PLAN DE CONTINUIDAD Y CONTINGENCIA PARA LOS SISTEMAS DE INFORMACION

MODELO DE ARQUITECTURA EMPRESARIAL (MAE)

CORPORACION PARA EL DESARROLLO SOSTENIBLE DEL NORTE Y EL ORIENTE AMAZÓNICO -CDA-

Inírida– Guainía

2026

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

TABLA DE CONTENIDO

Contenido

INTRODUCCION. 4
Enfoque del Plan 4
Objetivos Clave 4
OBJETIVOS. 5
VENTAJAS. 6
ALCANCE. 6
METODOLOGIA. 7
El Plan se ha estructurado en tres grandes Fases: 8
IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS 9
DEFINICIÓN 9
DESCRIPCIÓN Y ANÁLISIS DE RIESGOS 9
CAUSAS EXTERNAS QUE CONLLEVAN A RIESGOS. 10
CAUSAS INTERNAS QUE CONLLEVAN A RIESGOS. 11
IDENTIFICACION DE PROCESOS CRITICOS. 13
CRITERIOS PARA IDENTIFICACIÓN DE PROCESOS CRÍTICOS 13
NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECURSOS INFORMÁTICOS 13
PROCESOS CRÍTICOS 14
SOFTWARE 14
HARDWARE. 15
EQUIPOS DE COMUNICACIONES 16
DEFINICIÓN Y CONFORMACIÓN DEL GRUPO DE TRABAJO 16
PLAN DE MITIGACIÓN 19
PROCESO DE RESPALDO 19
DEFINICIÓN DE NIVELES DE BACKUP 20
CENTRO DE DATOS (DATA CENTER) 21
FASE DE EMERGENCIA. 22
SOFTWARE. 22
HARDWARE. 23
FASE DE RECUPERACION. 24

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

PREPARACIÓN REQUERIDA PARA RECUPERACIÓN DE DESASTRES 25
RECUPERACION DEL DESASTRE: PLAN DE ACCION 26
PRIMERA FASE. 26
SEGUNDA FASE. 27
TERCERA FASE 29
CUARTA FASE 30
QUINTA FASE 31
IMPLEMENTACIÓN DEL PLAN 31
PLAN DE PRUEBAS EXPERIMENTALES 32
RESPONSABILIDADES Y METODOLOGÍA DE PRUEBAS 33
PASOS PARA LA EJECUCIÓN DE PRUEBAS 33
AREAS O PARTES A PROBAR 34
COMPONENTES A EVALUAR EN LAS PRUEBAS 34
POLÍTICAS DE SEGURIDAD 36
POLÍTICAS DE SEGURIDAD DE INFORMACIÓN 36
REINICIALIZAR O RESTAURAR SU SISTEMA 36
PANTALLA EN BLANCO (PROTECCIÓN DE INFORMACIÓN) 37
GESTIÓN DE BACKUPS Y RECUPERACIÓN DE DATOS 37
ARCHIVO DE INFORMACIÓN: DIRECTRICES CLAVE 37
ENVÍO DE CORREOS ELECTRÓNICO INSTITUCIONAL 38
CONCLUSIONES 39

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

INTRODUCCION.

La Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA) reconoce que la información es el activo más valioso de toda institución. Por ello, implementa medidas de seguridad robustas para su protección y se prepara ante posibles contingencias o desastres que puedan afectar su operatividad.

El presente **Plan de Contingencias para los Sistemas de Información** tiene como objetivo garantizar la continuidad de las operaciones automatizadas, minimizando el impacto en la organización y asegurando el cumplimiento de su misión institucional.

Enfoque del Plan

Este plan se basa en un **proceso dinámico y continuo**, que abarca no solo las acciones a ejecutar durante una interrupción en el procesamiento de datos, sino también las medidas preventivas para anticiparse a dichos eventos.

Objetivos Clave

1. **Evaluar, mantener y mejorar** los procedimientos de recuperación, con el fin de mitigar riesgos potenciales antes de que ocurra un desastre.
2. **Facilitar la recuperación efectiva** en caso de un incidente, mediante una fase estructurada que cumpla tres propósitos esenciales:
    - **Claridad de roles**: Definir y comunicar las responsabilidades de ejecución, coordinación y toma de decisiones dentro del plan.
    - **Procedimientos documentados**: Establecer y actualizar protocolos detallados para actuar ante eventos inesperados.
    - **Revisión continua**: Evaluar la eficiencia y precisión de cada proceso, ajustando los procedimientos de recuperación según sea necesario.

El Plan de Contingencias servirá como hoja de ruta para la CDA, integrando los siguientes componentes:

- Definición de escenarios potenciales y sus impactos.
- Diseño de estrategias de almacenamiento y recuperación de datos.
- Gestión integral del Plan, incluyendo roles, responsabilidades y recursos.
- Implementación de procedimientos contingentes, con la participación activa de usuarios, administradores y grupos de trabajo especializados.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

OBJETIVOS.

1. **Establecer protocolos y recursos mínimos:** Dotar a la **Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA)** de los procedimientos y herramientas necesarios para responder ante contingencias que provoquen la interrupción de actividades o la inoperatividad de equipos por causas de fuerza mayor.

2. **Garantizar la continuidad operativa de los sistemas críticos:** Implementar soluciones que mantengan funcionales los sistemas de información y electrónicos esenciales**,** minimizando el impacto en las operaciones institucionales ante interrupciones parciales o totales en las instalaciones de procesamiento de datos.

3. **Evaluar riesgos y cuantificar potenciales pérdidas:** Identificar y medir la exposición a pérdidas asociadas a cada sistema automatizado y recurso informático, facilitando un análisis de riesgos detallado que oriente la ejecución del plan.

4. **Mitigar impactos financieros y operativos:**
    - Reducir pérdidas mediante procedimientos de recuperación ágiles y eficaces**.**
    - Minimizar las consecuencias de la pérdida de información mediante estrategias de respaldo confiables**,** manteniendo un nivel de riesgo aceptable.

5. **Asegurar la prestación continua de servicios:** Mantener un nivel de servicio adecuado para los usuarios, incluso durante situaciones de contingencia.

6. **Recuperar el Centro de Datos en tiempo óptimo:** Restablecer las operaciones en el menor plazo posible, adaptando la respuesta según la naturaleza y gravedad de la anomalía presentada.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

VENTAJAS.

Contar con un plan de contingencias estructurado para los sistemas de información y las TIC de la Corporación CDA ofrece múltiples beneficios, permitiendo prevenir, mitigar y responder eficazmente ante posibles siniestros. Entre sus principales ventajas destacan:

1. Reducción de vulnerabilidades
   Implementación de acciones preventivas basadas en el conocimiento de los sistemas automatizados, minimizando riesgos operativos.
2. Identificación y cuantificación de riesgos
   Evaluación de amenazas potenciales que afectan la integridad, disponibilidad y confidencialidad de la información institucional.
3. Agilidad en la toma de decisiones
   Respuesta oportuna y eficiente ante fallas técnicas o anomalías, reduciendo tiempos de inactividad.
4. Cultura organizacional de seguridad
   Promoción de buenas prácticas en el manejo seguro de la información, fortaleciendo la conciencia institucional en ciberseguridad.
5. Continuidad operativa
   Garantía de estabilidad técnica y funcional de la corporación, incluso ante incidentes críticos.
6. Evaluación de la seguridad
   Medición objetiva del nivel de protección de los sistemas de información, facilitando mejoras continuas.
7. Minimización de impactos
   Mitigación de daños por siniestros electrónicos, evitando pérdida de datos, deterioro de equipos y afectaciones económicas o reputacionales.

