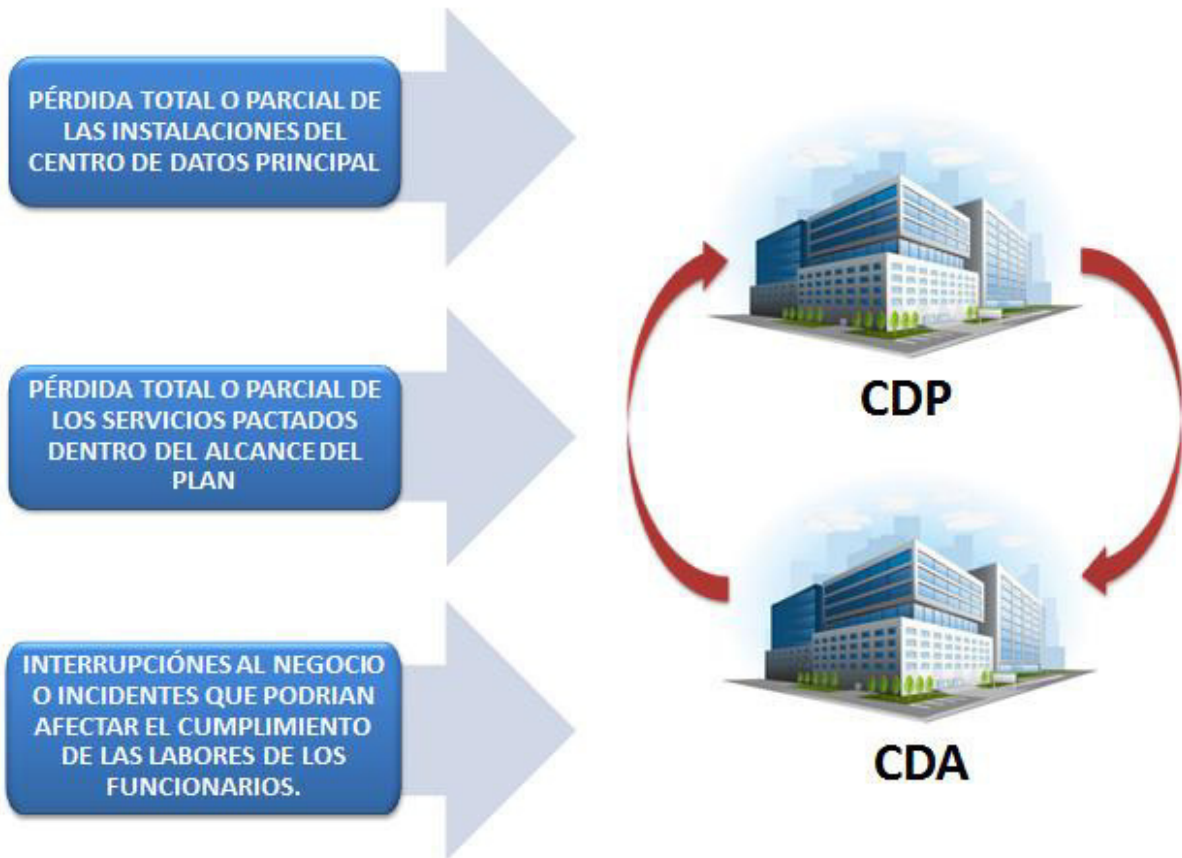


Figura 3 - Clasificación escenarios de desastre

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 perpetrados por terroristas y/o grupos armados ilegales.
- Hostilidades u operaciones bélicas ya sea o no declarada una guerra.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:20 de 53

- 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.

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

La pérdida total o parcial de los servicios pactados dentro del alcance del plan 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.
- 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.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:21 de 53

- 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, 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 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.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:22 de 53

- 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 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.

 <p>Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 23 de 53

- 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.
- 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

4.4. Centro de datos alternativo

El sitio alternativo para el Instituto de Hidrología, Meteorología y Estudios ambientales - IDEAM está ubicado en Colombia IVX Level 3 ubicado en la ciudad de Bogotá Calle 185 # 45-03.

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 24 de 53

Este Data Center tiene clasificación TIER III de acuerdo con las especificaciones requeridas por la norma NFPA75. 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.

