PLAN DE CONTINGENCIAS PARA LOS SISTEMAS DE INFORMACIÓN DE LA CORPORACION AUTONOMA REGIONAL DE LA GUAJIRA – CORPOGUAJIRA

EDUARDO JOSE DAZA CUELLO
Profesional Especializado
Líder del proceso Gestión de las TICs

2020

Contenido

1. INTRODUCCIÓN

CORPOGUAJIRA considera que la información es el patrimonio principal de toda Institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

El Plan de Contingencias para los Sistemas de Información de Corpoguajira que se encuentra en el presente documento tiene como finalidad garantizar la continuidad de las operaciones automatizadas para reducir su nivel de impacto en la organización y en el cumplimiento de su misión.

El Plan está basado en un proceso dinámico y continúo que incluye no sólo las actividades a realizarse en el evento de una interrupción de la capacidad de procesamiento de datos; sino además, en las actividades realizadas anticipando dicho evento.

Una actividad principal del plan, es evaluar, mantener y mejorar los procedimientos de recuperación, que permitan mitigar los daños potenciales antes que un "**desastre**" ocurra. Otra actividad es facilitar la recuperación en el evento de un desastre para lo cual, la fase de recuperación provee tres propósitos:

1. Los roles individuales (de ejecución, coordinación y toma de decisiones) deben ser entendidos y atendidos en el contexto de todo el plan.
2. Existe la necesidad de establecer y mantener las descripciones de los procedimientos a ser realizados en el evento inesperado.
3. El plan permite un repaso administrativo, al evaluar la perfección y exactitud de cada proceso y repasa los procedimientos de recuperación sobre la marcha.

En ese sentido, *El Plan de Contingencias para los Sistemas de Información de Corpoguajira* se convertirá en la carta de navegación, contemplando:

- Definición de escenarios.
- Diseños de programas de almacenamiento y estrategias.
- Detalle de la administración general del Plan.
- Establecimiento de procedimientos contingentes, organización de grupos de trabajo, funciones y responsabilidades, involucrando usuarios y administradores.

2. OBJETIVOS

- Plantear y dotar a la Corporación Autónoma Regional de La Guajira – CORPOGUAJIRA de los procedimientos y elementos mínimos requeridos para afrontar la contingencia relacionada con el eventual cese de actividades, inoperatividad de equipos causada por razones de fuerza mayor.
- Proveer una solución para mantener operativos los sistemas de información y electrónicos fundamentales de la institución, que permitan reducir el impacto en las operaciones normales cuando son interrumpidos o paralizados por contingencias que afectan parcial o totalmente las instalaciones donde se procesan aplicaciones automatizadas y los servicios de procesamiento de datos de la entidad.
- Cuantificar la exposición a pérdidas asociadas a cada sistema de información automatizado y/o recursos informáticos con que cuenta la entidad, permitiendo un análisis de riesgos comprensible de los sistemas, que sirva como guía durante la ejecución del plan.
- Minimizar la posible pérdida financiera y operativa en el evento inesperado, previendo procedimientos de recuperación efectivos y eficientes. Así mismo, reducir las consecuencias de la posible pérdida de información relacionada con el evento inesperado, en un nivel aceptable, al ejecutar procedimientos de respaldo apropiados.
- Mantener la prestación del servicio a los usuarios, en el nivel aceptable.
- Restablecer las operaciones del Centro de Datos en el menor tiempo posible, dependiendo de la anomalía que se presente.

3. VENTAJAS POTENCIALES

El hecho de tener estructurado el plan de contingencias para el proceso de Gestión de las TICs y los sistemas de información de CORPOGUAJIRA tiene varias ventajas potenciales que ayudan a prevenir o a disminuir el impacto de los siniestros. Algunas de estas ventajas son:

- Determinar acciones preventivas que reduzcan el grado de vulnerabilidad; por el conocimiento que se tiene de los sistemas automatizados de información.
- Cuantificar los riesgos potenciales a que están expuestos los sistemas de información.
- Facilitar la oportuna toma de decisiones ante anomalías o fallas.
- Contribuir a generar una cultura de seguridad y control en las áreas de sistemas e institucionalmente, haciendo énfasis en el manejo de la información.

- Asegurar la estabilidad operativa y de la corporación, frente a la evidencia de un siniestro.
- Medir el grado de seguridad en los sistemas de información institucionales.
- Disminuir el impacto de un siniestro electrónico y evitar el deterioro, pérdida de información y equipos.