ALCANCE.

Este plan de contingencias se desarrolla para mitigar el impacto operativo generado por la interrupción parcial o total de los servicios electrónicos y el procesamiento de información en la Corporación CDA, garantizando la continuidad de sus actividades críticas.

Cobertura del Plan

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

1. Ámbito Técnico
    - Actuaciones sobre hardware, software y equipos electrónicos vinculados a procesos críticos definidos en el plan.
    - Gestión de riesgos asociados al Centro de Datos, incluyendo su infraestructura física y operativa.
2. Responsabilidades
    - Procedimientos asignados a los grupos contingentes, con base en sus funciones y competencias.
    - Coordinación con las dependencias, bajo los recursos disponibles (capacitación, soporte técnico, presupuesto, etc.).

METODOLOGIA.

Dado que las operaciones críticas de la Corporación CDA dependen del soporte de las Tecnologías de la Información (TIC), la gestión efectiva de estos sistemas es fundamental para garantizar la continuidad operativa. Para ello, se han considerado los siguientes aspectos claves:

1. Tolerancia al Tiempo de Inactividad
    - Evaluación del período máximo en que la entidad puede operar sin sus recursos computacionales, minimizando impactos en los procesos institucionales.
2. Identificación de Amenazas
    - Análisis de riesgos potenciales que afecten la capacidad de procesamiento automatizado de información, con el fin de priorizar medidas de mitigación.
3. Aplicaciones Críticas
    - Determinación de los sistemas y aplicaciones esenciales que deben mantenerse operativos durante una contingencia, asegurando la continuidad de servicios prioritarios.
4. Impacto Operativo y Legal
    - Evaluación de las consecuencias derivadas de interrupciones en los servicios automatizados, incluyendo efectos operativos, estratégicos, legales y en la atención al usuario.
5. Inversión en Resiliencia
    - Justificación de los recursos asignados al plan de contingencias, garantizando su efectividad para preservar la operatividad y estabilidad institucional.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

El Plan se ha estructurado en tres grandes Fases:

1) **Fase de Mitigación:** la corporación CDA, asegura la conservación de su información vital y determina donde procesar sus trabajos críticos de procesamiento de datos, sistemas o aplicaciones automáticas críticas, en caso de falla de sus equipos o de los mismos aplicativos.

2) **Fase de Emergencia:** Contiene las acciones detalladas que deben ser llevadas a cabo durante el siniestro o emergencia.

3) **Fase de Recuperación:** Permite restablecer las condiciones originales y operación normal de los sistemas de información en su conjunto.

Los cuales implican el desarrollo de las siguientes Etapas:

1) **Revisión:** comprende la determinación de vulnerabilidad del área, inventario de recursos y limitaciones de la misma.

2) **Evaluación del impacto por interrupción del servicio:** comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones. Esta evaluación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla el análisis de riesgos.

3) **Implementación:** se realizan actividades específicas para la reducción y eliminación de riesgos que proponen las medidas de acción, en caso de presentarse alguna situación de emergencia.

a). **Cronograma:** El diseño de un cronograma de trabajo provee la oportunidad de registrar los logros de cada tarea, verificar si las actividades han sido cumplidas o no en el tiempo previsto, y analizar cuáles han sido los principales inconvenientes que se han presentado si se detectan desviaciones importantes en el cronograma inicial, antes de la ejecución de las pruebas.

b). **Documentación:** Se prepararán y archivarán todos los documentos donde se registren las actividades, logros e inconvenientes, programas, objetivos, cronograma, procedimientos, planillas y todo aspecto fundamental referente a las acciones generadas durante el desarrollo del Plan de Contingencias, creando un historial de referencia.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

4) **Ejecución:** se sigue el desarrollo de:

a) Medidas de protección planificadas por cada segmento afectado.

b) Iniciación de las acciones destinadas, por prioridad, a controlar la situación durante los primeros instantes de la emergencia.

c) Consideración de las responsabilidades extraordinarias que el comité directivo del plan tendría que asumir a fin de ofrecer protección y seguridad a los elementos materiales y humanos del área.

d) Evaluación del estado del área de informática, poniendo en operación los procedimientos planificados para la recuperación total del servicio.

IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

DEFINICIÓN

Riesgo es la posibilidad de que una amenaza explote una vulnerabilidad, generando un daño o pérdida en un activo de información. Según la [ISO 9001], se define como la combinación de la probabilidad de que ocurra un evento y sus consecuencias.

En términos generales, el riesgo representa:

- La probabilidad de que suceda un evento inesperado.
- La proximidad a un daño potencial, contingencia o peligro.
- Un factor de incertidumbre, azar o exposición a situaciones adversas.

DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

El presente análisis de riesgos evalúa el impacto por interrupción del servicio**,** considerando las pérdidas asociadas a una suspensión parcial o total de las operaciones. Esta valoración abarca no solo las consecuencias financieras, sino también operativas, reputacionales y legales derivadas de dicha interrupción.

En esta fase, se examinan:

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Probabilidad de ocurrencia**: Frecuencia estimada de materialización del riesgo.
- **Posibilidades de mitigación**: Medidas para reducir la exposición o el impacto.
- **Nivel de impacto**: Severidad del daño potencial (económico, operativo o estratégico).
- **Alternativas de corrección**: Acciones correctivas y preventivas para gestionar la anomalía.

Entre los **riesgos potenciales** que podrían comprometer la continuidad operativa y la estabilidad de los sistemas de información de la Entidad, se incluyen:

CAUSAS EXTERNAS QUE CONLLEVAN A RIESGOS.

1. Riesgos Políticos

Descripción: Cambios en el marco legal y administrativo debido a modificaciones constitucionales (asamblea constituyente, referendo, consulta popular, plebiscito o leyes orgánicas), así como reestructuraciones o supresión de entidades.
Impacto: Alteraciones en la operatividad, mandatos legales o estructura organizacional.
Mitigación: Monitoreo constante del entorno normativo y planes de adaptación ante reformas.

2. Fallas en el Flujo de Energía Eléctrica

Descripción: Interrupciones en el suministro eléctrico por factores externos fuera del control de la Entidad.
Impacto: Parálisis temporal de operaciones críticas.
Mitigación: Implementación de equipos de respaldo (UPS, generadores) para reducir el impacto de cortes temporales.

