	DIRECTIVA	Código: OPIA 22
		Fecha: 12 SET. 2016
		Página 1 de 2

Bogotá D.C., 12 SET. 2016

PARA: FUNCIONARIO DEL PROCESO DE GESTIÓN TECNOLÓGICA

DE: JEFE OFICINA ASESORA DE PLANEACIÓN, REPRESENTANTE DE LA ALTA DIRECCIÓN PARA EL SISTEMA INTEGRADO DE GESTIÓN DE MIGRACIÓN COLOMBIA

ASUNTO: ADOPTAR LA GUÍA PARA LA ADMINISTRACIÓN DE USUARIOS DEL DIRECTORIO ACTIVO - AGTG.10 (VERSIÓN 1) Y LA GUÍA PARA RECUPERACIÓN DE DESASTRES - AGTF.09 (VERSION 3).

1. VIGENCIA

A partir de la fecha de su expedición.

2. FINALIDAD

Establecer una guía para la administración de usuarios del directorio activo, la cual servirá como fuente de consulta para los funcionarios del Proceso de Gestión Tecnológica.

Ajustar la Guía para recuperación de desastres en la Unidad Administrativa Especial de Migración Colombia.

3. ALCANCE


Aplica a todos los funcionarios del Proceso de Gestión Tecnológica de la Unidad Administrativa Especial Migración Colombia.

Aplica a todos los servidores públicos de la Unidad Administrativa Especial Migración Colombia.

4. MARCO LEGAL

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del

f

	DIRECTIVA	Código: OPDA 22
		Fecha: 12 SET. 2016
		Página 2 de 2

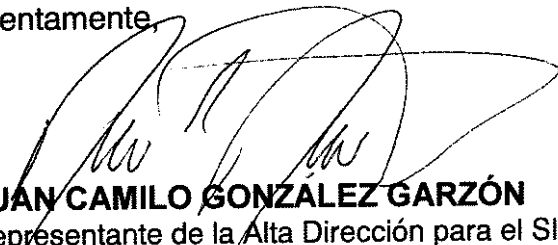
hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- Ley 734 de 2002. Por la cual se expide el Código Disciplinario Único.
- Decreto 2573 de 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Directiva 17 de 2014. Lineamientos de Política para la Seguridad de la Información.
- Directiva 54 de 2013. Política Sistema de Gestión de la Seguridad de la Información SGSI.

5. INSTRUCCIONES





- Adoptar la primera versión de la **Guía para la Administración de usuarios del directorio activo - AGTG.21**
- Adoptar la tercera versión de la **Guía para Recuperación de desastres - AGTG.09**
- Estos documentos hacen parte integral de esta Directiva y del Manual de Procedimientos del Proceso de Gestión Tecnológica y son de obligatorio cumplimiento.
- La Oficina de Tecnología de la Información debe socializar e implementar los presentes documentos del manual y deben identificar las respectivas oportunidades de mejora, así como gestionar la ejecución de las mismas.

Atentamente



JUAN CAMILO GONZÁLEZ GARZÓN
Representante de la Alta Dirección para el SIG

Anexo: Doce (12) folios: Guía para la Administración de usuarios del directorio activo - AGTG.21 (v1); y Guía para Recuperación de desastres - AGTG.09 (v3)

Proyectó: Polo Felix Suárez Gómez – Profesional Especializado 
Juan Carlos Rangel Gil – Coordinador Grupo de Seguridad de la Información y Calidad 
Revisó: Duberly Eduardo Murillo Barona – Jefe Oficina de Tecnologías de la Información 
Rolando Garnica Arias – Coordinador Grupo de Desarrollo Organizacional 

	GUÍA ADMINISTRACIÓN USUARIOS DIRECTORIO ACTIVO	Fecha: 12 SET. 2016
		Código: AGTG.10 (v1)
		Página 1 de 6

TABLA DE CONTENIDO

1. OBJETIVO.....	2
2. APLICACIÓN.....	2
3. RESPONSABLES	2
4. GENERALIDADES	3
4.1. Creación de Usuarios Directorio Activo	3
4.2. Delegación de permisos Directorio Activo.....	5

1. OBJETIVO

Definir el procedimiento aplicable a la administración (creación, desactivación) de usuarios dentro del Directorio Activo de la Unidad Administrativa Especial Migración Colombia - UAEMC.

2. APLICACIÓN

Aplica a todo el ámbito de actuación de la UAEMC, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las normas de seguridad de la UAEMC.

El presente procedimiento es de obligatorio cumplimiento para todo el personal que de manera permanente o eventual, preste sus servicios en la UAEMC, especialmente, los responsables de los servicios tecnológicos y de información de la UAEMC y los propios usuarios.

Se entiende por usuario cualquier funcionario público perteneciente o ajeno a la UAEMC, así como el personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la Entidad y que utilice o posea acceso a los Sistemas de Información de la UAEMC.

3. RESPONSABLES

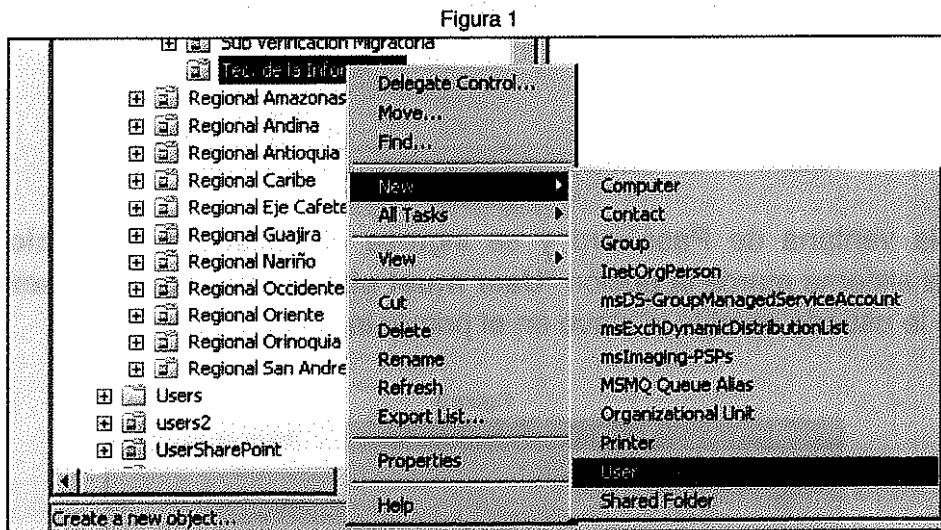
CARGO	RESPONSABILIDADES
Coordinador Grupo de Infraestructura Funcionarios designados del Grupo de Infraestructura	Administrar y gestionar los usuarios del Directorio Activo de la UAEMC <ul style="list-style-type: none"> ▪ Administrar la plataforma Microsoft ▪ Gestionar la inclusión de los funcionarios de la UAEMC en el Directorio Activo

4. GENERALIDADES

Para la administración de la plataforma Microsoft, se crea una cuenta de servicio y se entrega al funcionario designado. Esta cuenta tiene permisos de administrador (administrator) en el dominio.

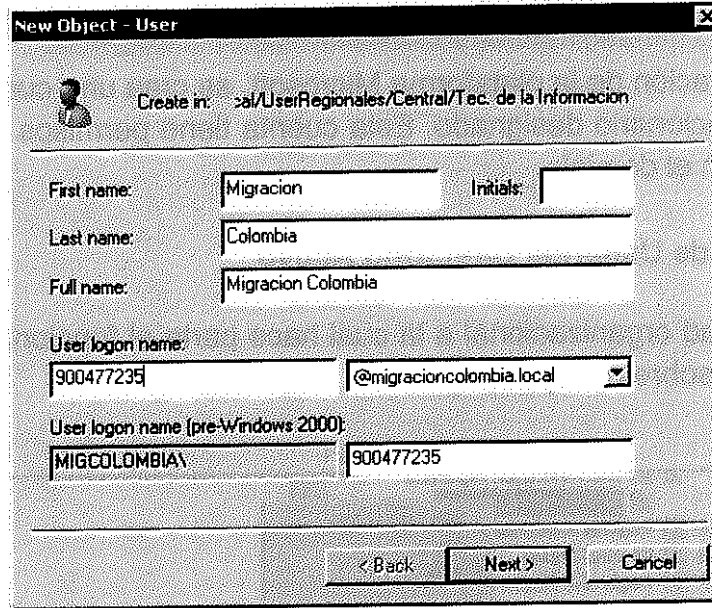
4.1. Creación de Usuarios Directorio Activo

Se ubica la unidad organizacional a la cual hace parte el funcionario, clic derecho sobre esta y clic sobre new y user.



Automáticamente se inicia el asistente, en el cual se ingresan los nombres, apellidos y logon Name el cual es el número de cedula del funcionario y clic en siguiente.

Figura 2



New Object - User

Create in: >al/UserRegionales/Central/Tec. de la Informacion

First name: Initials:

Last name:

Full name:

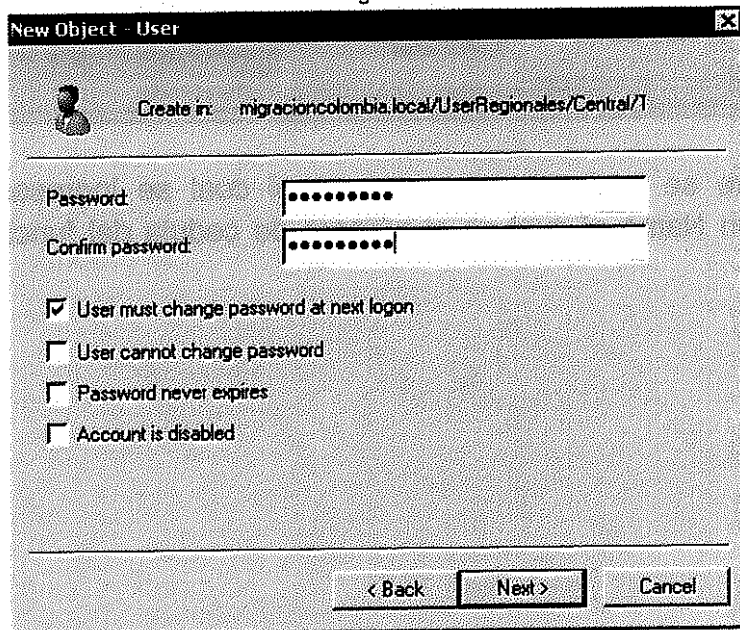
User logon name:

User logon name (pre-Windows 2000):

< Back Next > Cancel

Pasa a la ventana de Password y se ingresa el Password **"Migracion1"**, por defecto el sistema marca la opción **"User must change password at next logon"** para que le usuario cambie la clave en el primer inicio de sesión.

Figura 3



New Object - User

Create in: migracioncolombia.local/UserRegionales/Central/1

Password:

Confirm password:

User must change password at next logon

User cannot change password

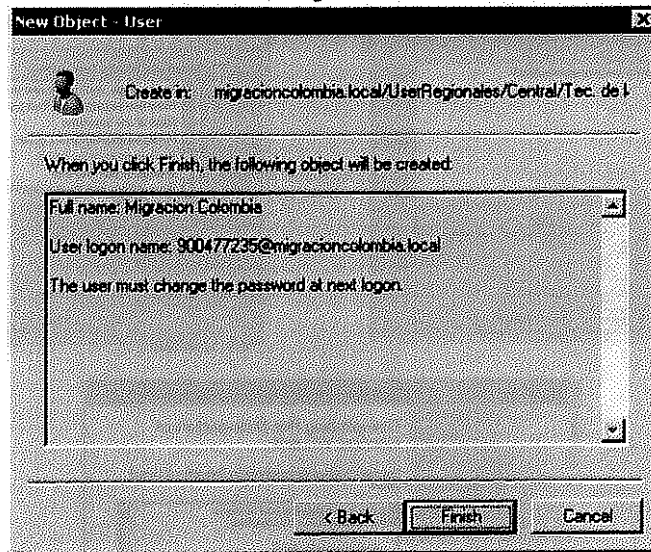
Password never expires

Account is disabled

< Back Next > Cancel

Para terminar se da clic en siguiente y el sistema muestra un resumen del usuario creado y finalizar.