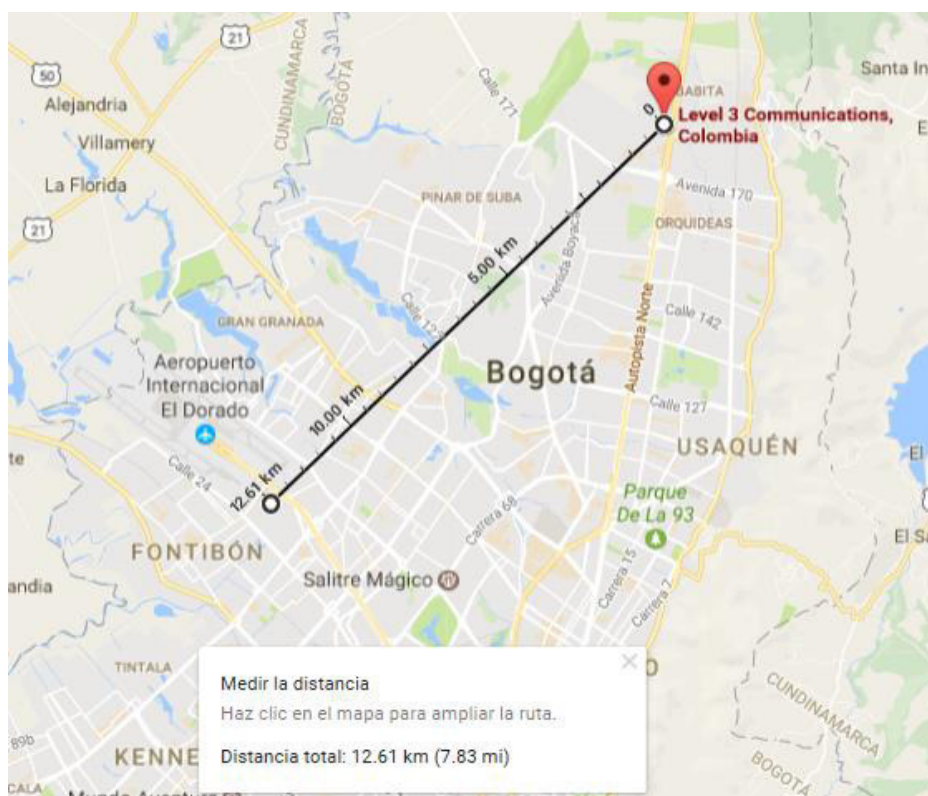


Figura 4 – Distancia lineal del centro de datos alternativo

La infraestructura del centro de datos provista por Level3 para el alojamiento de los componentes de Hardware que hacen parte de la solución para el Instituto de Hidrología, Meteorología y Estudios ambientales - IDEAM, es la siguiente:

- Suministrar toda la infraestructura tecnológica de servidores.
- Suministrar mínimo 6 TB de almacenamiento.
- Monitoreo y administración en contingencia.

- Replicación en línea y dos canales de datos L2L de 20 Mbps para redundancia
- Solo se contempla la implementación de los servidores replicando, mas no pruebas reales para la fase de implementación.

4.5. Canales de comunicaciones

Se dispondrán de los siguientes canales de comunicación:

Enlace de replicación de 20 Mbps con redundancia entre Instituto de Hidrología, Meteorología y Estudios ambientales - IDEAM y Level 3 modalidad Lan-to-Lan o Lan extendida, asegurando que los mismos segmentos de red de sitio principal se puedan usar en DataCenter de contingencia.