3. Fallas en el Servicio Telefónico o Red Móvil

Descripción: Interrupciones en los servicios de comunicación por fallas externas de los proveedores.
Impacto: Bajo, dado que la Entidad cuenta con infraestructura alternativa de comunicación (redes locales y datos).
Mitigación:

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Planificación de soluciones temporales (aplicaciones de mensajería alternativa, redes redundantes).
- Coordinación con proveedores para garantizar la rápida restauración del servicio.

CAUSAS INTERNAS QUE CONLLEVAN A RIESGOS.

1. **Incumplimiento.**
   Este riesgo puede materializarse debido a posibles retrasos en la ejecución o incumplimiento de las cláusulas de los contratos de actualización, modificación y mantenimiento de las plataformas, aplicativos y/o programas de la corporación CDA, adquiridos durante su vigencia. Los sistemas afectados incluyen:

- Pimisys
- Sistema de Gestión Documental
- Banco de Proyectos
- Página Web
- SIG (Sistema de Información geográfica)
- Correos electrónicos

2. **Posibles retrasos en procesos administrativos**

La implementación de los procesos tecnológicos asociados a los contratos requiere trámites administrativos con requisitos estrictos, lo que podría prolongar inesperadamente los plazos de ejecución del Plan Emergente.

3. **Adquisición sin asesoramiento técnico, que deriva en soluciones inadecuadas o incompatibles con los requisitos y recursos disponibles.**

Esto se debe a deficiencias en los procesos de análisis, evaluación, planificación y toma de decisiones para seleccionar las alternativas tecnológicas a implementar, así como a un posible desconocimiento de las características técnicas y especificaciones requeridas en cada solución, las cuales deben ser compatibles con los recursos disponibles.

4. **Posible pérdida de información**

Aunque este riesgo tiene una baja probabilidad de ocurrencia, el Plan de Contingencias lo mitiga mediante un proceso de respaldo (backup) que cubre:

- Archivos de trabajo (*Word, Excel, PowerPoint*, etc.).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Bases de datos y resultados de aplicaciones en producción.
- Información crítica de todas las dependencias de la Entidad.

5. **Posibles fallas en el suministro eléctrico**

Origen del riesgo:

- **Fallas en equipos de respaldo:**
  - UPS (Unidades de Energía Ininterrumpida) sin mantenimiento preventivo, lo que compromete su funcionamiento.
  - Plantas eléctricas sin garantía de operatividad ante cortes prolongados.
- **Infraestructura eléctrica vulnerable:**
  - Cableado en mal estado o redes internas deterioradas.

Impacto:
Puede provocar pérdida de información crítica por interrupciones repentinas en el suministro eléctrico.

6. **Posible calentamiento en la sala de cómputo**

Nivel de riesgo: Bajo (mitigado por controles existentes)

Medidas de mitigación implementadas:

- **Sistema de control climático en el centro de datos:**
  - Aire acondicionado especializado que mantiene temperatura estable
  - Monitoreo constante de condiciones ambientales

Efectividad:
Los equipos operan dentro de los rangos térmicos óptimos gracias a esta infraestructura.

7. **Posible Falla del Servicio Telefónico o red móvil.**

Este riesgo está relacionado con amenazas externas al control de la Entidad, la Corporación CDA no puede efectuar mitigación de este riesgo. Sin embargo, se puede planear las posibles alternativas a implementar ante las posibles fallas del servicio telefónico o red movil. La probabilidad de ocurrencia sólo es manejable por la entidad proveedora del servicio. El impacto sobre las operaciones de la Corporación es de nivel

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

bajo, ya que la Entidad posee una Infraestructura de Comunicación de datos y Redes locales.

IDENTIFICACION DE PROCESOS CRITICOS.

CRITERIOS PARA IDENTIFICACIÓN DE PROCESOS CRÍTICOS

Los planes de contingencia se consideran:

- "requeridos" para todos los sistemas de **prioridad 1,**
- "recomendables" para todos los sistemas de **prioridad 2**
- "sugeridos" para todos los sistemas de **prioridad 3.**

Prioridad 1.

Todos los sistemas vitales de la organización.

Prioridad 2.

- Sistemas con múltiples interfaces.
- Sistemas o dispositivos que no pueden ser sometidos a pruebas.
- Sistemas que alimentan datos a los sistemas vitales.

Prioridad 3.

- Sistemas cuya falla causa molestias menores.

NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECURSOS INFORMÁTICOS

La Corporación CDA ha clasificado sus recursos tecnológicos según su impacto operativo, definiendo tres niveles de prioridad:

PRIORIDAD

- **Prioridad Alta (Críticos)**

Recursos: Sistemas cuya falla o inadaptación paralizaría las operaciones misionales de la corporación.
Ejemplos: Plataformas centrales de gestión, sistemas transaccionales o herramientas sin alternativas operativas.

- **Prioridad Media (Esenciales)**

Recursos: Herramientas importantes para actividades administrativas y operativas, pero con procedimientos alternativos predefinidos.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Ejemplos: Sistemas de reportes internos, herramientas de productividad con redundancia.

- **Prioridad Baja (Complementarios)**

Recursos: Soluciones cuya falta de adaptación no afecta significativamente las operaciones y pueden modificarse en fases posteriores del proyecto. **Ejemplos:** Aplicaciones de soporte secundario, herramientas con versiones temporales disponibles.

CRITICIDAD

- **Criticidad A: (Máxima)**

No puede permanecer interrumpido(a) por un período mayor de 24 a 48 horas.

- **Criticidad B: (Intermedio)**

No puede permanecer interrumpida(o) por un período mayor a 5 días hábiles. Puede sustituirse parcialmente por un período, por un proceso manual.

- **Criticidad A: (Mínima).**

Puede permanecer interrumpida(o) por un período entre 10 días y 20 días hábiles. Puede sustituirse temporalmente por un proceso manual.

PROCESOS CRÍTICOS

Con base en el análisis de criticidad, se identificaron los siguientes procesos prioritarios para la Corporación CDA, junto con las acciones requeridas para garantizar su continuidad operativa:

SOFTWARE

1. Software Aplicativo

A. Aplicaciones de Desarrollo Externo

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Prioridad:** Alta (Crítico)
- **Riesgo:**
  - Alto potencial de pérdida de información
  - Posible paralización de procedimientos administrativos si no se mantienen adecuadamente
- **Acciones:**
  - Implementar soluciones inmediatas para aplicaciones contratadas externamente
  - Establecer contratos de soporte técnico y actualizaciones periódicas

B. Aplicaciones de Desarrollo Interno

- **Prioridad:** Media-Alta
- **Riesgo:**
  - Dependencia de recursos internos para su mantenimiento y adecuación
- **Acciones:**
  - Ejecutar procesos de adecuación y pruebas bajo la supervisión del área de Gestión TIC
  - Documentar y estandarizar los procesos de desarrollo interno

HARDWARE.