Figura 4



4.2. Delegación de permisos Directorio Activo

En las figuras 5 y 6 se muestra cómo se realiza la delegación de permisos del Directorio Activo

Figura 5

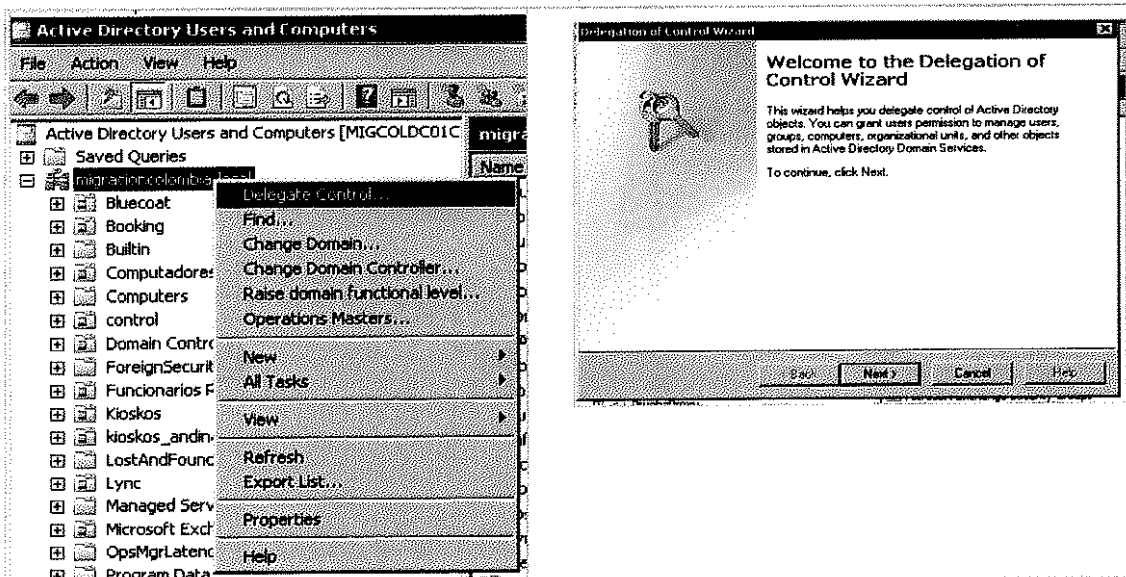
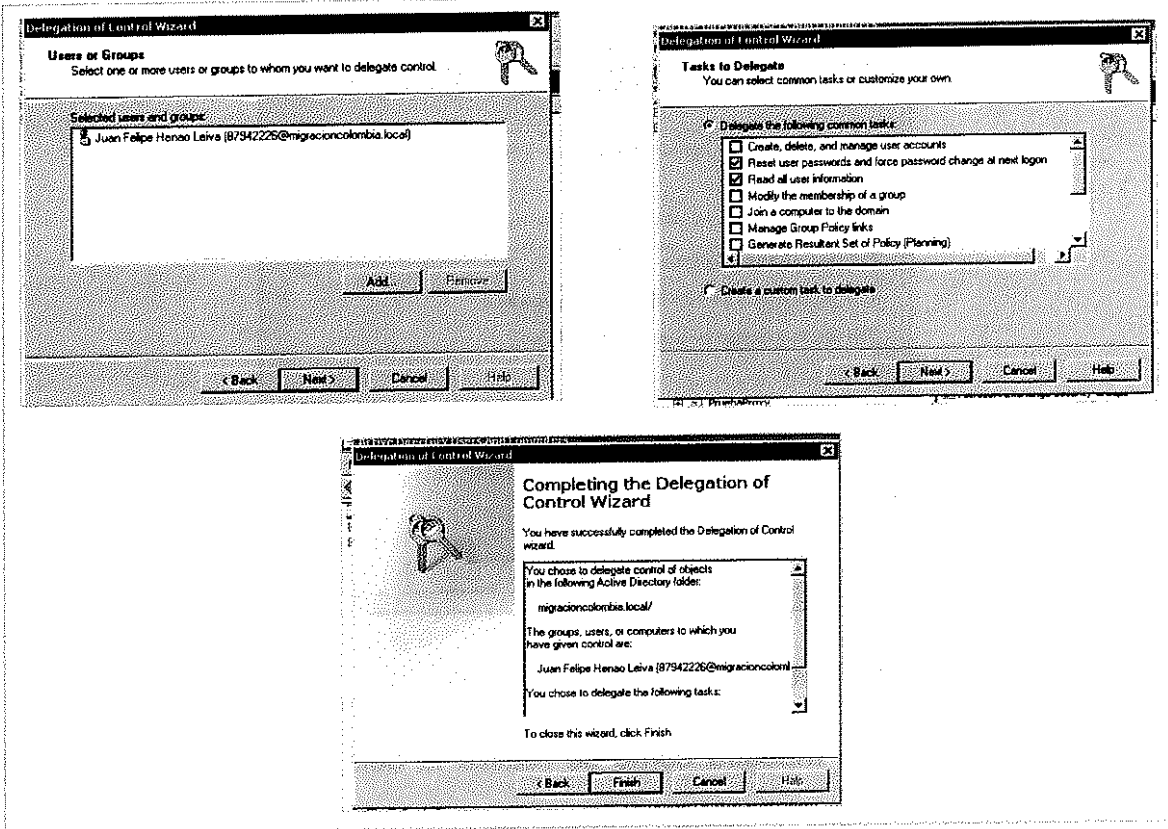


Figura 6





	GUÍA PARA RECUPERACIÓN DE DESASTRES	Fecha: 12 SET. 2016
		Código: AGTG.09 (v3)
		Página 1 de 45

TABLA DE CONTENIDO

INTRODUCCIÓN.....	2
1. OBJETIVO.....	3
1.1. Objetivos Específicos	3
2. ALCANCE	4
2.1. Exclusiones al alcance del DRP	4
3. ANTECEDENTES	5
4. CONDICIONES NORMALES DE OPERACIÓN TIC.....	5
5. ESCENARIOS DE DESASTRE	6
6. ESTRATEGIA DE RECUPERACIÓN	6
7. SUPUESTOS	7
8. DESCRIPCIÓN GENERAL DEL PLAN DE RECUPERACIÓN DE DESASTRES	8
8.1. Fase 1. Preventiva (antes del desastre)	8
8.2. Fase 2. Respuesta (durante el desastre).....	8
8.3. Fase 3. Restauración (después del desastre).....	9
9. GOBIERNO DEL PLAN DE RECUPERACIÓN DE DESASTRES.....	11
9.1. Aprobación del Plan de Recuperación de Desastres	11
9.2. Políticas del Plan de Recuperación de desastres	11
9.3. Roles y Responsabilidades	12
10. TAREAS ANTES DEL DESASTRE (FASE PREVENTIVA)	15
11. TAREAS DURANTE EL DESASTRE (FASE DE RESPUESTA)	18
11.1. Notificación y Activación	18
Recuperación	22
12. TAREAS DESPUÉS DEL DESASTRE (FASE DE RESTAURACIÓN)	27
12.1. Alistamiento del CDP	28
13. RETORNO A LA NORMALIDAD.....	30
14. RIESGOS DE ACTIVAR LA OPERACIÓN EN EL CDA	35
15. PROCEDIMIENTOS TÉCNICOS	37
16. GLOSARIO	38
17. ANEXOS.....	41
ANEXO A	41
ANEXO B	42

	GUÍA PARA RECUPERACIÓN DE DESASTRES	Fecha: 12 SET. 2016 Código: AGTG.09 (v3) Página 2 de 45
--	--	---

INTRODUCCIÓN

Los sistemas de información son vitales para la realización de los procesos y el logro de los objetivos de la Unidad Administrativa Especial Migración Colombia – UAEMC, por lo tanto, es fundamental la prestación y funcionamiento eficaz de los mismos sin interrupciones excesivas.

Este Plan de Recuperación de Desastres (DRP) establece los procedimientos integrales para recuperar los servicios críticos y la tecnología de apoyo con rapidez y eficacia, una vez se ha presentado la interrupción del servicio en el CDP (Centro de Datos Principal) y las estrategias de recuperación a nivel local han sido superadas por un desastre mayor.

1. OBJETIVO

Establecer los procedimientos para recuperar los sistemas de información y servicios tecnológicos más críticos de la UAEMC en el CDA (Centro de Datos Alterno), con el fin de hacer frente a un desastre grave que afecte las instalaciones del CDP (Centro de Datos Principal).

1.1. Objetivos Específicos

Los objetivos del Plan de Recuperación de Desastres son los siguientes:

- Maximizar la eficacia de las operaciones en contingencia, mediante el plan establecido que consta de las siguientes fases:
 - 1) **Activación y Notificación**, para informar la decisión de activar el plan
 - 2) **Recuperación**, durante la cual se inician los sistemas de información y servicios tecnológicos en el CDA (Centro de Datos Alterno),
 - 3) **Restauración**, para asegurar que el funcionamiento de los servicios se valida a través de pruebas y se retornan las operaciones de TIC a la normalidad en el CDP.
- Identificar las actividades, recursos y procedimientos necesarios para el funcionamiento de los sistemas de información y servicios tecnológicos en el CDA en una situación de desastre.
- Asignar responsabilidades la Oficina de Tecnología de la Información, la Mesa de Ayuda y terceros proveedores para proporcionar orientación a la recuperación de los sistemas de información y servicios tecnológicos en el CDA.
- Asegurar la coordinación con los líderes funcionales de las aplicaciones que son responsables por los controles preventivos, la planificación de imprevistos y la realización de tareas de recuperación y reanudación.
- Asegurar la coordinación con los puntos exteriores de contacto y proveedores relacionados con los sistemas de información y servicios tecnológicos de la UAEMC.

2. ALCANCE

Este Plan de Recuperación de Desastres - DRP se ha desarrollado para la recuperación de los sistemas de información y servicios tecnológicos que apoyan los procesos misionales Control Migratorio, Extranjería y Verificación Migratoria de la UAEMC. Dichos sistemas y servicios se listan a continuación:

Servicios:

- Redes y Comunicaciones.
- Firewall perimetral.
- Controlador de Dominio.
- DNS.
- Correo.
- Bases de Datos (PCM, Platinum).
- Almacenamiento y Carpetas Compartidas

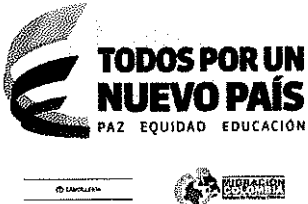
Sistemas de Información:

- Platinum – Plataforma Única de Información Misional, que incluye los módulos de:
 - PCM, Puesto de Control Migratorio
 - Extranjería.
 - Verificaciones.
 - SIRE, Sistema de Información para el registro de extranjeros
- Orfeo – Gestión Documental
- Sitios Web Institucionales

2.1. Exclusiones al alcance del DRP

El plan excluye:

- La pérdida de datos en computadores de usuario final.
- La recuperación en el CDA de otros sistemas de información o servicios de tecnología diferentes a los definidos en este alcance.
- La evacuación de personal de las instalaciones principales de la UAEMC o alguna de sus sedes.

	GUÍA PARA RECUPERACIÓN DE DESASTRES	Fecha: 12 SET. 2016
		Código: AGTG.09 (v3)
		Página 5 de 45

- La recuperación de la totalidad de las operaciones de la UAEMC, no incluidas en el alcance.

3. ANTECEDENTES

En el proceso de formulación del Plan de Recuperación de Desastres de la UAEMC, se han adelantado los siguientes pasos:

- 1) Identificación de los procesos críticos de negocio.
- 2) Análisis de riesgos tecnológicos (RA).
- 3) Identificación de los posibles escenarios de desastre.
- 4) Implementación de la estrategia de recuperación, que incluye la adecuación de en un CDA (Centro de Datos Alterno) en Medellín.
- 5) Definición de los objetivos y alcance del Plan de Recuperación de Desastres.

4. CONDICIONES NORMALES DE OPERACIÓN TIC

A continuación, se describen las principales características de la operación tecnológica en la UAEMC:

- Esquema centralizado con un CDP (Centro de Datos Principal) ubicado en la Sede Administrativa (Avenida Calle 26 No 59-51. Bogotá).
- Canales de comunicación (Acceso a Internet, Regionales, Puestos de Control Migratorio, Centros Facilitadores de Servicios Migratorios) a través de MPLS provista por Telefónica.
- Estrategia de Recuperación mediante CDA (Centro de Datos Alterno) ubicado en la Regional Antioquia (Calle 19 # 80A-40. Medellín)
- Acceso a Internet por el CDP (Centro de Datos Principal) únicamente.
- Canales de replicación entre el CDP y el CDA con Telefónica.
- Estrategia de respaldo de datos en CDP.