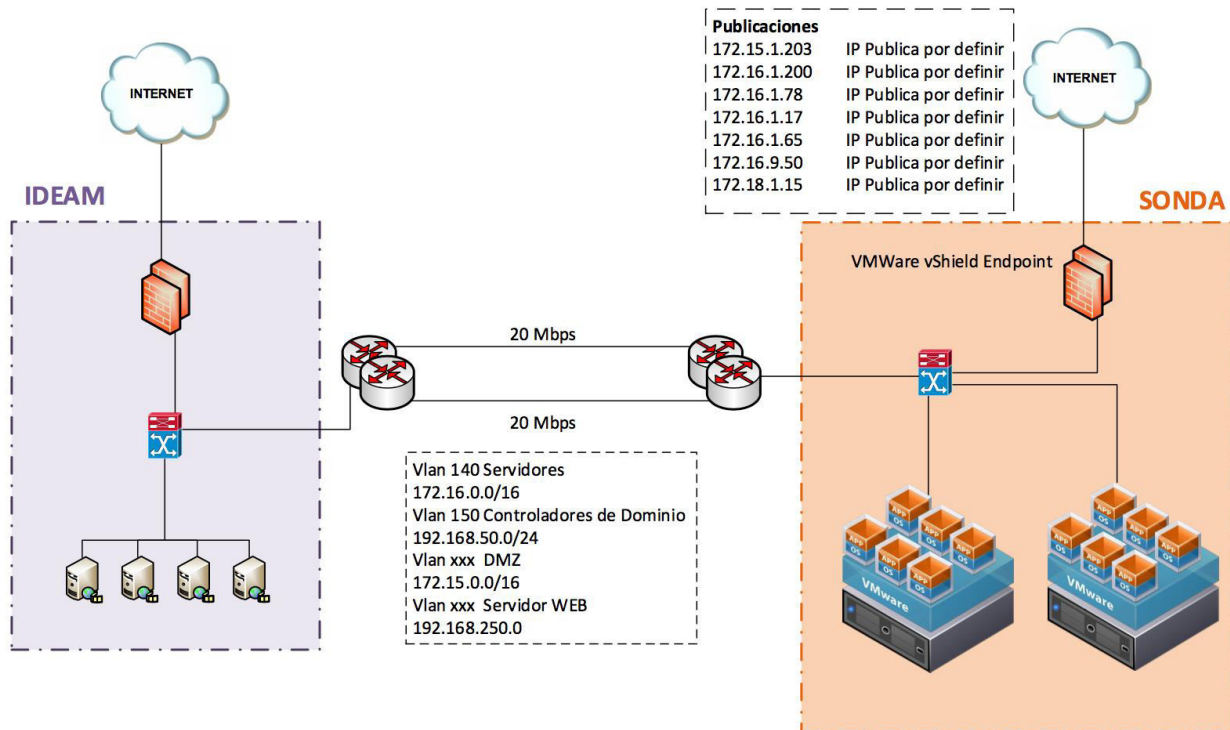


Figura 5 - Diagrama general de conectividad

 <p>Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:26 de 53

4.5.1. Conectividad

Los diferentes componentes físicos instalados en los racks, se encuentran conectados a través de los switches FC que hacen parte de la solución, permitiendo la gestión y comunicación adecuada. Toda la conectividad de management se centralizará en el Switch Management, generando separación física de tráfico y garantizando optimizar el tráfico productivo.

4.6. Centro de operaciones alternativo - COA

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.

SONDA DE COLOMBIA S.A. dispuso en sus instalaciones ubicadas en 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.

A continuación, se enuncian las principales características y servicios que presta el Centro de Operaciones Alterno (COA):

- Conexión con el Instituto de Hidrología, Meteorología y Estudios ambientales - IDEAM y con el Centro de Datos Alterno (CDA).

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:27 de 53

- 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

4.6.1. Centro de monitoreo

El Centro de Monitoreo se encuentra ubicado en las instalaciones de 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.
- Notificación en caso de alarmas o de alteraciones en los sistemas.

A continuación, se muestran las fotografías del Centro de Monitoreo:

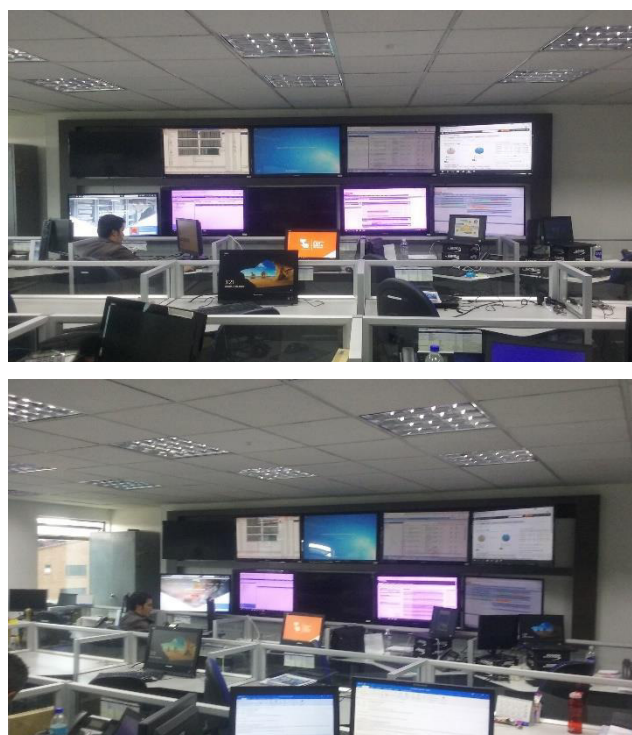


Figura 6 - Centro de monitoreo ROC – CDA

5. PROCEDIMIENTO DE NOTIFICACIÓN, ACTIVACIÓN Y RETORNO

Como parte de las estrategias inmediatas ante una posible crisis, se contemplan las tareas que deben efectuarse lo más rápido posible, después de que se presente el incidente, para reducir posibles impactos. En muchos casos, estos procedimientos contemplan la comunicación inicial con clientes y otros contactos externos, así como también direccionamiento de las estrategias de recuperación de las funciones de negocio más críticas.

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

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 29 de 53

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 de 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 de contingencia

Tabla 2 - Clasificación de eventos



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

 <p> IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales </p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:30 de 53

6. Activar 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
14. Regreso a 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

5.1 Procedimiento de notificación

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

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:31 de 53

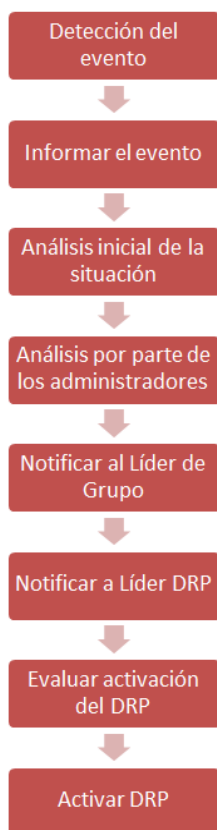


Figura 8 - Procedimiento de notificación

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. Es importante tener en cuenta que el procedimiento de notificación debe estar ligado 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:

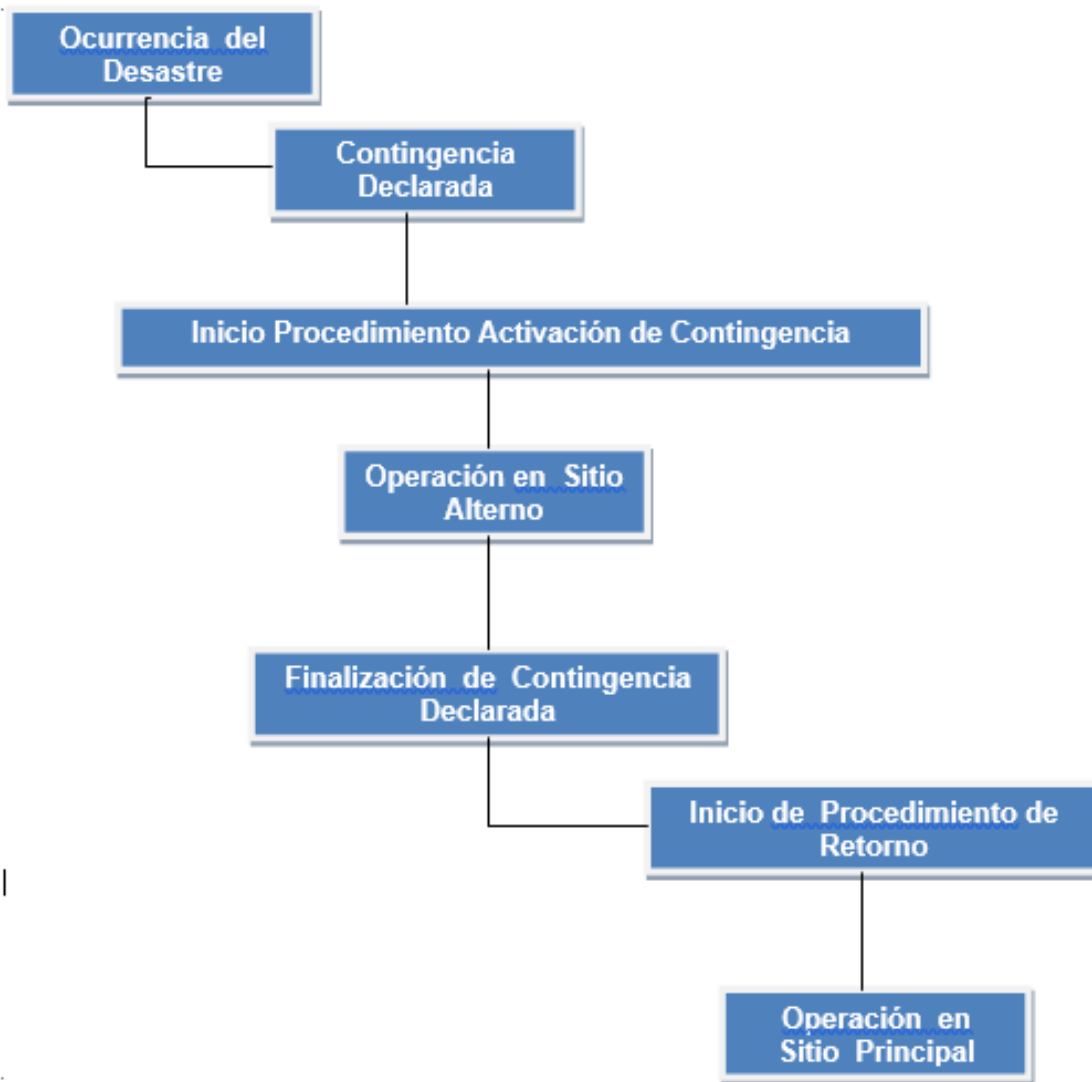


Figura 9 - Proceso de activación gestión del plan

El procedimiento de entrada a contingencia describe las actividades requeridas para la activación de los diferentes servicios que se encuentran respaldados en el centro de datos, cuando se activa el plan.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:33 de 53

5.2 Detección del evento

Los eventos que afectan la continuidad de las operaciones de los servicios y maquinas identificadas como críticas por el IDEAM, podrán ser reportados una vez identificados con el fin de iniciar a trabajar en una pronta atención y por ende 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:

1. Correo electrónico.
2. Portal institucional.
3. Aplicación móvil.
4. Gestor documental.
5. Portal SIAC.
6. Recepción de datos de estaciones automáticas.
7. Registro único ambiental – RUAS.
8. Pronósticos y alertas.
9. Subsistema hidrometeorológico – SSHM.
10. Sistema nacional de inventario forestal – SNIF.

Los anteriores servicios descritos, fueron definidos por la entidad como críticos, y en ellos se relacionan la totalidad de las maquinas que se encuentran en el alcance para su correcto funcionamiento.

 <p> IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales </p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:34 de 53

5.4 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.
- **Comité responsable de activación DRP:** se encuentra conformado por los responsables de la activación del plan de recuperación de desastres DRP.
- **Equipo de Recuperación 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 las maquinas contempladas dentro del alcance.