Infraestructura Tecnológica de la Corporación CDA

1. Equipos de Cómputo y Periféricos

- Distribución geográfica: Disponibles en las tres sedes principales (Guainía, Guaviare y Vaupés)
- Equipamiento:
  - Computadores de escritorio para puestos fijos
  - Portátiles para personal móvil
  - Impresoras y escáneres compartidos
- Arrendamiento: Impresoras de alta capacidad en la sede principal (Iniri.
- da)

2. **Infraestructura de Servidores**

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Centro de Datos Principal: Ubicado en Inírida
- Configuración:
    - Servidores Blade para virtualización y consolidación
    - Sistema de climatización y respaldo energético

3. **Equipos de Soporte Crítico**

- Sistemas UPS: La Entidad cuenta con varias UPS los cuales están distribuidos en diferentes dependencias, cabe aclarar que algunas UPS ya se encuentran obsoletas, por lo cual se requiere su cambio.

EQUIPOS DE COMUNICACIONES

La estructura de la red maneja cableado UTP categoría 6A para su segmento horizontal y vertical con Swich tplink, routers tplink.

DEFINICIÓN Y CONFORMACIÓN DEL GRUPO DE TRABAJO

Para garantizar el desarrollo efectivo del Plan de Contingencias en las áreas de sistemas de la entidad, se abordará su implementación como un proyecto estratégico. Con este fin, se conformará un Grupo de Desarrollo del Plan de Contingencias, integrado por funcionarios de la Corporación, cuya estructura y responsabilidades se detallan a continuación.

Grupo de Desarrollo del Plan de Contingencias

Conformación:
funcionarios designados de la Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA).

Responsabilidades:

1. Definir los lineamientos del Plan de Contingencias para los Sistemas de Información de la Corporación, alineados con los objetivos institucionales.
2. Analizar, evaluar y resolver los requerimientos técnicos y operativos que surjan durante el desarrollo e implementación del plan.
3. Recomendar la adquisición, actualización o mantenimiento de equipos, software e infraestructura necesarios.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

4. Coordinar la ejecución, implementación y mantenimiento continuo del Plan de Contingencias.
5. Evaluar y tomar decisiones sobre propuestas, requerimientos o recomendaciones presentadas al grupo.
6. Aprobar la celebración de convenios, contratos o adquisición de recursos asociados al plan.
7. Gestionar y asignar los recursos necesarios para el funcionamiento del grupo de desarrollo.
8. Comunicar oficialmente las decisiones adoptadas, el avance en la ejecución del plan y el estado de los recursos informáticos cubiertos.
9. Supervisar y garantizar el cumplimiento del plan, así como la operatividad de los canales de comunicación entre los equipos involucrados.
10. Brindar los recursos necesarios e informar oportunamente las decisiones a los funcionarios designados.
11. Designar al Coordinador del Plan de Contingencias, responsable de liderar su ejecución.

Coordinador del desarrollo del plan de contingencias.

FUNCIONES

1. Ejecutar oportunamente las actividades programadas, garantizando el cumplimiento de plazos y objetivos establecidos.
2. Elaborar y formalizar la documentación oficial del Plan de Contingencias, asegurando su validez y alineación con los estándares institucionales.
3. Gestionar y organizar toda la documentación asociada al proyecto, incluyendo registros y papeles de trabajo, para facilitar su acceso y trazabilidad.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

4. Desarrollar programas de capacitación dirigidos a los funcionarios de todos los niveles, con el fin de garantizar su participación efectiva en la implementación del plan.
5. Elaborar cronogramas y brindar soporte logístico para la ejecución de pruebas piloto de cada componente del plan.
6. Garantizar la operatividad y actualización permanente del Plan de Contingencias, incorporando mejoras y ajustes según las necesidades detectadas.

Subgrupo de Atención de Emergencias
Conformado por:

- El líder de sistemas TIC
- El profesional de Seguridad y Salud en el Trabajo
- El jefe del área afectada o su suplente
- El responsable (o su suplente) del procedimiento relacionado con el aspecto afectado

Designados por el encargado de Seguridad y Salud en el Trabajo, este grupo activará las medidas necesarias para proteger los recursos humanos y materiales durante emergencias.

Subgrupo de Supervisión
Integrado como mínimo por personal del área afectada, este equipo:

- Brinda apoyo e información al Subgrupo de Atención de Emergencias cuando sea requerido.
- Supervisa la situación en las áreas no impactadas por la contingencia.
- Reporta al Líder de Sistemas TIC y al profesional de Seguridad y Salud en el Trabajo.

Subgrupo de Evaluación de Daños
Conformado por:

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Los mismos miembros del Subgrupo de Supervisión
- Con apoyo del Líder de Gestión de TIC

Funciones:

- Evaluar la planta física e infraestructura.
- Identificar daños materiales (hardware) y operativos (software) causados durante la emergencia.

PLAN DE MITIGACIÓN

Conjunto de estrategias y procedimientos implementados *antes* de que se materialice un riesgo o emergencia, con el objetivo de:

- **Reducir la gravedad** del impacto.
- **Minimizar consecuencias** o pérdidas potenciales.

PROCESO DE RESPALDO

Procedimiento de mitigación que garantiza:

1. Protección de la información vital de la organización.
2. Continuidad operativa en el procesamiento de datos, incluso ante fallas de equipos.

Componentes del Sistema de Respaldo

Cubre los 5 elementos críticos de un sistema de información:

1. Datos: Información esencial respaldada periódicamente.
2. Documentación: Manuales, políticas y registros técnicos.
3. Software: Programas y aplicaciones necesarias para operar.
4. Procedimientos: Protocolos para recuperación y operación alternativa.
5. Hardware: Equipos redundantes o alternativos para sustituir los afectados.

Proceso de Respaldo Externo

Como sitio de respaldo externo se entiende una instalación diferente a la sede principal de la entidad donde se almacena una copia de los archivos de backup de la entidad, para que ante cualquier eventualidad que se presente en la sede principal se pueda reiniciar labores con los archivos almacenados en el sitio de respaldo externo. En la

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

entidad la instalación física que cumple con los requisitos de almacenamiento requeridos se encuentra ubicada en la oficina de sistemas.

Plan de Backups y Equipos de Respaldo

Un backup es una copia de seguridad de la información en un segundo medio (cinta, disco duro externo, Medio óptico, etc.) que nos garantiza recuperar la información contenida en nuestras maquinas en caso de que se presente alguna falla en el disco duro, un borrado accidental o un accidente imprevisto. Estos backup deben ser ejecutados por:

1. El Área encargada del proceso de Gestión de las TICS.
2. Usuarios con privilegios para realizar copias de seguridad.

DEFINICIÓN DE NIVELES DE BACKUP

La Oficina de sistemas o informática ha establecido los siguientes niveles de backup como política institucional:

1. Backup Anual

- **Frecuencia**: Último día del año.
- **Tipo**: Backup total.
- **Almacenamiento**: Medio físico guardado indefinidamente.

2. Backup Semestral

- **Frecuencia**: Último día de cada semestre (excepto el último día del año).
- **Tipo**: Backup total.
- **Almacenamiento**: Medios etiquetados como *Semestre1* y *Semestre2*, reutilizados anualmente.