4. ALCANCE

La necesidad de desarrollar un plan de contingencias, está relacionada con el impacto potencial que provoca la interrupción parcial o total de los servicios electrónicos y procesamiento de la información, sobre el normal desarrollo de las actividades de CORPOGUAJIRA, específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos.

Esto supone que los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al Hardware, Software y Equipos electrónicos involucrados en los procesos críticos definidos en el Plan. Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales del Centro de Datos de la entidad.

Las actividades y procedimientos, están relacionados con las funciones que competen a cada uno de los grupos contingentes establecidos para la ejecución del Plan, y dependen de la diligencia y colaboración de las dependencias usuarias y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

El desarrollo de las actividades y proyectos, está condicionado a la aprobación de los mismos por parte del Comité Anti trámites y de Gobierno en Línea.

5. METODOLOGÍA

Las operaciones y procesos más importantes de CORPOGUAJIRA se encuentran sistematizados y funcionan con el soporte de las tecnologías de información, por lo que el proceso de Gestión de las TICs es de gran relevancia para el funcionamiento de la misma, lo cual obliga a la consideración de los siguientes aspectos:

- El tiempo durante el cual la entidad puede funcionar sin sus recursos computacionales en operación.
- La identificación de las amenazas potenciales sobre la capacidad de procesamiento automatizado de la información en la entidad.

- La identificación de las aplicaciones críticas que deben ser procesadas mientras se restablecen las operaciones normales en la entidad.
- Identificación de las consecuencias operativas, estratégicas, legales o de servicio, por la carencia del servicio automatizado.
- El valor de la inversión en el desarrollo del plan de contingencias que asegure su continuidad y normal funcionamiento.

El Plan se ha estructurado en tres grandes Fases:

1) **Fase de Mitigación:** CORPOGUAJIRA, 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) **Valuación del impacto por interrupción del servicio:** comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones. Esta valuación 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.
4) **Simulación o simulacro:** se define el cronograma de simulacros, así como se designa a los responsables de dar inicio a las pruebas, ambientar el personal y los recursos, controlar los eventos, documentar las acciones y evaluar el resultado en su conjunto.
5) **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.

6. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

6.1. DEFINICIÓN

RIESGO es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Es la probabilidad de ocurrencia de un evento inesperado. Proximidad a un daño, contingencia, peligro, inseguridad, azar o exposición.

6.2. DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

El siguiente análisis de riesgos implica la valuación del impacto por interrupción del servicio, el cual comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones; esta valuación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el Impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía.

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal de los sistemas de información con que cuenta la Entidad, son entre otros:

6.2.1. Causas Externas que conllevan a Riesgos

6.2.1.1. Políticos

Modificaciones a la constitución política ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

6.2.1.2. Pandemias
6.2.1.3. Desastres naturales

6.2.1.4. Posibles Fallas en el Flujo de Energía Eléctrica

Este riesgo está relacionado con amenazas externas al control de la Entidad. La implementación de equipos para la mitigación del riesgo de corte temporal de energía eléctrica.

6.2.1.1. Posible Falla del Servicio Telefónico

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

El impacto sobre las operaciones de la Corporación es de nivel bajo, ya que la Entidad posee una Infraestructura de Comunicación de datos y Redes locales implementada sobre cableado estructurado.

6.2.2. Causas Internas que conllevan a Riesgos

6.2.2.1. Posible incumplimiento de los contratistas

Este riesgo puede ocurrir a causa del posible atraso en la ejecución o trasgresión del clausulado de los contratos de actualización, modificación, mantenimiento, que se asumieron durante la vigencia para los plataformas, aplicativos y/o programas de Nómina, Sistema de Información Financiera, Sistema de Gestión Documental, Banco de proyectos, Página Web y SIG Corpoguajira.

6.2.2.2. Posibles retrasos en Procesos Administrativos

La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos con exigencia en el cumplimiento de requisitos, ampliando el tiempo de ejecución de las actividades del Plan Emergente, de manera imprevista.

6.2.2.3. Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles.

Se relaciona con deficientes procesos de análisis, evaluación, planeación y toma de decisiones sobre la elección de las alternativas tecnológicas a ser implementadas, y con el probable desconocimiento de las características y especificaciones técnicas de los recursos disponibles y las necesarias en cada una de las soluciones elegidas, de manera compatible.