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:35 de 53

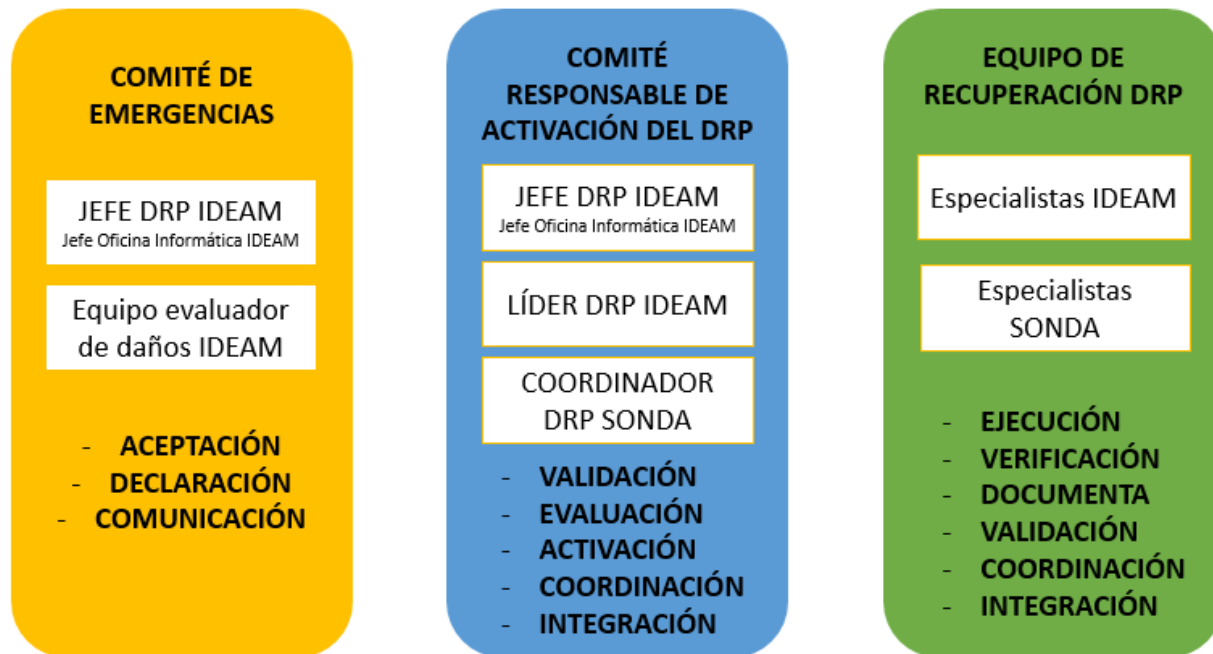


Figura 10 – Definición de recursos

5.4.1 Comité de emergencias

Realiza la evaluación de los daños y la magnitud del suceso, trabaja de la mano con el equipo de DRP, y su principal función es salvaguardar las vidas humanas, este comité es informado lo antes posible de cualquier incidencia para la toma de decisiones efectivas para la superación de eventos y dar alcance a la comunicación oportuna al jefe de DRP para iniciar a 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 DRP si se debe declarar una contingencia. La intervención de este grupo durante una situación de

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:36 de 53

contingencia está determinada por el tipo de daño, siendo necesaria su gestión en la ocurrencia de algún evento.

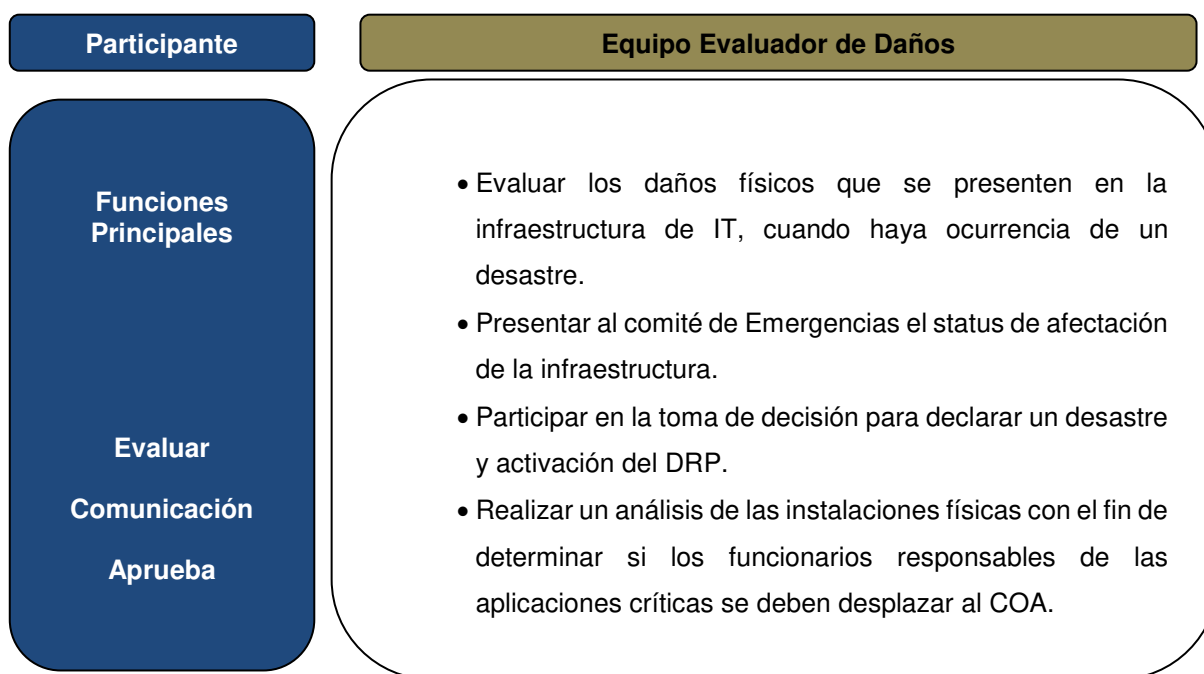


Tabla 3 – Equipo evaluador de daños

5.4.2 Comité de responsable 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 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

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 37 de 53

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, si existe, y alineadas con el Sistema de Gestión de Continuidad de Negocio, si existe.
- 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.