3. Backup Mensual

- **Frecuencia**: Último día de cada mes (excepto el último día del año).
- **Tipo**: Backup total.
- **Almacenamiento**: Medios etiquetados como Mes1, Mes2, ..., Mes12, reutilizados anualmente.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

4. Backup Semanal

- **Frecuencia**: Último día de la semana.
- **Tipo**: Backup total.
- **Almacenamiento**: Discos duros externos etiquetados como Semana1, ..., Semana4, reutilizados mensualmente.

5. Backup Diario

- **Frecuencia**: Al final de cada día.
- **Tipo**: Backup total de la información diaria.
- **Almacenamiento**: Medios etiquetados por día (lunes, martes, miércoles, jueves, viernes. etc.), reutilizados semanalmente.

6. Backup en Línea

- **Frecuencia**: Continuo (siempre que exista la infraestructura necesaria).
- **Tipo**: Copia de archivos y directorios críticos.
- **Almacenamiento**: Servidor remoto.

CENTRO DE DATOS (DATA CENTER)

Definición y Relevancia

El Data Center es la infraestructura física que alberga los recursos tecnológicos esenciales para el procesamiento y almacenamiento de la información institucional. Constituye un activo estratégico debido a:

- La alta inversión en sus componentes.
- La concentración de datos críticos para las operaciones de la entidad.

Componentes Principales

Incluye, entre otros:

- **Servidores**: Aplicaciones, bases de datos, correo electrónico, autenticación, Internet.
- **Seguridad**: Firewalls, proxies, antivirus.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Almacenamiento**: Sistemas SAN (Storage Área Network).
- **Respaldo/Recuperación**: Servidores dedicados.
- **Comunicaciones**: Redes de datos, *switches*, *routers*.

Requisitos de protección

El Data Center debe garantizar:

- **Ambientes físicos y lógicos** seguros.
- **Disponibilidad, confidencialidad e integridad** de los datos.
- **Monitoreo 24/7** con personal especializado.
- **Suministro permanente** de energía, conectividad y acceso controlado.

Limitación Actual

La Corporación CDA **no cuenta con un centro de datos alterno**, lo que refuerza la necesidad de:

- **Procedimientos robustos** de backup.
- **Protección reforzada** del Data Center principal.

FASE DE EMERGENCIA.

En esta fase se presentan las acciones detalladas que deben llevar a cabo durante la emergencia. Se proveen una serie de instrucciones a las áreas Operativas y Administrativas, en caso de materializarse el riesgo. Las soluciones que deben ser implementadas para mantener la continuidad de los procesos críticos en el momento de la materialización de los riesgos son las siguientes, para cada proceso crítico asociado a un riesgo, se define una acción o procedimiento a seguir.

SOFTWARE.

Aplicaciones de desarrollo externo.

Software financiero

Aplicación: Pimisys sas (tesorero, almacen, sicar, p&g, papiro).

- Se contrata anualmente con el proveedor la actualización, mantenimiento y soporte técnico del sistema Pimisys sas.
- El soporte técnico por un año, se tendrá asistencia técnica a permanente a través

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

de distintos medios.
- Mantenimiento y capacitación presencial y virtual cada año.

Software de gestión documental.

Aplicación: Mi doc millenium.

- Es propiedad de la corporación CDA, por lo cual no se contrata soporte técnico externo.
- El ingeniero de sistemas o quien se designe será el encargado de la instalación y mantenimiento del aplicativo.

HARDWARE.

Computadores personales

Estado Actual

La entidad cuenta con equipos de cómputo (escritorio y portátiles) operativos, distribuidos en todas sus dependencias.

Usuarios

Personal de todas las áreas de la entidad.

Riesgos Asociados

1. **Fallas operativas**:
   - Mal funcionamiento de aplicaciones críticas.
   - Averías en equipos con software esencial.
2. **Pérdida de información**:
   - Corrupción o borrado accidental de datos.
3. **Soluciones inadecuadas**:
   - Adquisición o implementación de hardware/software incompatible con la infraestructura actual.
4. **Fallas de hardware**:
   - Equipos obsoletos o fuera de inventario.

Plan de Contingencia

- **Redistribución de recursos**: Reasignación estratégica del hardware disponible para priorizar áreas críticas.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- **Optimización de equipos**: Uso eficiente de los activos existentes para cubrir necesidades operativas urgentes.

Equipos Servidores

Estado Actual: la corporación CDA tiene un data Center donde están ubicados los servidores HP tipo Blade que hacen parte de la infraestructura tecnológica de la entidad.

Usuario: Centro de Cómputo y Usuarios de Aplicaciones implementadas en los servidores activos.

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información,

Soluciones en Contingencia: Se debe garantizar el mantenimiento preventivo/correctivo de los computadores y la red de datos de la corporación CDA.

Equipos Electrónicos

Estado Actual: Actualmente se cuenta con una (1) UPS en la oficina de sistemas

Proveedor:

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Posibles retrasos en procesos administrativos, demoras en la efectividad de algunas comunicaciones, Posible daño de equipos o pérdida de protección ante ausencia de fuente regulada y soporte en corte de energía eléctrica.

Soluciones en contingencia: Se requiere tener un banco de baterías adicional en caso de fallas de la actual UPS.

FASE DE RECUPERACION.

Permite restablecer las condiciones originales y operación normal del sistema el cual contempla:

- Definición de las políticas (parámetros, límites, horas de recuperación)
- Definición de los objetivos y requerimientos de la continuidad
- Definiciones, términos y suposiciones

Protocolo de Activación del Centro de Datos Alterno en Caso de Interrupción Prolongada

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

1. Evaluación Inicial (Fase de Emergencia)

- **Determinación del Tiempo de Interrupción**:
  - El **Coordinador del Plan de Contingencias**, con apoyo del equipo técnico, evaluará el alcance del daño durante las primeras 24–48 horas.
  - Se activará el **Centro de Datos alterno externo** si:
    - La interrupción supera **5 días**.
    - El **60% o más** de las instalaciones físicas/tecnológicas están afectadas.

2. Activación del Centro de Datos Alterno (Días 1–5)

- **Objetivo**: Restaurar el servicio básico de procesamiento de datos antes del 5º día post-desastre.
- **Acciones Clave**:
  - Migración de copias de respaldo (aplicaciones y procedimientos automatizados).
  - Priorización de sistemas críticos para operaciones mínimas.

3. Recuperación Total (Días 6–15)

- **Reestructuración de Capacidades**:
  - 2–15 días hábiles para restablecer al 100% la red en línea y servicios asociados.
  - Enfoque en:
    - Restauración de bases de datos.
    - Reconfiguración de redes y seguridad.

PREPARACIÓN REQUERIDA PARA RECUPERACIÓN DE DESASTRES

Los grupos de recuperación de desastre, deben estar organizados a lo largo de las líneas funcionales de la entidad con el Líder del Proceso de Gestión de las TIC. Cada grupo es responsable del restablecimiento de la normalidad ante un desastre e igualmente son responsables del mantenimiento de los procedimientos que lleven a esa recuperación.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Los esfuerzos de planeación son para moderar el esfuerzo de la recuperación y maximizar el éxito de los procedimientos implementados en el evento de un desastre.