4

5. ESCENARIOS DE DESASTRE

En la UAEMC se identificaron los siguientes escenarios de desastre:


Tabla 1. Escenarios de Desastre

Escenario # 1:	Falla generalizada de la red. Categoría II
Escenario # 2:	No disponibilidad del CDP (Centro de Datos Principal). Sede Administrativa. Categoría II
Escenario # 3:	No disponibilidad de las instalaciones físicas de la UAEMC. Categoría II
Escenario # 4:	Interrupción de proveedores claves en la cadena de suministro de la UAEMC.
Escenario # 5:	Estado de emergencia nacional (Desastre natural, pandemia, ataque terrorista).

6. ESTRATEGIA DE RECUPERACIÓN

La estrategia de recuperación definida y que tiene implementada la UAEMC se reúne en las siguientes categorías:

- A. Centro de Datos Alterno:** La UAEMC cuenta con un Centro de Datos Alterno, ubicado en la Regional Antioquia (Calle 19 # 80A-40, Medellín), el cual cumple con todas las condiciones necesarias de adecuación y seguridad para prestar los servicios.
- B. Recuperación de telecomunicaciones:** El CDA cuenta con canales de comunicación alternos para garantizar la comunicación con: Acceso a Internet, Regionales, Puestos de Control Migratorio, Centros Facilitadores de Servicios Migratorios, a través de MPLS provista por Telefónica.
- C. Replicación de datos:** La UAEMC cuenta con canales de replicación entre el CDP y el CDA mediante el proveedor Telefónica, para replicar los sistemas de información y servicios críticos definidos en el numeral 2. Alcance.
- D. Recuperación de aplicaciones:** El CDA ha sido aprovisionado con la tecnología requerida para activar los sistemas de información y servicios tecnológicos críticos de la UAEMC, definidos en el numeral 2. Alcance.

	GUÍA PARA RECUPERACIÓN DE DESASTRES	Fecha: 12 SET. 2016
		Código: AGTG.09 (v3)
		Página 7 de 45


E. Copias de respaldo: La UAEMC cuenta con una estrategia de respaldo de datos en CDP.

F. Puestos de Control Migratorio: Los puestos de control migratorio cuentan con estrategia local, para garantizar la continuidad del módulo PCM del sistema Platinum, esto mediante servidores locales que asumen el servicio ante una falla del CDP y que una vez restaura el funcionamiento normal bien sea en el CDP o en el CDA sincronizan los cambios efectuados en la plataforma.

7. SUPUESTOS

El Plan de Recuperación de Desastres (DRP) definido se construyó bajo los siguientes supuestos:

- 1) El CDP de la UAEMC ha sufrido daños severos que inhabilitan su funcionalidad o se puede recuperar en término de días o semanas.
- 2) Se cuenta con respaldo de datos localizados en una instalación diferente al
- 3) CDP y se encuentran actualizados.
- 4) Los sistemas de información y servicios tecnológicos críticos son los relacionados en el Alcance.
- 5) El CDA (Centro de Datos Alterno) ha sido aprovisionado con la tecnología requerida para activar los sistemas de información y servicios tecnológicos críticos de la UAEMC, funciona y se han realizado pruebas al mismo.
- 6) Se cuenta con un sistema para restauración de copias en CDA, compatible con el utilizado para su generación en el CDP.
- 7) El CDA cuenta con canales de comunicación a: Acceso a Internet, Regionales, Puestos de Control Migratorio, Centros Facilitadores de Servicios Migratorios, a través de MPLS provista por Telefónica.
- 8) Los equipos de trabajo del Plan de Recuperación de Desastres han sido capacitados y entrenados oportunamente.

	GUÍA PARA RECUPERACIÓN DE DESASTRES	Fecha: 12 SET. 2016
		Código: AGTG.09 (v3)
		Página 8 de 45

8. DESCRIPCIÓN GENERAL DEL PLAN DE RECUPERACIÓN DE DESASTRES

El Plan de Recuperación de Desastres (DRP) se desarrolló para recuperar y restaurar los sistemas de información y servicios tecnológicos críticos de la UAEMC, usando un enfoque de tres fases.

Este enfoque garantiza que los esfuerzos de recuperación y restauración de los sistemas se realizan en una secuencia metódica para maximizar su eficacia y minimizar el tiempo de interrupción debido a errores y omisiones. Las tres fases son:

8.1. Fase 1. Preventiva (antes del desastre)

Son todas las tareas diarias que se realizan en CDP orientadas a la reducción de la probabilidad de materialización de eventos que se conviertan en desastres o la mitigación de su impacto.

8.2. Fase 2. Respuesta (durante el desastre)

Son las tareas que se llevan a cabo una vez se ha materializado un desastre que obligue a contemplar la activación de planes de contingencia. A su vez comprende dos fases: A) Activación y notificación y B) Recuperación.

A. Fase de Activación y Notificación: La activación del DRP se produce después de una interrupción de los sistemas de información y servicios tecnológicos del CDP y la magnitud del desastre obliga a trasladar el procesamiento al CDA (Centro de Datos Alterno).

El Líder de Recuperación de Desastres ha recibido la evaluación de daños del CDP y estima necesario activar el DRP. Una vez que el DRP se activa, los propietarios de los sistemas de información, servicios tecnológicos y los terceros requeridos son informados de la decisión.

B. Fase de Recuperación: Se ejecutan en orden los planes de contingencia de los sistemas de información y servicios tecnológicos críticos. Se incluyen actividades de notificación y comunicación sobre el estado de la recuperación a los propietarios y a los usuarios de dichos servicios y sistemas.

8.3. Fase 3. Restauración (después del desastre)

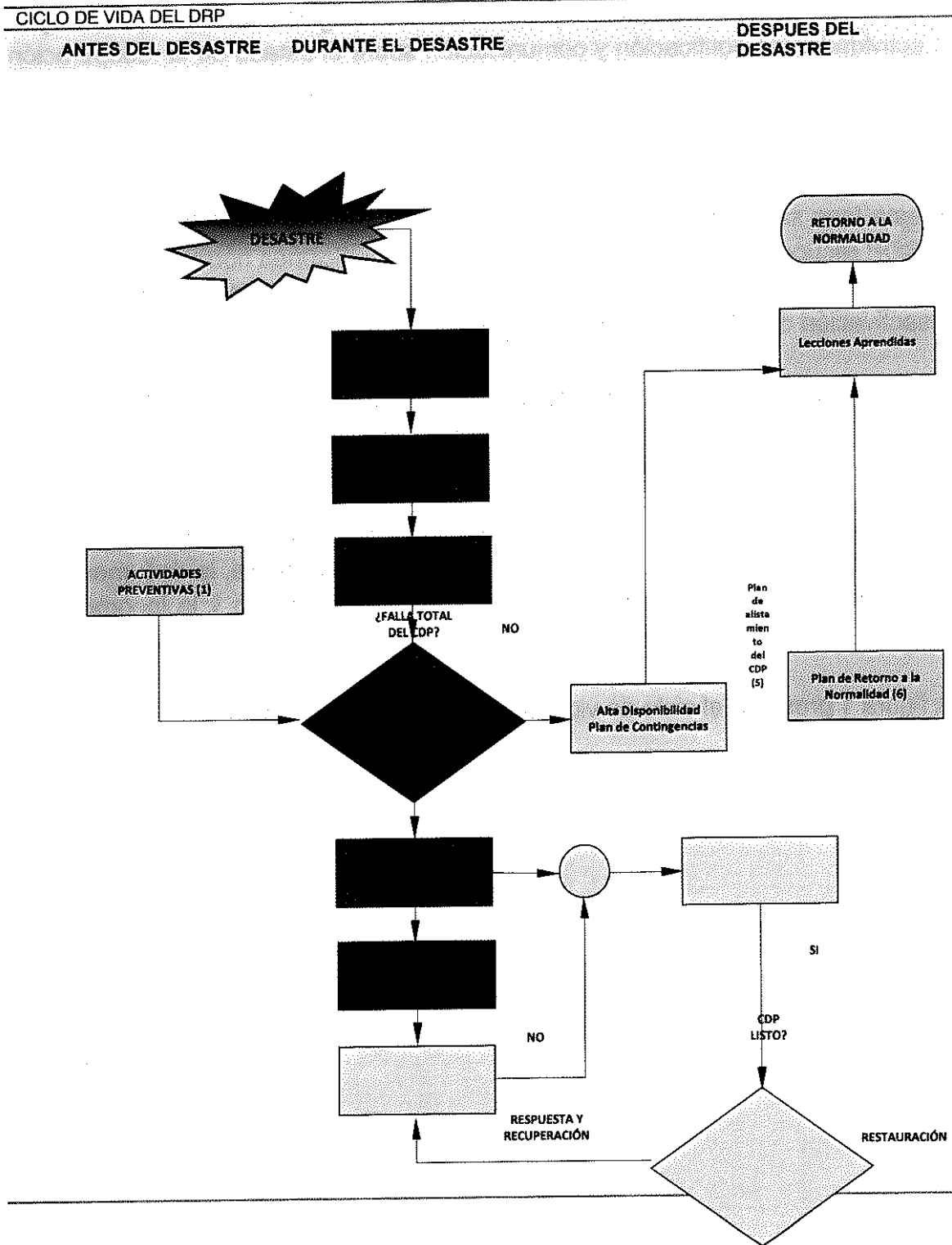
En esta fase se realizan acciones previstas para verificar y validar la capacidad del CDP recuperado para su funcionamiento en condiciones normales. Consta de 2 actividades principales: A) Validación de la restauración exitosa y B) Desactivación del plan (fin de la contingencia).


A. Validación de la restauración: Durante la validación, se prueban los sistemas, se declara la recuperación de los mismos y los dueños autorizan el inicio normal de operaciones.

B. Desactivación del plan: La desactivación incluye actividades de comunicación a los usuarios sobre el fin de la contingencia, la documentación de las actividades realizadas para superar la interrupción y la incorporación de las lecciones aprendidas en la actualización de los procedimientos.

La figura 1 presenta el ciclo de vida del Plan de Recuperación de Desastres.

Figura 1. Ciclo de vida del DRP de la UAEMC



	GUÍA PARA RECUPERACIÓN DE DESASTRES	Fecha: 12 SET. 2016
		Código: AGTG.09 (v3)
		Página 11 de 45

9. GOBIERNO DEL PLAN DE RECUPERACIÓN DE DESASTRES

9.1. Aprobación del Plan de Recuperación de Desastres

El **Anexo A** presenta un modelo de carta para la aprobación del Plan de Recuperación de desastres, el cual deberá ser firmado por el Jefe de la Oficina de Tecnología de la Información de la UAEMC. Dicha carta certifica que el DRP es completo y que la estrategia de recuperación seleccionada es apropiada para la UAEMC teniendo en cuenta una relación costo – beneficio.

9.2. Políticas del Plan de Recuperación de desastres

Las siguientes son las políticas que deberán cumplirse para el mantenimiento, divulgación, patrocinio y sostenibilidad del Plan de Recuperación de Desastres (DRP) definido por la UAEMC:

- Todo el personal de la UAEMC con responsabilidades en el Plan de Recuperación de Desastres deberá estar entrenado y capacitado en los planes y procedimientos definidos y conocer claramente sus roles y responsabilidades.
- El Plan de Recuperación de Desastres debe ser divulgado a todas las personas que intervienen en las operaciones de contingencia y recuperación, a través de campañas, talleres y simulacros.
- Las tareas de contingencia y recuperación definidas en el Plan de Recuperación de Desastres, deben estar integradas en el manual de funciones de los responsables.
- La Oficina de Tecnología de la Información reconoce que el Plan de Recuperación de Desastres, ayuda a la organización a recuperarse de desastres mayores que afecten las instalaciones principales de la UAEMC, por tanto, contará con un presupuesto anual apropiado para garantizar la sostenibilidad del plan.
- El Plan de Recuperación de Desastres deberá ser probado por lo menos una vez cada año.
- Las pruebas del Plan de Recuperación de Desastres deben ser acordadas con las áreas y terceros requeridos para las mismas.