6.2.2.4. Posible pérdida de información

Este riesgo tiene baja probabilidad de ocurrencia, si se tiene en cuenta que el Plan de Contingencias incluye un proceso de respaldo, que permite la mitigación del riesgo, efectuando copias de seguridad (backups), tanto a los archivos de trabajo (Word, Excel, PowerPoint, otros) como a los archivos de bases de datos y resultados de las aplicaciones específicas en producción para cada una de las dependencias de la Entidad.

6.2.2.5. Posible falla de equipos electrónicos y Hardware fuera de inventario

Este riesgo se presenta por la Falta de Previsión, con la no inclusión de soluciones para aspectos de baja prioridad o al excluir elementos de los inventarios, por desconocimiento o por no haber sido reportados a tiempo al Área encargada del proceso de Gestión de las TICS.

6.2.2.6. Posibles Fallas en el Flujo de Energía Eléctrica

Este riesgo está asociado con el uso de plantas eléctricas y de UPS (Unidad de Poder In-interrumpido) para salvaguardar la información. La UPS actual no funciona correctamente y no está cumpliendo con su objetivo ya que no tiene un contrato de mantenimiento. Problemas en el cableado o deterioro de la red de conducción interna.

6.2.2.7. Posible Calentamiento de la Sala de Cómputo

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que CORPOGUAJIRA Ha implementado procedimientos para su mitigación, tales como:

La implementación en el centro de Datos de un Sistema de control de temperatura provisto de un sistema de aire acondicionado, con sensores ambientales para el control y monitoreo de temperatura y alarmas locales. Cuenta con un de monitoreo por cámaras. El techo está provisto de detectores de humo y fuego que accionan un sistema de alarmas.

6.2.2.8. Posible Falla del Servicio Telefónico

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

El impacto sobre las operaciones de la Corporación es de nivel bajo, ya que la Entidad posee una Infraestructura de Comunicación de datos y Redes locales implementada sobre cableado estructurado.

7. IDENTIFICACION DE PROCESOS CRITICOS

7.1. 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**.

7.1.1. Prioridad 1

- Todos los sistemas vitales de la organización

7.1.2. Prioridad 2

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

7.1.3. Prioridad 3

- Sistemas cuya falla causa molestias menores

7.2. FACTORES CRÍTICOS A CONSIDERAR

7.2.1. Aplicaciones en Producción

1. Nivel de importancia de la aplicación en la entidad
2. Impacto operativo, financiero o contable
3. Oportunidad de procesamiento
4. Programas críticos
5. Comunicaciones: entrada y salida de datos
6. Implicaciones para el usuario en caso de ausencia del recurso aplicativo.
7. Documentación del sistema: manuales de usuario y procedimientos de operación.
8. Procedimientos de respaldo y recuperación a nivel aplicativo.

7.2.2. Personal

1. Funcionarios de posición clave y personal de dirección
2. Personal con alta dependencia en los sistemas automatizados
3. Personal de respaldo

4. Entrenamiento

7.2.3. Parque computacional y aplicaciones en uso

1. Servidores, computadores personales, impresoras, periféricos, etc.
2. Líneas de comunicación y equipos relacionados.
3. Sistemas operativos y programas producto.
4. Suministros: papel, formas continuas, medios magnéticos y formas especiales.
5. Archivos maestros y de movimiento considerados críticos de respaldo de los mismos.

7.3. NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECURSOS INFORMÁTICOS

Teniendo en cuenta los criterios y factores enunciados anteriormente, se han definido los siguientes niveles de prioridad y criticidad de los recursos informáticos con que cuenta la Corporación Autónoma Regional de La Guajira – CORPOGUAJIRA.

7.3.1. Niveles de Prioridad

7.3.1.1. Prioridad Alta

Corresponde a todas aquellas herramientas de la Corporación, que en el caso de no ser adaptadas oportunamente a las exigencias, generarían graves problemas que pueden llevar inclusive a paralizar las **actividades misionales**.

7.3.1.2. Prioridad Media

Se le asigna a todas aquellas herramientas de la Corporación, que aunque son importantes para el desarrollo normal de las **actividades administrativas, operativas y de control,** cuentan con procedimientos alternativos preestablecidos.

7.3.1.3. Prioridad Baja

Se le asigna a todas aquellas herramientas de la Corporación, cuya falta de adaptación no representa graves traumatismos y sus modificaciones **pueden aplazarse** para la última parte del proyecto.