RECUPERACION DEL DESASTRE: PLAN DE ACCION

El Plan presupone que debe utilizarse un Centro de Datos alterno externo al edificio de la sede Principal de la corporación CDA si la emergencia afecta en forma general (en un 60% o más) las instalaciones físicas y técnicas con que se cuenta. Los siguientes procedimientos se circunscriben a dichos hechos o casos.

PRIMERA FASE.

procedimientos iniciales de Respuesta/Notificación.

Los siguientes deben ser los procedimientos a ser implantados en el momento del desastre, procedimientos que deben continuar hasta que se restauren los servicios de procesamiento de datos en el sitio original u otro permanente. En el caso de incendio, explosión u otro desastre mayor en el Centro de Datos, debe implantarse inmediatamente los procedimientos de emergencia implementados por el grupo de Salud Ocupacional previa notificación a cada uno de sus integrantes.

Procedimientos de Emergencia en el Centro de Datos.

1.Evacuación Inmediata (Emergencia Crítica).

Si la naturaleza del desastre no permite tiempo para apagar equipos, la prioridad es la evacuación inmediata de todo el personal del centro de datos o área afectada. Una vez en un lugar seguro, se debe notificar de inmediato al Grupo de Administración de Emergencia o al Grupo de Salud Ocupacional/sus delegados).

2. Apagado Controlado (Si el tiempo lo permite)

En caso de contar con tiempo suficiente, seguir este orden de acciones:

1. **Activar:** los procedimientos de emergencia establecidos por el Grupo de Salud Ocupacional.
2. **Apagar:** servidores y dispositivos críticos según los protocolos definidos.
3. **Cortar suministros**: Apagar luces y accionar los interruptores en las cajas de distribución.
4. **Notificar:** al Grupo de Administración de Emergencia antes de evacuar.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Grupo de administración de emergencia de gestión tic.

1. Jefe o líder de la oficina de tecnología de la información o comunicaciones.
2. Técnicos de sistemas.

SEGUNDA FASE.

Procedimiento para el proceso de restauración.

Tan pronto como se haya declarado un desastre, los líderes de grupo serán llamados para implantar el Plan a tomar en el desarrollo del Plan de Contingencias. El grupo de Centro de Cómputo junto con el grupo de atención a usuarios establecerá un centro de control y empezarán la coordinación para la restauración de los sistemas que hayan sido afectados.

Dentro de las 5 primeras horas siguientes al desastre.

1. **Comunicación Inmediata.**
   - Notificar a los usuarios sobre la interrupción del servicio.
   - Informar al Centro de Cómputo Alterno (si aplica), Administrador de TI, Servicios de Soporte, director y demás partes clave.
2. **Continuidad Operativa.**
   - Activar el procesamiento manual de aplicaciones críticas (si es requerido).
   - Evaluar daños e identificar equipos reutilizables para su traslado al Centro de Datos Alterno.
3. **Coordinación con Proveedores y Equipo TIC.**
   - Notificar al proveedor las configuraciones de hardware necesarias y gestionar requerimientos.
   - Alertar a todo el personal del Área de Gestión TIC involucrado en el Plan de Continuidad.
4. **Preparación de Infraestructura Alterna.**
   - Seleccionar y organizar oficinas de servicio para el procesamiento de reportes de respaldo.
   - Acondicionar el Centro de Datos Alterno o de Respaldo:
     - Verificar suministro eléctrico.
     - Revisar sistemas contra incendios y ventilación/extractores.
   - Configurar circuitos de comunicación de datos en el sitio alterno (si es necesario).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Dentro de las 24 primeras horas siguientes al desastre.

Protocolo de Activación del Centro de Datos Alterno

1. **Gestión con Proveedores**
   - Solicitar formalmente al proveedor el soporte técnico requerido (hardware y software).
   - Verificar y confirmar la disponibilidad del soporte comprometido.
2. **Preparación de Infraestructura**
   - Coordinar la habilitación del Centro Alterno (energía, conectividad y ambientación).
   - Recopilar y trasladar la documentación técnica y respaldos magnéticos desde el almacenamiento externo designado.
3. **Operativización del Centro Alterno**
   - Ejecutar el procesamiento prioritario de reportes críticos en el nuevo entorno.
   - Validar el funcionamiento integral de todos los sistemas según los parámetros establecidos.

Dentro de los 2 días siguientes al desastre debe:

- Catalogar el despacho de suministros
- Trasladar el personal necesario y/o requerimientos al Centro Alterno
- Completar el ensamblaje de la documentación y los medios magnéticos en el Centro Alterno, coordinando la prestación de los servicios desde el Centro Alterno.

Dentro de los 3 días siguientes al desastre debe:

- El Centro Alterno debe estar totalmente preparado para operar
- Llevar el inventario de los medios magnéticos, los listados y otra documentación en el Centro Alterno.
- Recibir en el Centro Alterno suficientes suministros, muebles y equipo relacionado
- Determinar el punto inicial de aplicaciones críticas.
- Establecer un catálogo de procesamiento de las aplicaciones críticas.
- Evaluar las líneas de comunicación de datos catalogados para una restauración inicial.

Dentro de los 6 días siguientes al desastre:

- Asegurar la operación total de los sistemas críticos.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Continuar la implantación por fases de la red de comunicación de datos

Dentro de los 10 días siguientes al desastre:

- Restauración completa de la red de comunicación de datos y de las operaciones.

TERCERA FASE

Protocolo de Procesamiento en el Centro de Cómputo

Fase de Operaciones Paralelas

Esta etapa se activa cuando:

- Los sistemas críticos y redes están operativos, pero
- La restauración completa de datos no se ha finalizado**.**

Acciones clave:

1. **Ejecución Controlada**
   - Mantener operativos los servicios esenciales en el entorno actual (temporal o alterno).
   - Implementar procesamiento parcial mientras se completa la recuperación total.
2. **Comunicación y Documentación**
   - Informar al personal involucrado sobre:
     - El estado del plan de continuidad.
     - Las acciones tomadas hasta el momento.
   - Recolectar y analizar los logs de recuperación (a cargo del *Grupo de Administración de Emergencia de Gestión TIC*).
3. **Transición Planificada**
   - Preparar la migración al sitio original o permanente (infraestructura, datos y configuración).
   - Validar la integridad de los sistemas antes del retorno.

Criterio de Finalización:
La fase concluye cuando:

- Los servicios de procesamiento se restauran en su ubicación definitiva.
- Se verifica la estabilidad operativa y se cierra el registro de incidentes.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

Actividades de esta fase:

- Asegurar un medio ambiente físico y restablecer la seguridad en los datos
- Comenzar el procesamiento de transacciones críticas
- Tener todos los recursos en su lugar en el Centro de Datos Alterno
- Localizar los procedimientos de backup y almacenamiento
- Obtener una recuperación total
- Distribución del grupo de personal y reportar a la administración

CUARTA FASE

Recuperación en el sitio original.

Durante la operación en el Centro Alterno, se planificará la recuperación total en el sitio original. En casos de desastre mayor o según los planes organizacionales, podrá ejecutarse en un sitio alterno improvisado. Esta fase sigue una estructura similar a la Fase 3 (*Operaciones Paralelas*), pero en una ubicación permanente.