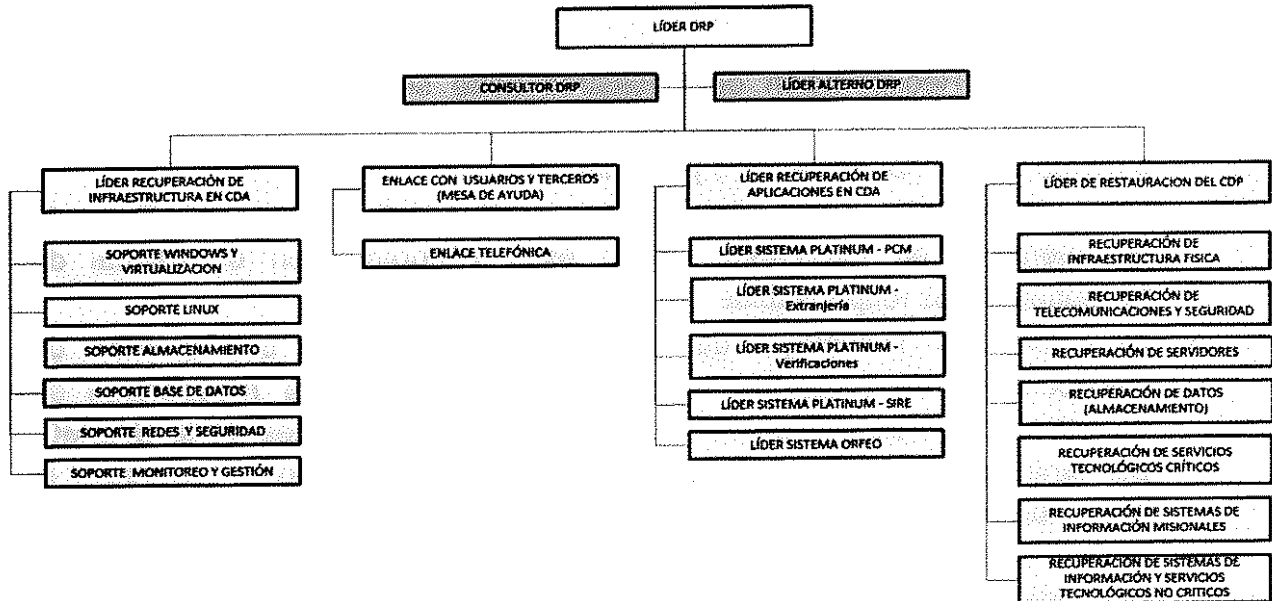
- La UAEMC debe llevar un monitoreo constante sobre el funcionamiento y desempeño del CDA. Todos los informes deberán ser objeto de análisis y retroalimentación.
- El Líder de Recuperación de Desastres es responsable por la actualización constante del Plan de Recuperación de Desastres.

Este documento permanecerá en la Intranet de la UAEMC vigente, en la ruta descargas/DRP. Las copias físicas serán responsabilidad de quien las imprima y llevarán la marca "copia sin control". Adicionalmente se tendrá una copia digital en el sitio de custodia de las cintas con el nombre "Plan de Recuperación de Desastres (DRP) Vigente aa_mm_dd".

9.3. Roles y Responsabilidades

En la figura 2 se presenta la organización de los equipos de trabajo responsables por realizar las tareas del Plan de Recuperación de desastres definido.

Figura 2. Roles y Responsabilidades del DRP



En la tabla 1, se presentan la conformación de los equipos de recuperación y las responsabilidades definidas:

Tabla 1. Equipos de Recuperación

Equipo	Líder Principal	Líder Alterno	Responsabilidades
Líder DRP			Declarar la activación del plan de recuperación de desastres
			Declarar el fin de operaciones en el CDA y coordinar el retorno a la normalidad
Consultor DRP			Experto en DRP.
Líder de Recuperación de Infraestructura en CDA			Coordinar la interacción entre los líderes de recuperación de la UAEMC y sus proveedores
			Definir los funcionarios de la UAEMC que deben desplazarse al CDA.
			Declarar la funcionalidad del CDA.
			Informar los eventos importantes a la gerencia de la UAEMC.
Soporte Windows y Virtualización			Experto en virtualización y sistemas operativos Windows
Soporte Linux			Experto en sistemas operativos Linux
Soporte Almacenamiento			Experto en almacenamiento
Soporte Base de Datos			Experto en bases de datos
Soporte Redes y Seguridad			Experto en Redes y Seguridad.
Soporte Monitoreo y Gestión			Experto en monitoreo y gestión del Centro de Datos Principal
Enlace con usuarios y terceros (Mesa de Ayuda)			Notificar a terceros de TIC sobre la activación del DRP.
			Dar las instrucciones a terceros y usuarios sobre la funcionalidad del CDA.
			Coordinar el soporte a usuarios durante la contingencia.
			Coordinar con los terceros y usuarios las tareas para el fin de contingencia y retorno a la normalidad.
			Informar los eventos importantes al Líder de Recuperación en el CDA.
Enlace Telefónica (UAEMC)			Dar solución a incidentes sobre la WAN que provee Telefónica.
Líder de Recuperación de Aplicaciones en el CDA			Validar con el equipo del CDA la integridad de los datos.
			Realizar las pruebas funcionales de los servicios críticos DRP.
			Informar al Líder de Recuperación de Infraestructura en CDA, la funcionalidad de las aplicaciones
			Informar los eventos importantes al

Equipo	Líder Principal	Líder Alternativo	Responsabilidades
			Líder de Recuperación de Infraestructura en CDA. Coordinar las actividades necesarias para la finalización de operaciones en el CDA.
Líder del Sistema PLATINUM - PCM			Dar solución a incidentes en el módulo de PCM del sistema PLATINUM.
Líder del Sistema PLATINUM - Extranjería			Dar solución a incidentes en el módulo de Extranjería del sistema PLATINUM.
Líder del Sistema PLATINUM - Verificaciones			Dar solución a incidentes en el módulo de Verificaciones del sistema PLATINUM.
Líder del Sistema PLATINUM - SIRE			Dar solución a incidentes en el módulo de SIRE del sistema PLATINUM.
Líder del Sistema ORFEO			Dar solución a incidentes sobre el sistema ORFEO.
Líder de Restauración del CDP			Finalizar la evaluación de daños del CDP. Formalizar el presupuesto de restauración del CDP. Recomendar la decisión: Reconstruir o tomar en arriendo un DataCenter Coordinar las adquisiciones y contrataciones requeridas Conducir las pruebas de funcionalidad del nuevo CDP. Informar los eventos importantes a la gerencia de la UAEMC. Coordinar el traslado de datos y aplicaciones del CDA al CDP Declarar la funcionalidad del CDP
Recuperación de Infraestructura Física			Recuperar la infraestructura física
Recuperación de Telecomunicaciones y Seguridad			Recuperar mesa infraestructura de telecomunicaciones y seguridad
Recuperación de Servidores			Recuperar la infraestructura de servidores
Recuperación de Datos (almacenamiento)			Recuperar los datos
Recuperación de servicios tecnológicos críticos			Recuperar los servicios tecnológicos críticos.
Recuperación de Sistemas de Información			Recuperar los sistemas de información misionales.
Recuperación de Sistemas de información y servicios			Recuperar los sistemas de información y servicios tecnológicos no críticos.

Equipo	Líder Principal	Líder Alternativo	Responsabilidades
tecnológicos No Críticos			

10. TAREAS ANTES DEL DESASTRE (FASE PREVENTIVA)

El líder de recuperación de desastres, es el responsable de asegurar que se realicen las actividades listadas en la tabla 3 de forma periódica

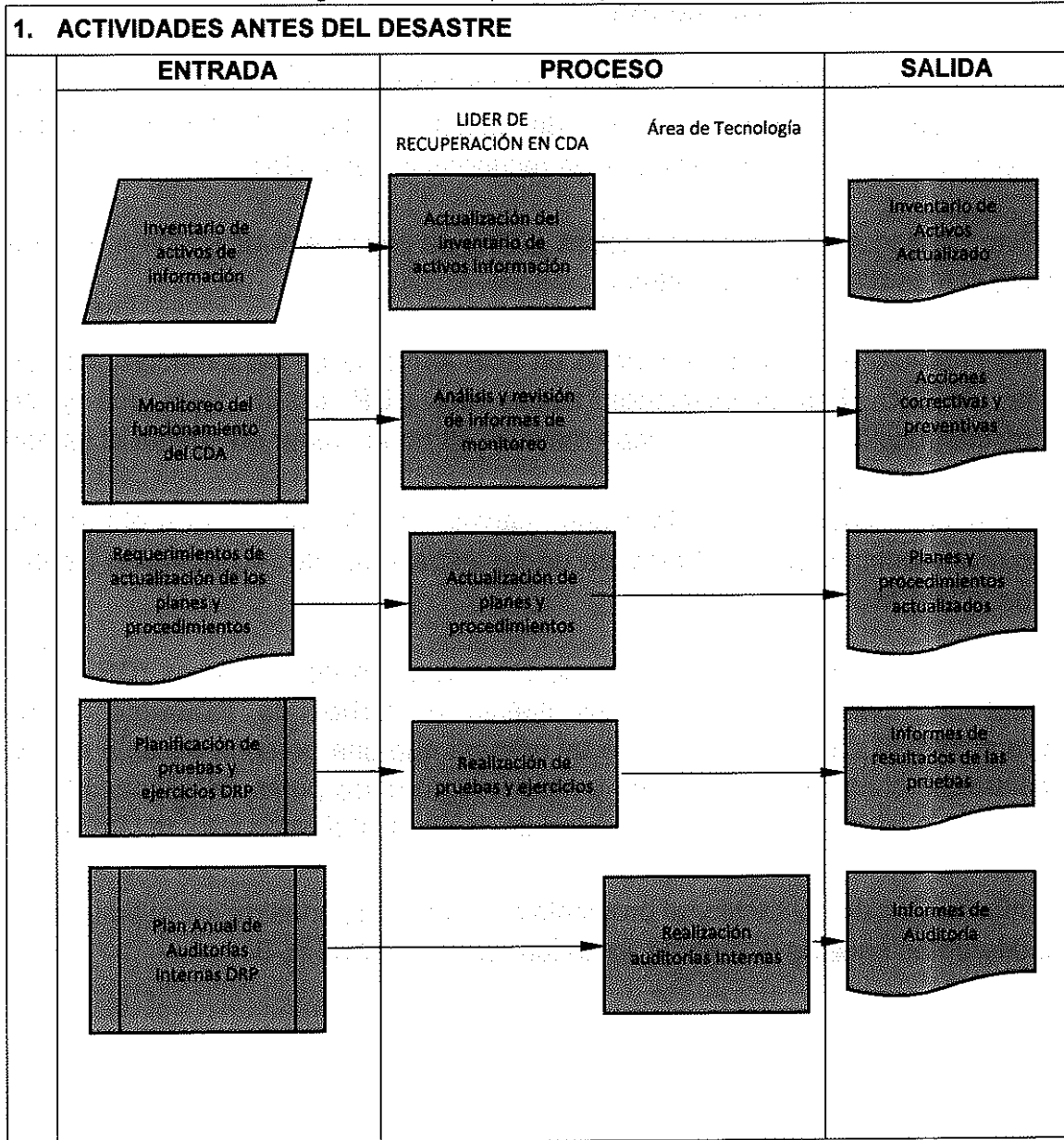
Tabla 3. Actividades preventivas del DRP

No.	Actividad	Detalles de Implementación	Recursos	Responsable	Debe interactuar con
1	Actualización del inventario de activos.	Auditar el inventario de la infraestructura tecnológica del CDA y verificar la actualización de cambios que se presenten: Nuevos dispositivos, dispositivos retirados, ampliación de canales, almacenamientos, entre otros.	Archivo Excel con el inventario de activos del CDA.	Líder de Recuperación en CDA.	Control de cambios.
2	Revisión de informes de monitoreo del CDA.	Revisar e indagar por los informes diario, semanal y mensual de monitoreo de disponibilidad de los servicios del CDA.	Reportes de Monitoreo.	Líder de Recuperación en CDA.	Control de cambios.
3	Pruebas y simulacros del DRP.	Planear y realizar pruebas y simulacros de funcionamiento del CDA.	<ul style="list-style-type: none"> • Diseño de pruebas • Informe de pruebas realizadas. 	Líder de Recuperación en CDA.	Líder de restauración del CDP.
4	Actualizar información de contacto de los funcionarios y terceros con	Con motivo de las pruebas y auditorias del DRP se debe verificar la actualización de los	Hoja Excel con Información de Contacto de los Miembros de los equipos de	Líder de Recuperación en CDA.	<ul style="list-style-type: none"> • Líder de restauración del CDP • Líder de Recuperación

No.	Actividad	Detalles de Implementación	Recursos	Responsable	Debe Interactuar con
	responsabilidad en el DRP.	datos de contacto del personal de la UAEMC, y terceros con responsabilidad en el DRP.	Recuperación.		de aplicaciones • Líder de contacto con terceros.
5	Actualizar los planes y procedimientos del DRP.	Con base en los resultados de las pruebas y ejercicios, el control de cambios y los informes de auditoría, se deben actualizar los planes y procedimientos del DRP: Cambios en servicios, tecnología, proveedores, entre otros.	Planes y procedimientos de recuperación documentados.	Líder de Recuperación en CDA.	Líder de restauración del CDP.
6	Auditoría interna al DRP.	Coordinar con Control Interno la realización de auditorías periódicas al DRP.	Procedimiento de Auditoría al DRP.	La Oficina de Tecnología de la Información.	Líder de Recuperación de Desastres.