RESPONSABLES DE ACTIVACIÓN DE DRP IDEAM	
OFICINA DE INFORMÁTICA IDEAM	
	<p><u>PRINCIPAL</u> Ing. Leonardo Cardenas lcardenas@ideam.gov.co Celular: 3153881599</p>
	<p><u>SUPLENTE</u> Ing. Francisco Bernal fbernal@ideam.gov.co Celular: 3002130286</p>

Figura 11 – Activación DRP IDEAM

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:38 de 53

Participante	Comité responsable de activación del DRP
Funciones Principales Aceptación Comunicación Declaración	<ul style="list-style-type: none"> Mantener comunicado al enlace ejecutivo del desarrollo del plan de contingencia Determinar conjuntamente con el Coordinador CDA el Plan de Respuesta inmediato y el Plan de Acción de los Equipos DRP Monitorear la ejecución del Plan DRP hasta el regreso a modo normal de operación. Gestionar la disponibilidad de los recursos técnicos mínimos para la activación de los servicios v maquinas del DRP

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

En conjunto como parte del equipo de trabajo se encuentran:

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

Participante	Coordinador DRP – Líder DRP IDEAM
Funciones Principales Activar Comunicación Documentar	<ul style="list-style-type: none"> Garantizar la operatividad del Plan de Recuperación de Desastres. Planear y coordinar las pruebas del Plan de Contingencias en conjunto con el líder DRP IDEAM. Identificar los responsables para la administración, mantenimiento y ejecución de pruebas de la contingencia en conjunto con el líder DRP IDEAM. Ejecutar las actividades de Divulgación y Capacitación del Plan de Contingencias. Evaluar el incidente reportado y estimar el impacto en la operación de los servicios. Proporcionar toda la información necesaria al comité directivo de contingencias para que se declare la situación de contingencia. Notificar y alertar a los Equipos de Recuperación correspondientes. Registrar los eventos y acciones desarrolladas durante el estado de Contingencia. Coordinar todas las actividades que se requieran realizar en el Centro de Datos Alterno de común acuerdo con el personal técnico de la Entidad y con el Centro de Datos Principal. Brindar servicios de calidad en los tiempos esperados (RPO y RTO) y garantizar la continuidad del servicio. Definir, implementar y documentar nuevos procedimientos y acciones de mejora. Consolidar los informes de gestión, estadísticas y demás información de los servicios implementados que le competan Supervisar todo cambio realizado en las instalaciones de la Infraestructura Tecnológica.

Tabla 5 – Coordinador DRP – Líder DRP IDEAM

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 39 de 53

5.4.3 Equipo de recuperación DRP

Está compuesto por: Equipo evaluador de daños (IDEAM), Coordinador 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.