Procedimientos Clave:

1. **Planificación Estratégica**
   - Definir tiempos críticos y asignar el equipo de recuperación.
   - Elaborar procedimientos de recuperación adaptados a la ubicación permanente.
2. **Preparación del Sitio**
   - Restaurar infraestructura física (energía, climatización, seguridad).
   - Garantizar la integridad ambiental (protección contra incendios, control de accesos).
3. **Restauración Técnica**
   - Reinstalar y configurar sistemas críticos (*hardware*, *software*, redes).
   - Ejecutar pruebas de funcionamiento parcial y total.
4. **Transición a Producción**

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- Migrar procesamientos desde el entorno alterno al permanente.
- Validar la estabilidad operativa antes del retorno definitivo.

5. **Cierre y Mejoras**
   - Realizar auditoría post-desastre (lecciones aprendidas).
   - Gestionar reclamaciones ante aseguradoras (si aplica).
   - Presentar informe ejecutivo a la alta administración.

QUINTA FASE

MANTENIMIENTO

El mantenimiento del Plan incluirá la programación de sistemas necesarios para adaptar los programas a los cambios tecnológicos, tanto de *hardware*, *software* y aplicaciones a lo largo del tiempo. Este aspecto es fundamental para garantizar el éxito futuro del Plan.

Asimismo, es crucial mantener actualizados los nombres, responsabilidades y números telefónicos de los participantes clave. El Plan será auditado periódicamente para verificar que esta información se revise de manera rutinaria tanto en el documento original como en todas sus copias.

IMPLEMENTACIÓN DEL PLAN

Para la implementación efectiva del Plan, se deben establecer y documentar formalmente los siguientes procedimientos operativos:

- Respaldo y retención de archivos: tanto permanentes como corrientes, en cada dependencia.
- Software específico y operativo: gestión y actualización de las herramientas tecnológicas necesarias.
- Recuperación ante fallos: protocolos para resolver errores y fallas del sistema.
- Seguridad: medidas físicas y lógicas para proteger la información.
- Mantenimiento de equipos: acciones preventivas y correctivas para garantizar su funcionamiento óptimo.

Proceso de aprobación y adopción:

1. Revisión y aprobación: El Plan debe ser evaluado y aprobado por el Comité de Informática.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

2. Pruebas y simulacros: Una vez aprobado, se llevarán a cabo pruebas de implementación.
3. Adopción institucional: Se formalizará mediante un Acto Administrativo, específicamente a través de una Resolución emitida por la Dirección General.

Posteriormente, se recopilarán las modificaciones al Plan de manera semestral, garantizando así su continua actualización.

PLAN DE PRUEBAS EXPERIMENTALES

El Plan de Contingencias incluye la ejecución de un plan experimental de pruebas, en el que se simularán distintos escenarios de siniestros para evaluar la eficacia del plan. Si se detectan deficiencias, se realizarán los ajustes necesarios para garantizar su correcto funcionamiento.

El enfoque principal estará en:

1. Simulacros de emergencia para validar los protocolos.
2. Procedimientos posteriores a la emergencia, especialmente aquellos relacionados con la recuperación operativa de la Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA).

OBJETIVOS DE CONTROL Y AUDITORÍA DE LAS PRUEBAS

Las pruebas del plan buscan:
✓ Validar la capacidad del personal y la eficacia de los procedimientos en situaciones de recuperación ante desastres.
✓ Verificar la factibilidad de las instalaciones de respaldo y los procesos asociados.
✓ Identificar y corregir fallos en el diseño del plan.
✓ Promover la capacitación y difusión de los protocolos de recuperación.
✓ Garantizar el compromiso con el plan y su correcta ejecución en emergencias.
✓ Optimizar costos de seguros mediante una evaluación técnica de riesgos.
✓ Mantener actualizados los procedimientos, incentivando la participación activa del equipo involucrado.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

RESPONSABILIDADES Y METODOLOGÍA DE PRUEBAS

La Oficina Asesora de Control Interno será responsable de:

- Definir las responsabilidades durante las pruebas.
- Establecer la frecuencia de las simulaciones y actualizaciones, considerando cambios en el entorno tecnológico.

El Jefe de Gestión de TIC y el Jefe de Control Interno, en coordinación con el Comité de Sistemas, determinarán los niveles de prueba:

- Pruebas por segmentos (áreas específicas).
- Pruebas globales (simulación completa del plan).

Métodos de prueba recomendados:

- Pruebas en papel (análisis teórico de escenarios).
- Pruebas reales (ejecución parcial de protocolos).
- Simulacros a gran escala (ejercicios prácticos con participación multidisciplinaria).

PASOS PARA LA EJECUCIÓN DE PRUEBAS

El equipo desarrollador del plan presentará al jefe de sistemas el protocolo de pruebas, considerando:

1. Selección del módulo a evaluar - Identificación de los capítulos específicos del plan sujetos a verificación
2. Definición de objetivos y métricas - Establecimiento de criterios de éxito y métodos de medición
3. Revisión con el comité directivo - Presentación de la propuesta para obtener aprobación y recursos
4. Notificación oficial - Comunicación formal de:
    - Alcance de la prueba
    - Factores críticos
    - Duración estimada
5. Compilación de resultados - Documentación integral de los hallazgos

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

6. Análisis de desempeño - Evaluación de:
    - Avances
    - Dificultades
    - Resultados alcanzados
7. Validación de escalabilidad - Determinación de si los resultados parciales pueden extrapolarse al plan completo
8. Propuesta de mejoras - Elaboración de:
    - Recomendaciones específicas
    - Plazos para implementación
9. Reporte a dirección general - Presentación formal de conclusiones al director de la CDA
10. Actualización documental - Ajuste de manuales y procedimientos cuando corresponda.

AREAS O PARTES A PROBAR

COMPONENTES A EVALUAR EN LAS PRUEBAS

1. Recuperación de sistemas aplicativos usando Backups externos
2. Funcionamiento en modo degradado
3. Restauración de discos y procedimientos de arranque con respaldos externos
4. Adaptación a configuraciones alternas en sitios de contingencia
5. Disponibilidad de:
    - Equipos principales y periféricos
    - Sistemas de soporte (energía, climatización)
    - Recursos logísticos (transporte, comunicaciones)
6. Protocolos de evacuación del centro de datos
7. Capacidad de priorización de sistemas con recursos limitados
8. Operación sin personal clave

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

9. Adaptabilidad a incidentes menores
10. Efectividad de procesos manuales alternativos
11. Capacidad de:
    - Ingreso de datos en instalaciones externas
    - Continuidad operativa en sistemas no críticos
    - Contacto organizado con personal clave
12. Cumplimiento de estándares normativos
13. Cobertura de recursos por pólizas de seguro
14. Distribución adecuada de:
    - Reportes impresos
    - Transmisión de datos
    - Documentación crítica
15. Control de formularios numerados
16. Adherencia a protocolos de seguridad durante crisis
17. Ejecución de:
    - Procedimientos de evacuación
    - Primeros auxilios
18. Recuperación de datos en sistemas en línea
19. Medición de tiempos y eficiencia en ejecución