La figura 3, presenta las actividades preventivas del DRP.

Figura 3. Actividades preventivas (Antes del desastre)



✶

11. TAREAS DURANTE EL DESASTRE (FASE DE RESPUESTA)

11.1. Notificación y Activación

En esta fase se definen las acciones que se toman ante la interrupción de los sistemas de información y servicios de tecnología del CDP. Las actividades incluyen la notificación a los equipos de recuperación definidos.

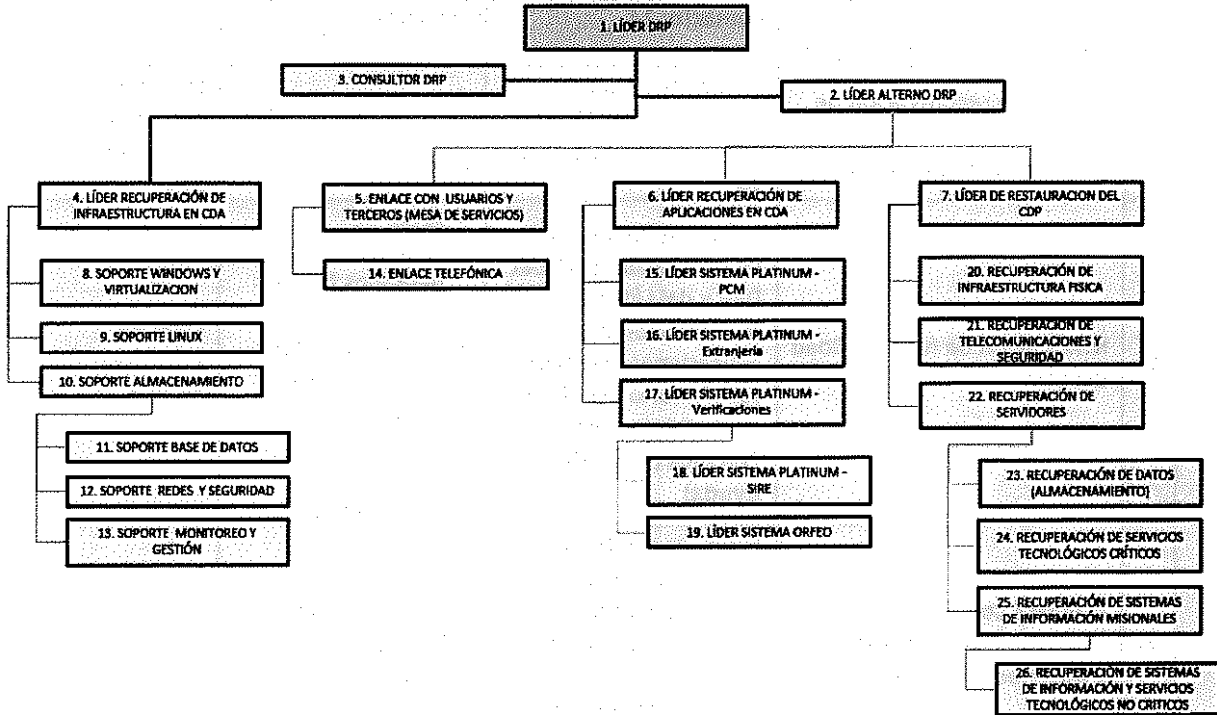
El Plan de Recuperación de Desastres (DRP) se puede activar si uno o más de los siguientes criterios se cumplen:

- Se presentó un desastre natural o un acto terrorista en las inmediaciones de la UAEMC. Las instalaciones físicas del CDP están destruidas y su reconstrucción tomará un tiempo mayor a 48 horas (tener en cuenta el tiempo de toma de la decisión).
- En general cualquier tipo de evento, causado por la naturaleza o el hombre, cuyos efectos superan el alcance de las estrategias de recuperación locales de la UAEMC.

Para notificar la activación del Plan de Recuperación de Desastres (DRP) y el control del avance del mismo se definió el “**árbol de llamadas**” como herramienta de comunicaciones, de tal manera que una persona máxima realice y controle 3 contactos hacia abajo y reporte a un único punto de contacto hacia arriba. En la figura 4, se observa el árbol de llamadas definidas para la UAEMC.

La información de contacto y el protocolo de comunicaciones de los miembros de los diferentes equipos de trabajo se encuentran en el **Anexo B**.

Figura 4. Árbol de llamadas del DRP



Para notificar y activar el Plan de Recuperación de Desastres se procede de la siguiente manera:

No.	Actividad	Detalles de Implementación	Recursos	Responsable
1.	Alertar a los líderes de recuperación.	El Líder DRP alerta a sus tres contactos: 2, 3 y 4	Árbol de llamadas, teléfonos fijos y celulares.	Líder DRP
2.	Alertar a los líderes de recuperación.	El Líder Alterno de DRP alerta a sus tres contactos: 5, 6 y 7	Árbol de llamadas, teléfonos fijos y celulares.	Líder Alterno DRP
3.	El líder de recuperación inicia los procedimientos de activación del CDA	El líder de Recuperación de Infraestructura en CDA alerta a sus tres contactos: 8, 9 y 10. 10 notifica a 11, 12 y 13.	Árbol de llamadas, teléfonos fijos y celulares.	Líder de recuperación de infraestructura en CDA
4.	La mesa de Ayuda notifica a los usuarios y a los	El enlace con usuarios y terceros alerta a su	Árbol de llamadas, teléfonos fijos y	Mesa de servicios

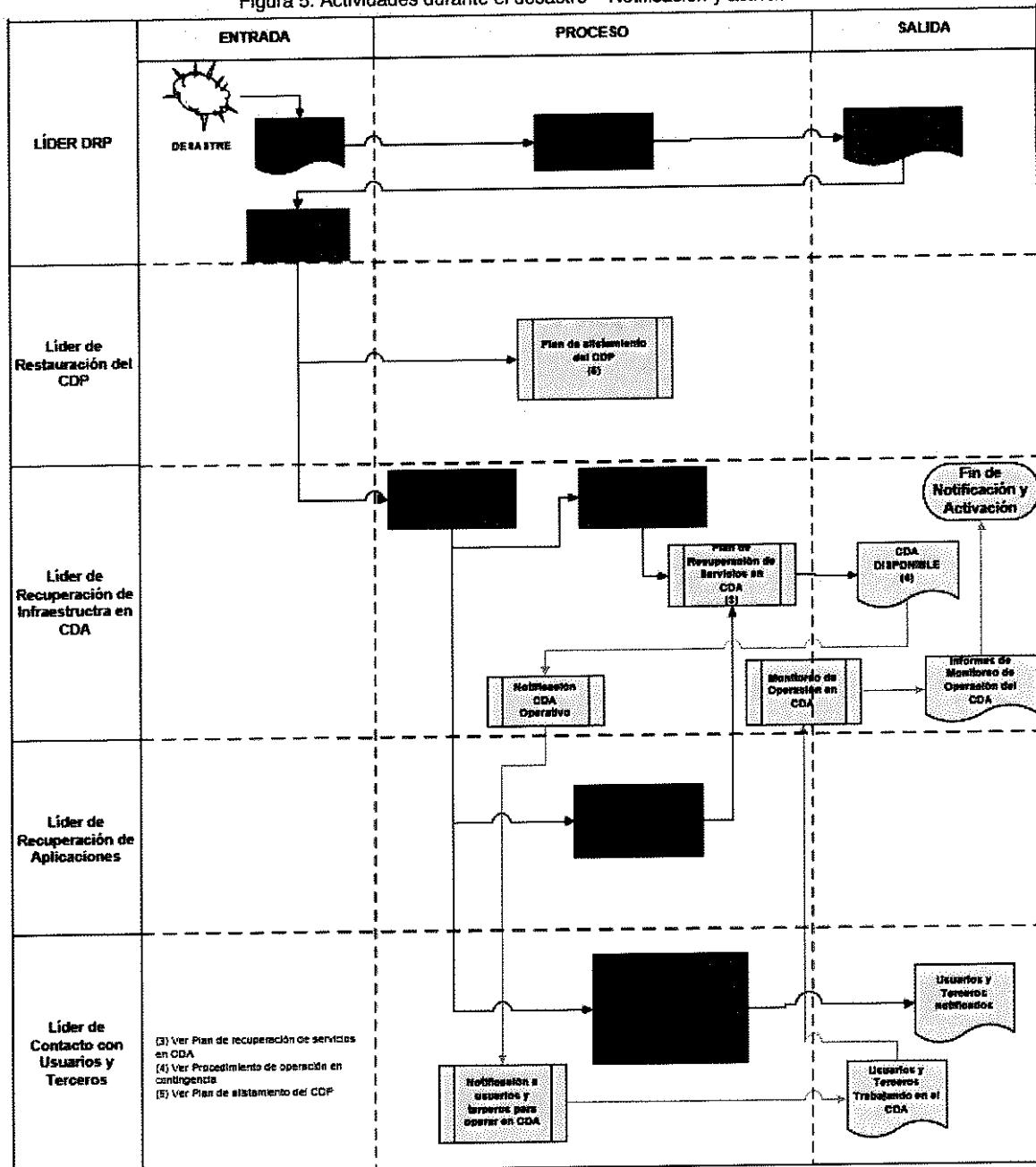
No.	Actividad	Detalles de Implementación	Recursos	Responsable
	proveedores de TIC requeridos por el DRP	contacto: 14	celulares.	
5.	El Líder de recuperación de aplicaciones notifica a su grupo la activación del DRP	El líder notifica a sus tres contactos: 15, 16 y 17. 17 notifica a 18 y 19.	Árbol de llamadas, teléfonos fijos y celulares.	Líder de recuperación de aplicaciones en CDA
6.	Notificación de funcionalidad del CDA	El líder de recuperación en CDA recibe del Líder DRP y del Líder de recuperación de aplicaciones el estado satisfactorio del CDA y avisa al Enlace con Terceros (Mesa de Ayuda)	<ul style="list-style-type: none"> Árbol de llamadas, teléfonos fijos y celulares. Procedimientos De recuperación de servicios críticos DRP (Punto 4. Recuperación) 	Líder de Recuperación en CDA
7.	El enlace con terceros contacta a usuarios externos e internos (Mesa de Ayuda).	El enlace con terceros avisa a usuarios externos e internos el inicio de sistemas de información y servicios tecnológicos desde el CDA.	Árbol de llamadas, teléfonos fijos, celulares	Enlace con Terceros (Mesa de Ayuda)
8.	Inicio de actividades de restauración del CDP	El Líder DRP gestiona con el Líder de restauración del CDP la logística necesaria para iniciar el procedimiento de reconstrucción del CDP. Notifica a 20, 21 y 22. 22 notifica a 23, 24 y 25. 25 notifica a 26.	<ul style="list-style-type: none"> Árbol de llamadas, teléfonos fijos, celulares. Informe de evaluación de daños Presupuesto de reconstrucción Equipo humano requerido 	<ul style="list-style-type: none"> Líder DRP Líder de Restauración del CDP Líder de Recuperación de Infraestructura en CDA
9.	Ejecución de procedimiento de restauración del CDP.	El Líder de restauración del CDP inicia el procedimiento y gestiona la recuperación de infraestructura, datos, aplicaciones y servicios en el CDP	<ul style="list-style-type: none"> Presupuesto Cronogramas de trabajo Órdenes de compra Evaluaciones de avance Informes de prueba de funcionalidad del CDP 	<ul style="list-style-type: none"> Líder de restauración del CDP Líder DRP

No.	Actividad	Detalles de Implementación	Recursos	Responsable
10.	Inicia el retorno a la normalidad	El Líder DRP, el Líder de Recuperación CDA y el Líder de Restauración del CDP analizan el estado de alistamiento y definen la logística para el retorno a la normalidad	Procedimiento de retorno a la normalidad Plan de trabajo del Retorno	Líder DRP

NOTA: La única persona autorizada para activar el plan de recuperación de desastres es el Líder DRP o su alterno.

La figura 5, presenta el diagrama de flujo del proceso de notificación y activación del DRP.