7.3.2. Niveles de Criticidad

7.3.2.1. Criticidad A: (Máxima)

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

7.3.2.2. Criticidad B: (Intermedia)

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

7.3.2.3. Criticidad C: (Mínima)

Puede permanecer interrumpida(o) por un período entre 15 días y 30 días hábiles.
Puede sustituirse temporalmente por un proceso manual.

7.4. PROCESOS CRÍTICOS

Con base en lo anterior, se establecieron los Procesos Críticos de Corpoguajira descritos en la siguiente relación de recursos informáticos señalando la prioridad y las acciones a seguir para cada problemática en particular.

7.4.1. SOFTWARE

7.4.1.1. Software Aplicativo

7.4.1.1.1. Aplicaciones de Desarrollo Externo

Se determinó que las aplicaciones en producción que presentan un alto riesgo de pérdida de información y que pueden provocar parálisis en los procedimientos administrativos (en caso de no ser debidamente adecuadas), son aquellas elaboradas e implementadas a través de procesos contractuales; por lo tanto, serán objeto de inmediata solución.

7.4.1.1.2. Aplicaciones de Desarrollo Interno

Corresponden a las aplicaciones que la Corporación ha desarrollado y que actualmente operan en la entidad, para las cuales se ha iniciado procesos de adecuación y prueba bajo la responsabilidad del proceso de Gestión de las TICS.

7.4.2. HARDWARE

7.4.2.1. Computadores personales

La Corporación cuenta con 69 Computadores personales de escritorios, 15 portátiles, 55 impresoras y 3 escáneres distribuidos en tres sedes (Oficina Principal Riohacha, Laboratorio Riohacha y la Territorial del Sur en Fonseca). Igualmente tiene en alquiler 83 Computadores personales de escritorios y 15 computadores portátiles.

7.4.2.2. Equipos Servidores

La corporación cuenta con Servidores tipo Blade y tipo Rack instalados en el centro de datos ubicado en la sede principal de Riohacha.

7.4.3. EQUIPOS ELECTRÓNICOS

Los equipos electrónicos no-informáticos con que cuenta el centro de cómputo que requieren ser ajustados o reemplazados, son:

- **UPS**: La Entidad cuenta con UPS principal que da continuidad eléctrica a todos los computadores de la sede principal. Las sedes del Laboratorio y la Territorial del sur no cuentan con UPS. La Corporación no cuenta en la actualidad con contrato de mantenimiento preventivo ni correctivos para estos elementos. Las UPS presentan problemas en cuanto a su autonomía de funcionamiento debido a que la vida útil de sus baterías se ha cumplido, lo que significa, que en eventual momento de corte del fluido eléctrico no se puede mantener los sistemas en funcionamiento.

- **Sistemas de Alarmas:** El sistema de alarma contra incendios solo está instalado en la sede principal. No se tiene contrato de mantenimiento para este dispositivo Se requiere un sistema de alarmas tanto para el Laboratorio como para la territorial sur.

7.4.4. EQUIPOS DE COMUNICACIONES

7.4.4.1. Infraestructura de Redes

La estructura de la red maneja cableado UTP nivel 6A para su segmento horizontal con switchs HP en sus bordes y un Backbone de fibra óptica para su segmento vertical que converge en switch principal. Las sedes de Laboratorio y la Territorial del sur tienen un tendido de cable categoría 5E para la red de voz y

datos; cuenta con equipos activos (switches) y sus respectivos Patch Panel de tendido horizontal tanto como para voz como para datos.

7.4.4.2. Hardware de Comunicaciones

Consolidado de Recursos por Sede, relacionando los puntos de red, enlaces de radiofrecuencia y switches de cada uno de las sedes.

8. DEFINICION Y CONFORMACION DEL GRUPO DE TRABAJO

Para dar cumplimiento al desarrollo del plan de contingencias en las áreas de sistemas de la entidad, es necesario tratarlo como un proyecto. Por esta razón, se conformará un grupo de desarrollo responsable del plan. Se sugiere la estructuración del grupo encargado del desarrollo, implantación y mantenimiento del plan de contingencias.

8.1. Grupo de Desarrollo del Plan de Contingencia

Conformado por funcionarios de la Corporación integrantes del Comité Antitrámites y de Gobierno en Línea.