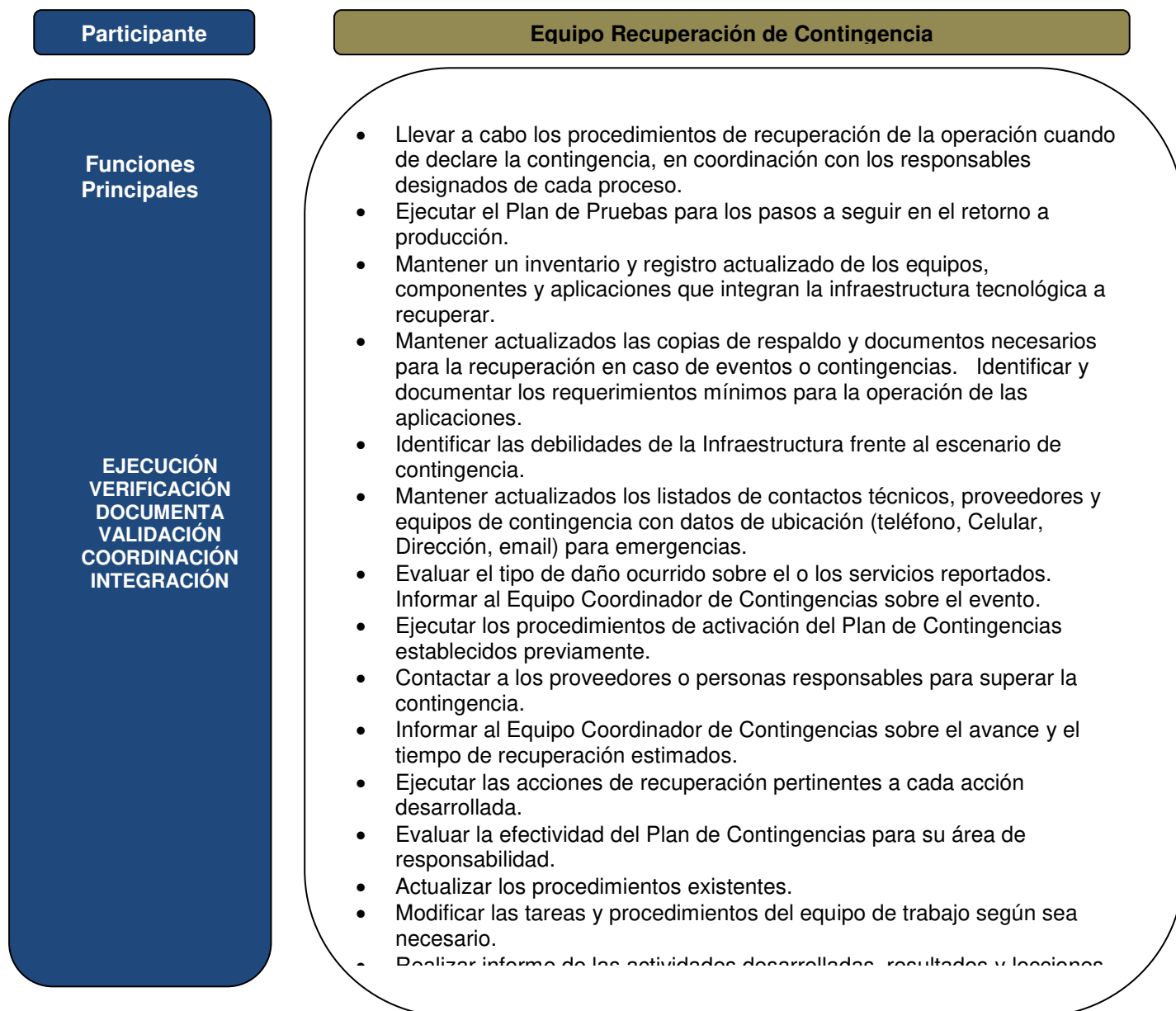


Tabla 6 – Equipo recuperación contingencia

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:40 de 53

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 Cómputo 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.
- 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.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:41 de 53

- 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 Cómputo 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 Computo Principal y del Centro Computo 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 Computo Alterno.
- Asistir la recuperación de la plataforma en el Centro Computo Principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:42 de 53

- Restaurar el servicio en el Centro Computo Principal.
- Alistar el Centro Computo 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 Cómputo 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 Cómputo 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 actualización (toda mejora, cambio y demás debe estar documentada y validar que en el sitio alternativo 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.

 <p>Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:43 de 53

- 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 Computo Alterno.
- Asistir la recuperación de la plataforma en el Centro Computo Principal.
- Documentar fallas y su solución.
- Proveer soporte técnico según requerimientos del momento.
- Restaurar el servicio en el Centro Computo Principal.
- Alistar el Centro Computo 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 TIC en un Centro de Cómputo 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 o desde el COA Centro de Operación Alterna.

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 CCP y del CCA, en HW y SW.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:44 de 53

- 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 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.

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 Cómputo Alterno.

- Mantener actualizados los procedimientos de instalación y arranque de las aplicaciones.
- 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 CCP y del CCA, en HW y SW sean apropiadas para el correcto funcionamiento de las aplicaciones.
- Velar porque las versiones de las aplicaciones disponibles en el CCP y el CCA 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.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:45 de 53

- 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 CCA.
- Proveer soporte técnico según requerimientos del momento.
- Documentar fallas y su solución.
- Asistir la recuperación de las aplicaciones en el CCP.
- Restaurar el servicio en el CCP.
- Alistar el CCA 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 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 auditorias)
- 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.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:46 de 53

- 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 IDEAM
- Soporte Nivel I y II de la Mesa de Ayuda
- Operadores de Centros de Datos Alterno

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.

5.4.3.1 Responsables oficina de informática IDEAM para la activación de DRP

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

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 47 de 53

corresponda:

RESPONSABLES OFICINA DE INFORMÁTICA PARA LA ACTIVACIÓN DE LOS SERVICIOS DRP IDEAM	
PRINCIPAL MAIL BART LISTAS EFA	 Ing. Andres Felipe Arias afarias@ideam.gov.co Celular: 3122890963
SUPLENTE MAIL BART LISTAS EFA	 Ing. Francisco Bernal fjbernal@ideam.gov.co Celular: 3002130286

Figura 12 – Responsable activación servicios servidores BART – LISTAS – EFA - MAIL.

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:48 de 53



RESPONSABLES OFICINA DE INFORMÁTICA PARA LA ACTIVACIÓN DE LOS SERVICIOS DRP IDEAM	
PRINCIPAL ZASCA PRUEBAS JBOSS AMAKANA ORFEO QUEMES	 Ing. Sergio Moreno samoreno@ideam.gov.co Celular: 3174281269
SUPLENTE ZASCA PRUEBAS JBOSS AMAKANA ORFEO QUEMES	 NO DEFINIDO POR IDEAM

Figura 13 – Responsable activación servicios servidores ZASCA – PRUEBAS JBOSS – AMAKANA – ORFEO - QUEMES.