Figura 5. Actividades durante el desastre – Notificación y activación

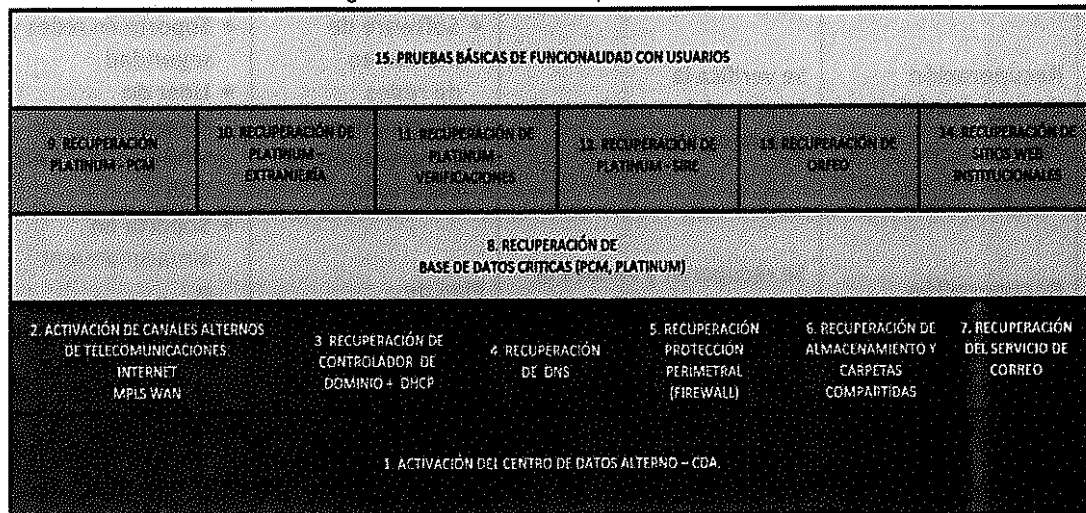


Recuperación

En esta fase se describen las actividades a realizar una vez se activa el Plan de Recuperación de Desastres (DRP). El objetivo de esta fase es la recuperación de

los servicios y sistemas de información críticos en el CDA. La secuencia de recuperación se presenta en la figura 6.

Figura 6. Secuencia de recuperación en el CDA



NOTA: Se entrega a producción todo el CDA. No se prevé activación escalonada de servicios

El procedimiento a seguir es el siguiente:

Tabla 5. Procedimiento de recuperación de sistemas y servicios críticos en el CDA

No.	Actividad	Detalles de Implementación	Recursos	Responsable
1.	Movilización del personal al CDA	El líder de recuperación en CDA determina que ingenieros de la Oficina de Tecnología de la Información requieren movilizarse al CDA si es necesario.	Lista de personal de la Oficina de Tecnología de la Información.	Líder de Recuperación de Infraestructura en CDA
2.	Recuperación de telecomunicaciones del CDA	Se verifica la disponibilidad de los canales WAN e Internet del CDA.	<ul style="list-style-type: none"> Software de monitoreo de redes Procedimiento de recuperación de telecomunicaciones 	<ul style="list-style-type: none"> Soporte en redes y seguridad Líder de Recuperación de Infraestructura en CDA
3.	Recuperación de servidores de dominio	Se verifica la disponibilidad y funcionamiento de los servicios de Dominio,	Procedimiento técnico de activación de Dominio, DHCP,	<ul style="list-style-type: none"> Soporte en redes y seguridad Líder de Recuperación de

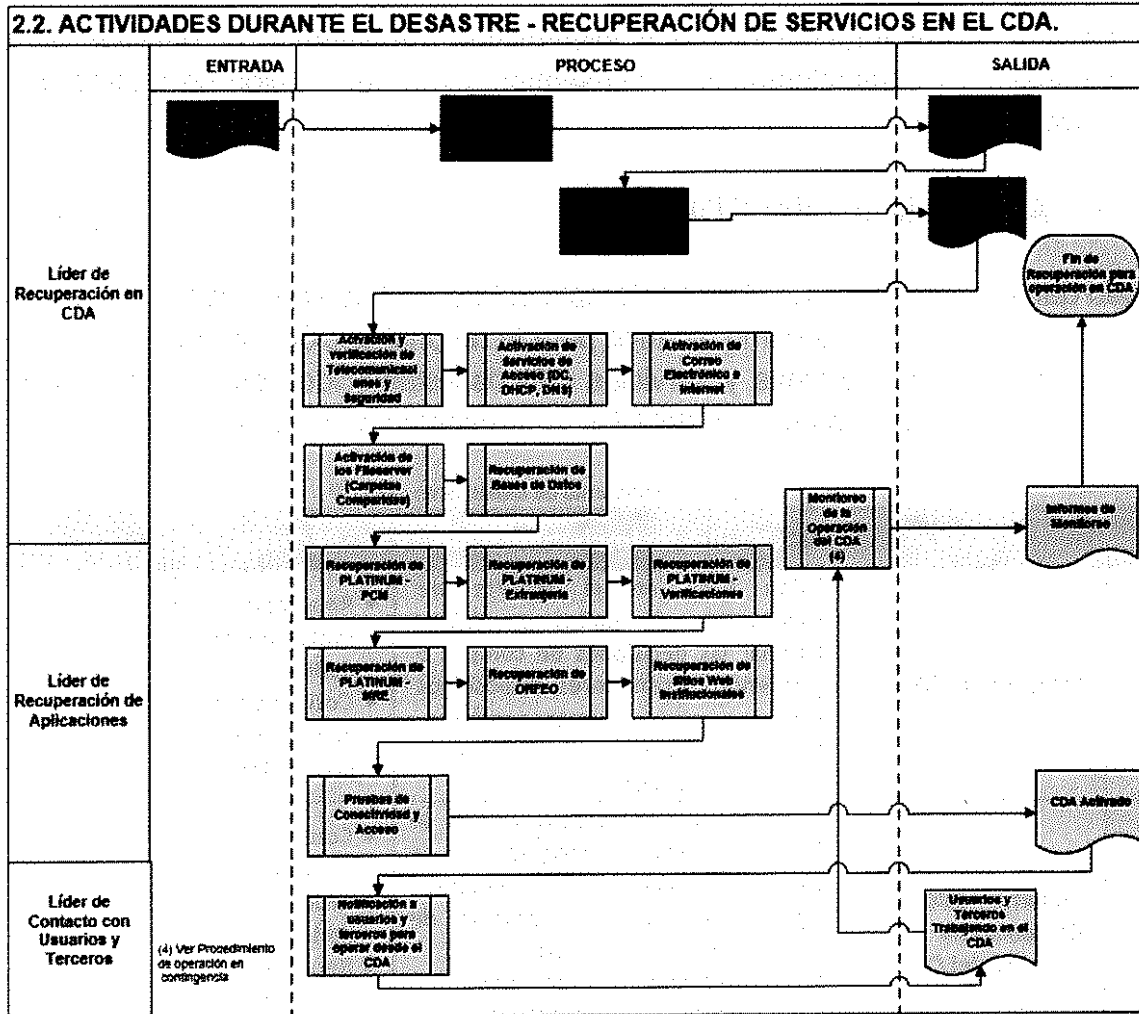
No.	Actividad	Detalles de implementación	Recursos	Responsable
		DHCP, DNS	DNS	Infraestructura en CDA
4.	Recuperación de seguridad del CDA	Se verifica la funcionalidad del firewall perimetral del CDA	<ul style="list-style-type: none"> Software de monitoreo de redes Procedimiento de recuperación de seguridad 	<ul style="list-style-type: none"> Soporte en redes y seguridad Líder de Recuperación de Infraestructura en CDA
5.	Recuperación de servidores de almacenamiento	Se recuperan y verifica la funcionalidad de los servidores de almacenamiento.	Plan de recuperación FILE SERVER	<ul style="list-style-type: none"> Soporte en almacenamiento Líder de Recuperación de Infraestructura en CDA
6.	Recuperación de correo electrónico	Se verifica la disponibilidad y funcionamiento del servicio de correo electrónico	Procedimiento técnico de activación del correo electrónico	<ul style="list-style-type: none"> Soporte en Correo Líder de Recuperación de Infraestructura en CDA
7.	Recuperación de Base de Datos	Se verifica la disponibilidad y funcionamiento de las bases de datos críticas (PCM, PLATINUM)	Procedimiento técnico de base de datos.	<ul style="list-style-type: none"> Soporte en Bases de Datos Líder de Recuperación de Infraestructura en CDA
8.	Recuperación PLATINUM - PCM	Se recuperan y verifica a funcionalidad de PLATINUM - PCM	Plan de recuperación de PLATINUM - PCM	<ul style="list-style-type: none"> Líder de Recuperación de Infraestructura en CDA Líder PLATINUM - PCM (la UAEMC)
9.	Recuperación PLATINUM - Extranjería	Se recuperan y verifica a funcionalidad de PLATINUM - Extranjería	Plan de recuperación de PLATINUM - Extranjería	<ul style="list-style-type: none"> Líder de Recuperación de Infraestructura en CDA Líder PLATINUM - Extranjería (la UAEMC)
10.	Recuperación PLATINUM - Verificaciones	Se recuperan y verifica a funcionalidad del servicio PLATINUM - Verificaciones	Plan de recuperación de PLATINUM - Verificaciones	<ul style="list-style-type: none"> Líder de Recuperación de Infraestructura en CDA Líder PLATINUM -

No.	Actividad	Detalles de Implementación	Recursos	Responsable
				Verificaciones (la UAEMC)
11.	Recuperación PLATINUM - SIRE	Se recuperan y verifica a funcionalidad del servicio de PLATINUM - SIRE	Plan de recuperación de PLATINUM - SIRE	<ul style="list-style-type: none"> • Líder de Recuperación de Infraestructura en CDA • Líder PLATINUM - SIRE (la UAEMC)
12.	Recuperación ORFEO	Se recuperan y verifica a funcionalidad del servicio de ORFEO	Plan de recuperación de ORFEO	<ul style="list-style-type: none"> • Líder de Recuperación de Infraestructura en CDA • Líder ORFEO (la UAEMC)
13.	Recuperación Sitios Web Institucionales	Se recuperan y verifica a funcionalidad del servicio de Sitios Web Institucionales	Plan de recuperación de Sitios Web Institucionales	<ul style="list-style-type: none"> • Líder de Recuperación de Infraestructura en CDA • Líder Sitios Web Institucionales (la UAEMC)
14.	Pruebas de conectividad de las aplicaciones	Dar acceso a usuarios remotos (sedes) y verificar la funcionalidad de las aplicaciones en el CDA	Chequeo básico de aplicaciones	Enlace con terceros (la UAEMC)
15.	Informe de activación del CDA	Informar al Líder de Recuperación en CDA la disponibilidad y funcionalidad del CDA (Centro de Datos Alterno).	Árbol de llamadas, teléfonos fijos, celulares	Líder de Recuperación de Infraestructura en CDA
16.	Notificar a usuarios la disponibilidad del CDA	Informar a los usuarios internos y externos la disponibilidad de los servicios en el CDA	Árbol de llamadas, teléfonos fijos, celulares	Enlace con terceros (Mesa de Ayuda - la UAEMC)
17.	Iniciar operaciones	Iniciar operaciones desde el CDA con los usuarios autorizados.		Líder de Recuperación de Infraestructura en CDA
18.	Monitorear el desempeño del CDA	Verificar el nivel de operación y calidad del servicio del CDA en todos sus aspectos: Volumen de trabajo, comunicaciones, almacenamiento,	Revisiones de la red Monitoreo de servidores	Líder de Recuperación de Infraestructura en CDA

No.	Actividad	Detalles de Implementación	Recursos	Responsable
		conectividad de terceros (proveedores y usuarios)		
19.	Copias de respaldo del CDA	Verificar disponibilidad de medios para obtención de backups y realización de los mismos. Envíos de medios a custodia.	<ul style="list-style-type: none"> • Sistema de copias • Medios magnéticos (cintas) 	Líder de Recuperación de Infraestructura en CDA
20.	Retorno de personal al CDP	Una vez normalizada la operación en el CDA se define que personal de la UAEMC queda allí y quienes regresan a apoyar la restauración del CDP	Informe de monitoreo del CDA	Líder de Recuperación de Infraestructura en CDA

La figura 7 presenta el diagrama de flujo del proceso de recuperación.

Figura 7. Actividades de recuperación de servicios en CDA



12. TAREAS DESPUÉS DEL DESASTRE (FASE DE RESTAURACIÓN)

La fase de restauración tiene como fin lograr el retorno a la normalidad, la cual se caracteriza por:

- 1) Todos los servicios que soportan los procesos críticos de la Entidad se encuentran listos para su utilización en el CDP.