8.1.1. Responsabilidades

- Definir los lineamientos del plan de contingencias para los Sistemas de Información de la Corporación Autónoma Regional de La Guajira.
- Estudiar, evaluar y decidir sobre los requerimientos que se presenten en el desarrollo e implantación del plan.
- Recomendar acerca de la adquisición o el mantenimiento de equipos, programas e instalaciones.
- Coordinar el desarrollo, implantación y mantenimiento del plan de contingencias.
- Estudiar, evaluar y decidir sobre los requerimientos o recomendaciones planteadas al grupo de desarrollo.
- Aprobar el establecimiento de convenios, contratos o adquisición de recursos para el plan.
- Organizar y disponer los recursos para el grupo de desarrollo del plan.
- Transmitir las decisiones tomadas en torno a las acciones del Plan de Contingencias, los niveles de ejecución del Plan y el estado de los Recursos Informáticos que cubre el Plan.
- Monitorear y asegurar el cumplimiento estricto del Plan y del mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo.
- Proveer los recursos necesarios y notificar las decisiones a los funcionarios delegados.
- Delegar al funcionario encargado de la ejecución del Plan de Contingencias, quien será el Coordinador del Desarrollo del Plan de Contingencias.

8.2. Coordinador del desarrollo del plan de contingencias

Funciones

- Ejecutar, en tiempo y forma, cada una de las actividades planeadas.
- Documentar y formalizar el plan de contingencias.
- Ordenar la documentación inherente y los papeles de trabajo del proyecto.
- Diseñar planes de entrenamiento para los funcionarios de la entidad, a todo nivel, para que se involucren en las tareas del plan.
- Diseñar cronogramas y apoyar logísticamente las pruebas de cada segmento del plan.
- Mantener operativo y debidamente actualizado el plan de contingencias. El Coordinador del Plan y el funcionario Líder del proceso de Gestión de las TICs, elaborarán el plan de trabajo para el desarrollo e implantación del proyecto.

Así mismo, se conformarán los siguientes subgrupos de trabajo para la ejecución del Plan.

8.2.1. Subgrupo de Atención de Emergencias

Conformado por el encargado del **Sistema de Seguridad y Salud en trabajo**, el jefe de piso del área afectada o su suplente y el responsable (o su suplente) del procedimiento a seguir según el aspecto afectado. Estas personas son las designadas por el encargado del **Sistema de Seguridad y Salud en trabajo**. Este grupo se encargará de activar las medidas necesarias para salvaguardar los recursos humanos y materiales en caso de emergencias.

8.2.2. Subgrupo de supervisión

Conformado como mínimo, por **personal del área afectada** encargados de la operación de sistemas automatizados, el cual prestará apoyo e información al grupo de atención de emergencias, si así lo amerita. Encargándose, así mismo, de supervisar la situación del segmento no afectado por el siniestro en el momento de la contingencia y de informar al Líder del proceso de Gestión de las TICs y al coordinador del área de los sistemas afectados, para que apoye las labores de supervisión, dirija, participe en la ejecución del plan y la soporte técnicamente.

8.2.3. Subgrupo de evaluación de daños

Conformado por los mismos funcionarios del subgrupo de supervisión con el apoyo del Líder del proceso de Gestión de las TICS, quienes se encargarán de la revisión de la planta física, identificando los daños físicos y lógicos (Hardware y

Software) originados durante la contingencia, para luego, informar los resultados al grupo de desarrollo.

8.2.4. Subgrupo de Reorganización

Conformado por los funcionarios del área afectada; que forman parte del grupo de desarrollo, el cual se encargará de la evaluación de los daños y de la toma de decisiones pertinentes encaminadas al rescate progresivo de las funciones del área.

8.3. Grupo de Seguimiento y Control

Conformado por los funcionarios representantes de la Oficina Asesora de Control Interno, apoyados por el ingeniero coordinador de las labores del área afectada y que hace parte del grupo de desarrollo; quienes se encargaran de hacer seguimiento y control a las labores que se ejecuten, velando por el respeto del plan y la seguridad en su efectiva aplicación, así como la coherencia y consistencia en la aplicación de los procedimientos establecidos.

9. PLAN DE MITIGACION

Consiste en el establecimiento, desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas. Los cuales se resumen a continuación.

9.1. PROCESO DE RESPALDO

El Proceso de Respaldo establecido como procedimiento de Mitigación, a través del cual la Corporación asegura la conservación de su información vital y determina donde realizar sus trabajos críticos de procesamiento de datos en caso de falta o falla de sus equipos.