RESPONSABLES OFICINA DE INFORMÁTICA PARA LA ACTIVACIÓN DE LOS SERVICIOS DRP IDEAM	
PRINCIPAL TAUSA BAGUE	 Ing. David Perez dfperez@ideam.gov.co Celular: 3504181074
SUPLENTE TAUSA BAGUE	 NO DEFINIDO POR IDEAM

Figura 14 – Responsable activación servicios servidores TAUSA – BAGUE.

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 49 de 53



RESPONSABLES OFICINA DE INFORMÁTICA PARA LA ACTIVACIÓN DE LOS SERVICIOS DRP IDEAM	
PRINCIPAL HYDRAS 3	 Ing. Carlos Pedraza cpedraza@ideam.gov.co Celular: 3133862571
SUPLENTE HYDRAS 3	 NO DEFINIDO POR IDEAM

Figura 15 – Responsable activación servicios servidores HYDRAS 3.

RESPONSABLES OFICINA DE INFORMÁTICA PARA LA ACTIVACIÓN DE LOS SERVICIOS DRP IDEAM	
PRINCIPAL SUA NOREIMAKO BORFEO	 Ing. Jose Francisco Blanco jfblanco@ideam.gov.co Celular: 3006773280
SUPLENTE SUA NOREIMAKO BORFEO	 NO DEFINIDO POR IDEAM

Figura 16 – Responsable activación servicios servidores SUA – NOREIMAKO – BORFEO.

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 50 de 53



RESPONSABLES OFICINA DE INFORMÁTICA PARA LA ACTIVACIÓN DE LOS SERVICIOS DRP IDEAM	
PRINCIPAL FURACHOGUA	 Ing. Javier Hernán García jhgarciag@ideam.gov.co Teléfono: 352 7160 Ext. 1346 Celular: 3214656127
SUPLENTE FURACHOGUA	 NO DEFINIDO POR IDEAM

Figura 17 – Responsable activación servicios servidores FURACHOGUA.

RESPONSABLES OFICINA DE INFORMÁTICA PARA LA ACTIVACIÓN DE LOS SERVICIOS DRP IDEAM	
PRINCIPAL COMUNICACIONES	 Ing. Jeffer Bohórquez jbohorquez@ideam.gov.co Celular: 3195023273
SUPLENTE COMUNICACIONES	 NO DEFINIDO POR IDEAM

Figura 18 – Responsable activación servicios servidores COMUNICACIONES.

 <p>IDEAM Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página:51 de 53

NOTA: Es importante destacar que el personal relacionado anteriormente es el que se encuentra actualmente disponible en la oficina de informática del IDEAM, actualmente no se cuenta con la definición de personal suplente por cada uno de los ingenieros que se encuentran a cargo de las maquinas críticas para la entidad, por lo que representa un riesgo al momento de realizar la activación del plan de recuperación de desastres DRP y falte algún ingeniero (personal critico).

5.4.4 Árbol de llamadas

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 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 su 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:

 <p>Instituto de Hidrología, Meteorología y Estudios Ambientales</p>	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 52 de 53

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.
3	Telefonía Fija	
4	Skype - Viber (requiere Smartphone e internet)	
5	Radios de dos vías (walkie talkie)	Es un medio de comunicación predilecto en áreas de seguridad y para las Brigadas de Emergencias. Tiene restricciones de distancia y de uso.
6	Máquinas de FAX	Permite enviar documentos de manera rápida. Dentro de sus debilidades se encuentra que no hay un acuse de recibo del receptor directo del mensaje.
7	Mensajería Instantánea – Link (requiere Computador Personal e internet Whats Up (requiere Smartphone e internet)	La mensajería instantánea como un tipo de correo permite interactuar más rápida y efectivamente entre una o varias personas. Depende de los medios y restricciones impuestos por la corporación y de la disposición de los intercomunicadores.
8	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.
9	Correo Físico Certificado	El correo certificado permite enviar documentos de forma más segura a cualquier destinatario. Este tipo de medio ha evolucionado y hoy en día permite realizar un seguimiento vía Internet a los paquetes y/o documentos enviados.
10	Correo Físico Normal	El correo físico normal, es uno de los medios más antiguos y que sigue teniendo vigencia. Este depende de los medios de transporte y las distancias para asegurar una buena efectividad.
11	Redes sociales (Facebook, Twitter y Google +)	Para ubicar a las personas de los diferentes equipos del DRP.

Tabla 7 – Medios de comunicación

	MANUAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	Código: E-SGI-SI-M004
		Versión: 03
		Fecha: 20/06/2018
		Página: 53 de 53

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
01	01/06/2017	Creación del documento.
02	21/06/2017	Actualización del documento.
03	20/06/2018	Actualización documento para SGI

ELABORÓ: Leidy Puentes Hernández Coordinador DRP	REVISÓ: Luis Alejandro Pinilla Peralta Líder DRP	APROBÓ: Leonardo Cárdenas Chitiva Jefe Oficina Informática
--	--	--