- 2) El procesamiento finaliza en el CDA (se interrumpe el servicio del CDA) y se traslada al CDP.
- 3) La fase de restauración incluye el alistamiento (reconstrucción) del CDP para atender los requerimientos de procesamiento y la declaración de retorno a la normalidad.

12.1. Alistamiento del CDP

Dado que el alcance del DRP no contempla la totalidad de servicios tecnológicos de la UAEMC, se asume como alcance para la reconstrucción, dejar el CDP listo con, al menos, los sistemas y servicios críticos establecidos en el alcance del DRP. Las tareas de alistamiento del CDP se presentan en la tabla 6.

Tabla 6. Procedimiento de alistamiento del CDP

No.	Actividad	Detalles de Implementación	Recursos	Responsable
1	Dotación del CDP	Con base en el reporte de evaluación de daños se deben tomar las decisiones de compra o arriendo de servidores, dispositivos de almacenamiento, comunicaciones, seguridad, Hosting inclusive.	<ul style="list-style-type: none"> • Reporte de evaluación de daños • Cotizaciones de terceros proveedores. 	Líder de Restauración del CDP.
2	Implementación de elementos de cómputo del CDP	Con los diferentes proveedores se definen los cronogramas de implementación de elementos particulares y la integración de componentes y servicios. Es necesario contar con interventoría del proyecto de restauración del CDP.	<ul style="list-style-type: none"> • Contratos con terceros • Cronogramas de trabajo • Reportes de gerencia de proyectos. 	
3	Inspección de la infraestructura física	Se realiza la revisión de las obras físicas y se firma la aceptación de las mismas. En caso contrario se documentan las observaciones y se entregan al contratista respectivo. Se deben revisar: Muros, bajantes, acometidas eléctricas, ductos de aire y otros elementos físicos del CDP.	Archivo de Excel con el checklist de evaluación.	
4	Evaluación de la infraestructura de cómputo	Se realiza la revisión de las implementaciones de servidores, máquinas virtuales y sistemas de	Archivo de Excel con el checklist de	

No.	Actividad	Detalles de Implementación	Recursos	Responsable
		almacenamiento (SAN). Se firma el acta de aceptación de las mismas o en caso contrario se documentan las observaciones y se entregan al contratista respectivo.	evaluación Informes de pruebas.	
5	Evaluación del cableado estructurado	Se determina la funcionalidad de: <ul style="list-style-type: none"> ▪ Red local. ▪ Canales de internet del CDP. ▪ Canales WAN. ▪ Canales de replicación hacia el CDA. ▪ Firewall. ▪ Funcionamiento de las VLAN's. ▪ Sistema de telefonía. 	Archivo de Excel con el checklist de evaluación Informes de pruebas.	
6	Alistamiento de la infraestructura de cómputo	Se implementa y determina la funcionalidad de: <ul style="list-style-type: none"> ▪ Servidores físicos. ▪ Servidores virtuales. ▪ Sistemas de almacenamiento. ▪ Servicios críticos TIC. 	Guion de pruebas Informe de pruebas a los servicios críticos TIC.	
7	Informe de alistamiento del CDP	Emitir el reporte de alistamiento y recomendación del traslado de las operaciones al CDP.	Software de ofimática	

La figura 8, presenta las actividades de alistamiento del CDP

Tabla 7. Procedimiento de retorno a la normalidad

No.	Actividad	Detalles de Implementación	Recursos	Responsable
1	Definir fecha, hora y duración estimada para el traslado de operaciones al CDP.	<ul style="list-style-type: none"> Revisión del informe con las duraciones estimadas por actividad. Evaluación de fecha y hora más conveniente. Notificación a áreas usuarias de la suspensión del servicio. Notificación a terceros de la maniobra de traslado de operaciones. 	<ul style="list-style-type: none"> Plan de traslado. Árbol de llamadas. 	<ul style="list-style-type: none"> Líder DRP Líder de restauración del CDP Líder de recuperación de aplicaciones Enlace con terceros (Mesa de Ayuda)
2	Suspensión del servicio del CDA.	En la fecha y hora establecida se suspende el procesamiento en el CDA.	Software de monitoreo de redes.	Líder de restauración del CDP
3	Obtención de backups del CDA.	Se toman los respaldos totales de las aplicaciones e información procesada durante la contingencia en el CDA.	<ul style="list-style-type: none"> Medios magnéticos Software de backups 	Soporte de almacenamiento.
4	Restauración de información	La información procesada en el CDA se puede recuperar de dos maneras posibles: <ul style="list-style-type: none"> Restauración de backups Réplica cero del CDA 	<ul style="list-style-type: none"> Medios magnéticos Software de backups Sistema de replicación 	Líder en almacenamiento.
5	El CDA vuelve a modo pasivo.	El CDA de contingencia recupera la configuración normal de trabajo (activo para replicación, pasivo para	<ul style="list-style-type: none"> Configuraciones de telecomunicaciones y seguridad originales. 	Líder de restauración del CDP

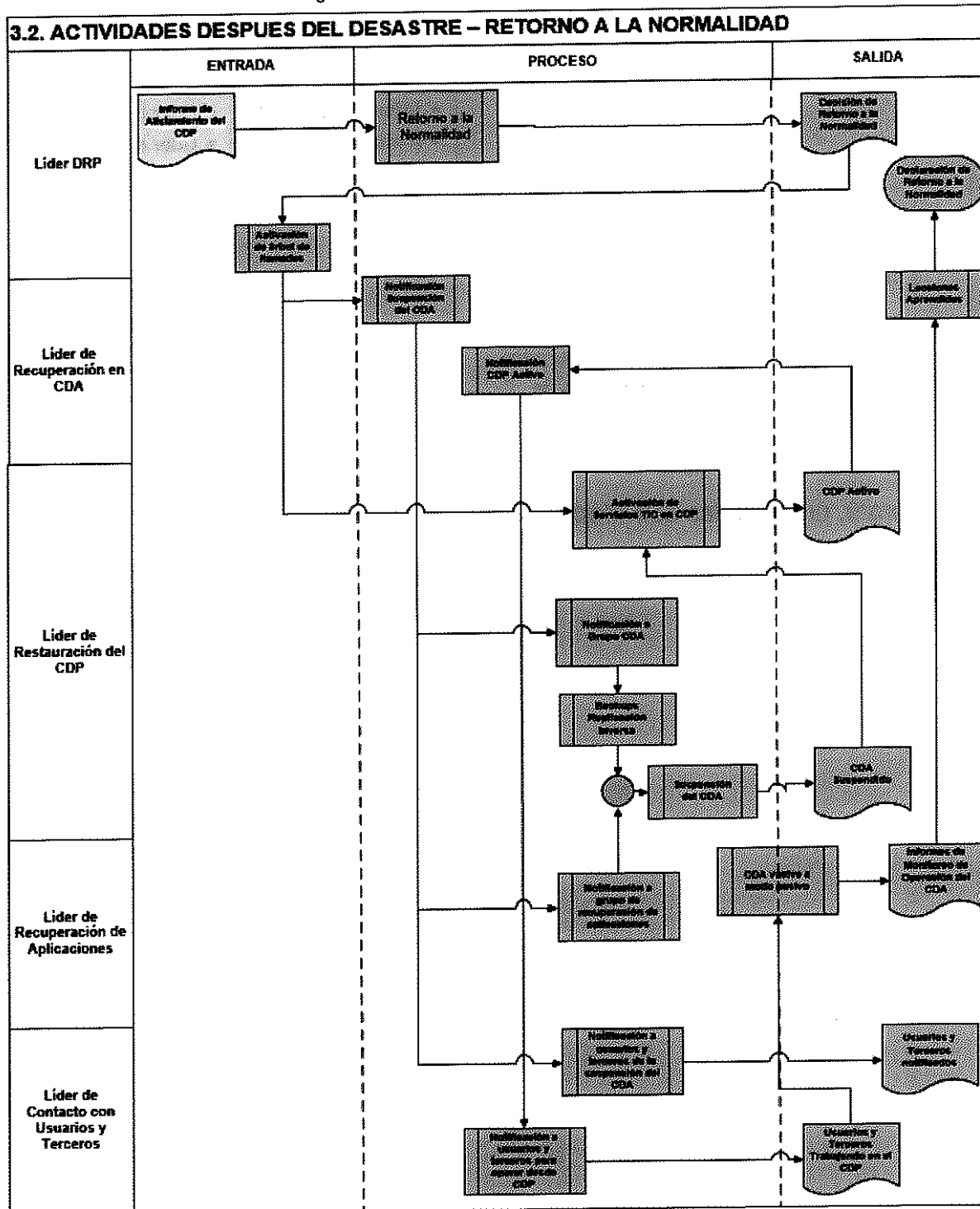
✍

No.	Actividad	Detalles de Implementación	Recursos	Responsable
		procesamiento)	<ul style="list-style-type: none"> • Configuraciones de replicación originales. 	
6	Pruebas de funcionalidad de las aplicaciones.	Solicitar a funcionales y algunos usuarios remotos la verificación del funcionamiento de las aplicaciones.	Diseño de pruebas de funcionalidad de aplicaciones.	Enlace con terceros (Mesa de Ayuda).
7	Notificar la funcionalidad del CDP	Informar a los usuarios internos, externos y proveedores la disponibilidad y funcionalidad del CDP.	<ul style="list-style-type: none"> • Árbol de llamadas • Teléfonos fijos • Celulares 	<ul style="list-style-type: none"> • Líder de restauración del CDP • Enlace con terceros (Mesa de Ayuda)
8	Iniciar operaciones en el CDP	Iniciar operaciones desde el CDP	Informe de avance del plan de retorno a la normalidad	<ul style="list-style-type: none"> • Líder DRP • Líder de restauración del CDP
9	Monitorear el desempeño del CDP	Verificar el nivel de operación y calidad del servicio del CDP en todos sus aspectos: Volumen de trabajo, comunicaciones, almacenamiento, conectividad de terceros proveedores, servicio a usuarios remotos.	Servicio de Monitoreo de red	<ul style="list-style-type: none"> • Líder en redes y comunicaciones • Líder de restauración del CDP
10	Normalización en el respaldo de datos	Aplicar la política de replicación y toma de backups en el CDP	<ul style="list-style-type: none"> • Sistema de copias • Medios magnéticos (cintas) 	Líder de restauración del CDP
11	Declarar el fin de la contingencia	Revisar informes de monitoreo del CDP Notificar a los funcionarios terceros y equipos de recuperación la finalización	Árbol de llamadas, teléfonos fijos, celulares	Líder DRP

No.	Actividad	Detalles de Implementación	Recursos	Responsable
		de la contingencia y declarar el retorno a la normalidad		
12	Lecciones aprendidas	Solicitar reunión con los líderes participantes en la ejecución del DRP Solicitar a los asistentes los puntos de mejora del DRP Definir acciones correctivas Solicitar el ajuste a los procedimientos de recuperación	<ul style="list-style-type: none"> • Salón de reuniones • Anotaciones hechas durante la ejecución del DRP 	<ul style="list-style-type: none"> • Líder DRP • Líder de restauración del CDP

La figura 9, presenta las actividades de retorno a la normalidad.

Figura 9. Actividades de retorno a la normalidad



14. RIESGOS DE ACTIVAR LA OPERACIÓN EN EL CDA

En la siguiente tabla se incluyen los riesgos de operación del CDA, los cuales deben ser analizados de manera conjunta por el Líder del DRP y el Jefe de la Oficina de Tecnología de la Información de la UAEMC, para su debido tratamiento y mitigación.