PROCESO GENERAL PARA PRUEBA ANUNCIADA

1. Presentación a consideración del comité directivo
2. Procedimiento de comunicación formal
3. Desarrollo de la prueba

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

PROCESO GENERAL PARA SIMULACRO

1. Presentación a consideración del comité directivo
2. Desarrollo del simulacro

POLÍTICAS DE SEGURIDAD

POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

Las políticas de seguridad constituyen el fundamento esencial para garantizar la protección efectiva de los activos informáticos de la organización. Su importancia radica en que:

1. Establecen el marco de referencia para el desarrollo de estándares y procedimientos de seguridad
2. Garantizan consistencia en la toma de decisiones relacionadas con protección de datos
3. Mitigan vulnerabilidades que podrían ser explotadas tanto por amenazas internas como externas

Esta implementación inicial busca:

- Evaluar el grado de adopción organizacional
- Verificar el cumplimiento efectivo
- Identificar oportunidades de mejora.

REINICIALIZAR O RESTAURAR SU SISTEMA

Los propietarios de los sistemas de información deben garantizar la existencia de un *backup* completo y que los procedimientos de recuperación estén implementados.

Descripción: Permite reinstalar los componentes necesarios para asegurar un reinicio exitoso del equipo después de una interrupción, ya sea voluntaria o involuntaria.

Riesgos:

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- La falta de disponibilidad del sistema tras una interrupción puede afectar la eficiencia operativa de la entidad.
- La pérdida de información puede interrumpir operaciones y retrasar procesos críticos.

PANTALLA EN BLANCO (PROTECCIÓN DE INFORMACIÓN)

Los usuarios de los equipos corporativos de **CDA** deben asegurarse de que su monitor quede en blanco (suspendido) cuando no esté en uso.

Riesgos:

- Si la pantalla permanece visible en ausencia del usuario, personas no autorizadas podrían acceder a información confidencial.
- Observar cómo se accede a sistemas sensibles facilita intentos de copia o robo de datos, incluso durante ausencias breves.

GESTIÓN DE BACKUPS Y RECUPERACIÓN DE DATOS

La realización de *backups* y la capacidad de recuperar información son prioridades críticas. La administración debe garantizar que:

- La frecuencia de los *backups* y los procedimientos de recuperación se alineen con las necesidades de la organización.
- Los procesos de recuperación estén **documentados claramente** y **se prueben periódicamente**.

Descripción: Cuando los procedimientos de Backups son inadecuados o débiles, la información puede perderse o no estar disponible, lo que compromete la confiabilidad de los procesos de la organización.

ARCHIVO DE INFORMACIÓN: DIRECTRICES CLAVE

Selección de medios y formatos:

- Los soportes de almacenamiento deben garantizar la preservación acorde al ciclo de vida requerido por cada tipo de información (temporal o permanente).

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

- El formato de archivo debe priorizar estándares abiertos y compatibilidad a largo plazo, evitando dependencia de formatos propietarios que puedan quedar obsoletos.

Beneficios de un archivo eficiente:

- Reduce la carga de almacenamiento y recursos al migrar datos no críticos del entorno operativo diario.

Riesgos críticos:

1. **Medios inadecuados:** La degradación física de soportes (discos, cintas, etc.) puede imposibilitar la recuperación futura de datos.
2. **Obsolescencia de formatos:** El uso de formatos dependientes de sistemas específicos puede dejar la información inaccesible ante actualizaciones tecnológicas.

ENVÍO DE CORREOS ELECTRÓNICO INSTITUCIONAL

Uso apropiado del correo electrónico:

El correo electrónico debe emplearse exclusivamente para fines institucionales, manteniendo un estándar de comunicación profesional acorde con las demás formas de interacción oficial de la Corporación CDA.

Protocolo para archivos adjuntos:

Antes de adjuntar cualquier archivo a un correo electrónico, es obligatorio:

1. Clasificar adecuadamente la información que se enviará
2. Escanear y verificar que el archivo esté libre de virus, malware o cualquier código malicioso

Consideraciones de seguridad:

• El correo electrónico, aunque esencial en el entorno empresarial actual, presenta vulnerabilidades inherentes de seguridad que muchos usuarios subestiman al transmitir mensajes, información confidencial o instrucciones sensibles.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

• La implementación de firmas digitales y el uso de encriptación (cuando sea necesario) son medidas fundamentales para garantizar la autenticidad, integridad y confidencialidad de los mensajes. Los correos recibidos sin estos elementos de seguridad deben considerarse potencialmente no confiables.

Riesgos asociados al uso inadecuado:

1. Transmisión de virus: Un archivo infectado puede no solo comprometer los sistemas informáticos, sino también causar daños irreparables a la reputación institucional.
2. Interceptación de información: El envío de correos a través de redes públicas (como Internet) expone los datos a posibles accesos no autorizados, similar a enviar una postal sin sobre donde cualquiera puede leer el contenido.
3. Filtración de datos confidenciales: El envío de información sensible como archivos adjuntos puede violar protocolos de confidencialidad y derivar en consecuencias financieras o legales para la organización.
4. Problemas de gestión documental: La distribución indiscriminada de copias de archivos entre colegas genera duplicidad innecesaria y puede comprometer la integridad del documento original.

CONCLUSIONES

El presente Plan de Contingencias establece los protocolos, metodologías y acciones estratégicas que la Corporación para el Desarrollo Sostenible del Norte y Oriente Amazónico (CDA) implementará para garantizar la resiliencia operacional ante eventuales desastres que puedan comprometer su infraestructura tecnológica, integridad de datos o continuidad de procesos críticos.

1. **Protección y continuidad operativa:**
    - Se han definido procedimientos técnicos y administrativos para salvaguardar la información y asegurar la recuperación ágil de sistemas ante interrupciones, minimizando impactos en el cumplimiento de los objetivos institucionales.
2. **Integración tecnológica inter-sedes:**
    - El plan promueve la sinergia entre las sedes de la CDA mediante la estandarización de aplicaciones interoperables, asegurando coherencia

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

operativa, redundancia en centros de datos y continuidad funcional en todas sus jurisdicciones.

3. **Cultura organizacional de ciberseguridad:**
    - Se enfatiza la corresponsabilidad de todos los funcionarios en la protección de datos, trascendiendo al área de TIC. Esto incluye capacitación continua y adopción de buenas prácticas para mitigar riesgos humanos y técnicos.
4. **Estructuración de roles y responsabilidades:**
    - Se han delineado perfiles especializados para el equipo de contingencia, asignando tareas específicas de monitoreo, respuesta temprana y recuperación post-incidente, asegurando una ejecución coordinada y eficiente del plan.

Este documento no solo cumple con estándares de gestión de riesgos TI, sino que también se alinea con los compromisos institucionales de la CDA en materia de gobernanza digital y sostenibilidad operativa, reforzando su capacidad para enfrentar desafíos en entornos críticos.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co