Tabla 8. Riesgos de Activar el CDA

# Ítem	Descripción del Riesgo	Falla - Causas (amenaza y/o vulnerabilidad)	Probabilidad	Impacto	Nivel de riesgo inherente	# Control	Control Actual	Nivel de riesgo residual
R1	Problemas de conectividad	Falla de alguno de los Switches en CDA.	2	5	Medio	Alto	Mantener actualizados, Switches.	
		Falla de puertos en Switch de CDA.	2	5	Medio	Alto	Se debe analizar los logs de los switches de CDA para identificar y corregir falla, mantener en monitoreo periódico.	
R2	Máquinas virtuales no disponibles.	Falla o mal funcionamiento de los recursos de telecomunicaciones.	2	5	Medio	Alto	Mantenimiento preventivo. Monitoreo de redes e Acuerdos de RMA con fabricantes. Respaldo de configuraciones.	
		Imposibilidad de conexión del administrador vía VPN en el momento del incidente.	2	5	Medio	Alto	Instalación del software cliente VPN en los usuarios autorizados previamente. Definir un sitio para la descarga del software VPN cliente junto con las instrucciones de instalación y	

A

# Ítem	Descripción del Riesgo	Falla - Causas (amenaza y/o vulnerabilidad)	Probabilidad	Impacto	Nivel de riesgo inherente	# Control	Control Actual	Nivel de riesgo residual
							conexión a los aplicativos.	
R3	Personal no capacitado	Personal no capacitado para el inicio de los servidores / servicios. Personal sin conocimiento del plan de recuperación ante desastres. Personal sin participación previa en pruebas / simulacros.	3	5	Medio	Medio	Documentación del levantamiento Divulgación del DRP en la UAEMC.	Medio
R4	Data incorrecta	Archivos corruptos o mal copiados en la réplica del servidor BD. Diferentes versiones de Platinum –PCM en Puestos de Control Migratorio.	2	5	Medio	Alto	Monitoreo periódico de la plataforma de replicación. Inventario actualizado de versiones en Puestos de Control Migratorio a nivel nacional.	Bajo
R5	Backups desactualizados	Cintas con datos demasiado antiguos	3	5	Medio	Alto	Se tienen backups digitales actualizados. Validación de los RPO de los servidores en caso de pérdida total.	Bajo
R6	Cambios sobre la infraestructura no replicados al CDA	Ausencia de control y replicación de cambios en el CDA.	3	5	Medio	Alto	Mantener procedimientos de control y replicación de cambios hacia el CDA.	Bajo
R7	El CDA queda como CDP	El desastre deja totalmente destruido el CDP y su	2	5	Medio	Alto	Se tiene un Plan de Recuperación	Medio

# ítem	Descripción del Riesgo	Falla - Causas (amenaza y/o vulnerabilidad)	Probabilidad	Impacto	Nivel de riesgo inherente	# Control	Control Actual	Nivel de riesgo residual
		reconstrucción toma más tiempo de lo estimado.					de desastres. Negociación con terceros para adecuación del CDP. Aprovechamiento de infraestructura en CDA para brindar servicios no cubiertos por el DRP.	
R8	Imposibilidad de activar el DRP por los mecanismos contemplados.	Se presenta una falla generalizada de telecomunicaciones que imposibilita las llamadas telefónicas, el uso de mensajería y/o redes sociales.	1	5	Medio	Alto	Se cuenta con la información de contacto necesaria del personal que conforma el DRP (# Teléfono 1, # Teléfono 2, Mail 1, Mail 2, Dirección de Residencia)	Medio

15. PROCEDIMIENTOS TÉCNICOS

El Plan de Recuperación de Desastres se soporta en la aplicación de los procedimientos técnicos que se listan a continuación:

Tabla 9. Procedimientos técnicos que soportan el DRP

Tipo	Procedimiento	Responsable
Servicios de Tecnología	Procedimiento Recuperación Bases de datos (Misional)	Administrador de base de datos
	Procedimiento Recuperación Correo	Administrador de infraestructura
	Procedimiento Recuperación DNS	Administrador de infraestructura
	Procedimiento Recuperación Dominio	Administrador de infraestructura
	Procedimiento Recuperación PLATINUM - SIRE	Líder de implementaciones
	Procedimiento Recuperación PLATINUM - Verificaciones	Líder de implementaciones
	Procedimiento Recuperación PLATINUM - Extranjería	Líder de implementaciones

Tipo	Procedimiento	Responsable
	Procedimiento Recuperación PLATINUM - PCM	Líder de implementaciones
	Procedimiento Recuperación ORFEO	Líder de implementaciones

16. GLOSARIO

- **Acción Correctiva:** Acción para eliminar la causa de una no conformidad y prevenir la recurrencia.
- **Actividad:** Procesos o conjunto de procesos emprendido por la organización que desarrollan o soportan uno o más productos y servicios.
- **Actividades priorizadas:** Actividades que deben ser priorizadas siguiente a un incidente con el fin de mitigar los impactos.
- **Acuerdos de ayuda mutua:** Entendimiento entre dos o más entidades para hacer o brindar asistencia a los demás.
- **Administración de la continuidad de negocios:** Proceso holístico gerencial que identifica las amenazas potenciales en la organización y el impacto de dichas amenazas en las operaciones si se llegasen a dar. Persigue mejorar la resiliencia para establecer la capacidad de la empresa para construir la capacidad de una respuesta efectiva a la salvaguarda de los intereses de las partes involucradas, reputación, marca y actividades para crear valor.
- **Análisis de Impacto en el Negocio (BIA):** Proceso de análisis de actividades y efecto que en un negocio podría tener sobre ellas la interrupción de procesos.
- **Apetito de Riesgo:** Monto de riesgo que una organización acepta o retiene.
- **Conformidad:** Cumplimiento de un requerimiento
- **Continuidad de Negocios:** capacidad de la organización para continuar desarrollando los productos o servicios en un nivel aceptable predefinidos, posterior a un incidente.
- **Ejercicio:** Procesos de entrenamiento para evaluar, practicar e implementar mejoras en una organización.
- **Evaluación de desempeño:** Proceso para determinar los resultados de la medición.
- **Evaluación de Riesgo:** Cubrimiento de los procesos de identificación, análisis y evaluación de riesgos.

- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.
- **Incidente:** Situación que puede ser o podría dar lugar a una interrupción, pérdidas, emergencias o crisis.
- **Infraestructura:** Sistemas, equipos y servicios necesarios para la operación de una organización.
- **Mejora Continua:** Actividades recurrentes para desarrollar la mejora.
- **Monitoreo:** Determinación del estado de un sistema, un proceso o una actividad.
- **No conformidad:** No cumplir con un requerimiento.
- **Partes Interesadas:** Personas u organizaciones que pueden resultar afectadas o afectar a ellos mismos o a un tercero por alguna decisión respecto a una actividad.
- **Plan de continuidad de negocios:** Procedimiento documentado que guía a la organización para responder, recuperar y restaurar a un nivel predefinido los niveles de la operación de la compañía tras una interrupción de la operación.
- **Política:** Intenciones y dirección de una organización expresada formalmente por la alta dirección.
- **Procedimiento:** Vía específica para llevar una actividad o un proceso.
- **Proceso:** Conjunto de actividades interrelacionadas en las que se transforman entradas en salidas.
- **Productos y Servicios:** Beneficio que provee una organización para sus clientes, proveedores y partes interesadas.
- **Programa de continuidad de negocios:** Gestión continua y procesos de gobierno corporativo soportados por la alta dirección y utilizando recursos de forma apropiada para implementar y mantener la gestión de la continuidad de negocios.
- **Pruebas:** Procedimiento para evaluar el SGCN
- **Recursos:** Todos los activos, personas, habilidades, información, tecnología, premisas, proveedores, que una organización ha tenido disponible para su uso, cuando lo necesitó, alineado con la operación y el cumplimiento de los objetivos.
- **Requerimiento:** necesidad o expectativa que es fijada, generalmente implica obligatoriedad.
- **Riesgo:** Efecto de un evento sobre los objetivos.

X




GUÍA PARA RECUPERACIÓN DE DESASTRES

Fecha: **12 SET. 2016**

Código:
AGTG.09 (v3)

Página 40 de 45

- **Tercerizar:** Forma de establecer que una entidad externa desarrolle parte de las funciones, procesos u operación de una organización.

	GUÍA PARA RECUPERACIÓN DE DESASTRES	Fecha: 12 SET. 2016
		Código: AGTG.09 (v3)
		Página 41 de 45

17. ANEXOS

ANEXO A

APROBACIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES

Como responsable de la Oficina de Tecnología de la Información de la UAEMC, por la presente certifico que el Plan de Recuperación de Desastres (DRP por sus siglas en inglés) es completo, y que la información contenida en este documento proporciona una representación precisa de las aplicaciones, el hardware, software, componentes de telecomunicaciones y terceros proveedores necesarios para la prestación de nuestros sistemas de información y servicios tecnológicos en el CDA (Centro de Datos Alterno).

También certifico que la estrategia de recuperación seleccionada e implementada proporcionará la capacidad de recuperar la funcionalidad de los sistemas con el método más conveniente y a una relación costo – beneficio acorde con la criticidad de los mismos en lo que respecta al logro de los objetivos de la UAEMC.

Adicionalmente manifiesto que el presente Plan de Recuperación de Desastres será probado por lo menos una vez al año. Este plan fue probado para su aceptación el dd/mm/aa. La documentación relacionada con las pruebas se encuentra en el repositorio de información definido. Este documento será modificado cuando se produzcan cambios y se mantendrá bajo control de versiones, de acuerdo con la política de gestión documental de la UAEMC.

Jefe de la Oficina de Tecnología de la Información

Fecha:



GUÍA PARA RECUPERACIÓN DE DESASTRES

Fecha: **12 SET. 2016**

Código:
AGTG.09 (v3)

Página 42 de 45

ANEXO B

A continuación, se presenta la información de contacto de todo el personal que hace parte del DRP en la UAEMC.

Rol	Cargo	Nombre	Teléfono 1	Teléfono 2	e-Mail 1	e-Mail 2	Dirección Física
Líder DRP							
Líder Alterno DRP							
Consultor DRP							
Líder de Recuperación de Infraestructura en CDA							
Líder Alterno de Recuperación de Infraestructura en CDA							
Soporte Windows y Virtualización							
Soporte Alterno Windows y Virtualización							
Soporte Linux							
Soporte Alterno Linux							
Soporte Almacenamiento							
Soporte Almacenamiento							
Soporte Base de Datos							
Soporte Alterno de Base de Datos							
Soporte Redes y Seguridad							
Soporte Alterno Redes y Seguridad							
Soporte Monitoreo y Gestión							
Soporte Alterno Monitoreo y Gestión							
Enlace con usuarios y terceros (Mesa de Ayuda)							

GUÍA PARA RECUPERACIÓN DE DESASTRES

Fecha: **12 SET. 2016**

Código:
AGTG.09 (v9)

Página 43 de 45

Rol	Cargo	Nombre	Teléfono 1	Teléfono 2	e-Mail 1	e-Mail 2	Dirección Física
Enlace Backup con usuarios y terceros (Mesa de Ayuda)							
Enlace Telefónica (la UAEMC)							
Enlace de backup Telefónica (la UAEMC)							
Líder de recuperación de aplicaciones en el CDA							
Backup Líder de recuperación de aplicaciones en el CDA							
Líder del Sistema PLATINUM - PCM							
Backup Líder del Sistema PLATINUM - PCM							
Líder del Sistema PLATINUM - Extranjería							
Backup Líder del Sistema PLATINUM - Extranjería							
Líder del Sistema PLATINUM - Verificaciones							
Backup Líder del Sistema PLATINUM - Verificaciones							
Líder del Sistema PLATINUM - SIRE							
Backup Líder del Sistema PLATINUM - SIRE							
Líder del Sistema ORFEO							
Backup Líder del Sistema ORFEO							
Líder de Restauración del CDP							



GUÍA PARA RECUPERACIÓN DE DESASTRES

Fecha: **12 SET. 2016**

Código:
AGTG.09 (V3)

Página 44 de 45

Rol	Cargo	Nombre	Teléfono 1	Teléfono 2	e-Mail 1	e-Mail 2	Dirección Física
Backup Líder de Restauración del CDP							
Líder Recuperación de Infraestructura Física							
Backup Recuperación de Infraestructura Física							
Líder Recuperación de Telecomunicaciones Y Seguridad							
Backup Recuperación de Telecomunicaciones Y Seguridad							
Líder Recuperación de Servidores							
Backup Recuperación de Servidores							
Líder Recuperación de Datos (Almacenamiento)							
Backup Recuperación de Datos (Almacenamiento)							
Líder Recuperación de servicios tecnológicos críticos							
Backup Recuperación de servicios tecnológicos críticos							
Líder Recuperación de Sistemas de información							
Backup Recuperación de Sistemas de información							
Líder Recuperación de Sistemas de información Y							



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

© 2011



GUÍA PARA RECUPERACIÓN DE DESASTRES

Fecha: **12 SET. 2016**

Código:
AGTG.09 (v3)

Página 45 de 45

Rol	Cargo	Nombre	Teléfono 1	Teléfono 2	e-Mail 1	e-Mail 2	Dirección Física
servicios tecnológicos No Críticos							
Backup Recuperación de Sistemas de información y servicios tecnológicos No Críticos							

(Handwritten mark)