El diseño del proceso de respaldo incluye los cinco (5) principales componentes de un sistema de información, a saber:

- Los datos
- La documentación
- Los programas (software)
- Los procedimientos

- Los equipos (hardware)

9.1.1. 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 backups 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 entidad la instalación física que cumple con los requisitos de almacenamiento requeridos se encuentra ubicada en la Sede del Laboratorio.

9.1.2. Plan de Backups y Equipos de Respaldo

Un backup es una copia de seguridad de la información en un segundo medio (cinta – cartridge, 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.

9.1.3. Definición de Niveles de Backup

Los niveles de backup que se han establecido como política en la dirección de Informática son los siguientes:

- ANUAL: Debe realizarse al final de cada año (último día del año), es un backup total en un **medio de almacenamiento** que se guardan indefinidamente.
- SEMESTRAL: Debe realizarse al final de cada semestre un backup total (último día de cada semestre exceptuando el último día del año). Estos **medios de almacenamiento** se pueden denominar semestre1, semestre2 y se reutilizan anualmente.
- MENSUAL: Debe realizarse al final de cada mes un backup total (último día de cada mes exceptuando el último día del año). Estos **medio de almacenamiento** se pueden denominar mes1, mes2, mes3,…. mes12 y se reutilizan anualmente.

- SEMANAL: Se debe realizar al final de la semana (último día de la semana), es un backup total en cintas. Estos **medio de almacenamiento** se pueden denominar semana1,….semana4 y se reutilizan mensualmente.
- DIARIO: Se debe realizar al final del día, es un backup total de la información diaria en un **medio de almacenamiento**. Estos **medio de almacenamiento** se pueden denominar Lunes, Martes, Miércoles y Jueves y se reutilizan semanalmente.
- EN LINEA: Este backup se hace siempre y cuando se posea la infraestructura para copiar los archivos o directorios considerados como información vital al disco duro de un servidor remoto.

9.1.4. Procedimiento para Efectuar Backup o Copias de Respaldo a la Información de las Dependencias

Este procedimiento se realiza acorde con el procedimiento del Sistema de Gestión de la Calidad de la Corporación.

9.2. Centro de datos Alterno

Un centro de procesamiento de datos o centro de cómputo o en inglés Data Center, es la ubicación física donde se concentran todos los recursos de cómputo y comunicaciones, necesarios y esenciales para el procesamiento de la información de la entidad.

Dichos recursos consisten principalmente de equipos servidores de aplicaciones, servidores de bases de datos, servidores de correo electrónico, servidores de autenticación, servidores de Internet, servidores de seguridad (Firewall, Proxy, antivirus), sistemas de almacenamiento centralizado de datos (SAN – Storage Área Network), servidores de respaldo/ recuperación y sistemas de comunicaciones (red de datos, switches, routers), entre otros.

El centro de datos o Data Center se constituye en un elemento esencial y estratégico para CORPOGUAJIRA teniendo en cuenta que los componentes allí contenidos, han requerido un alto nivel de inversión y concentran la información crítica para el funcionamiento de la entidad, razón por la cual, requiere ser protegidos en ambientes físicos y lógicos adecuados de disponibilidad, confidencialidad e integridad, que garanticen el uso por parte de los funcionarios y la ciudadanía en general.

La entidad no cuenta con un centro de datos alterno, pero se plantea la adecuación y habilitación de un espacio en la sede del Laboratorio con las

características físicas de seguridad, humedad, aireación propia para el correcto desempeño de los servidores y elementos activos de red.

Teniendo en cuenta que el centro de cómputo (Data Center) requieren condiciones ambientales adecuadas, suministro de potencia, comunicación y acceso permanentes, seguridad física y lógica de los elementos y sistemas de información, monitoreo las 24 horas al día, con elementos y personal especializado, y actualmente ninguna de las sedes de Corpoguajira provee este tipo de condiciones, las cuales requieren para su adecuación la inversión de recursos económicos y técnicos importantes, se plantea como alternativa contratar con una empresa especializada los servicios de arrendamiento de un sitio para hospedar o alojar el Centro de cómputo (Data Center) de la Entidad, en las condiciones ambientales, físicas y lógicas, que mitiguen los riesgos de daños a la infraestructura de equipos de cómputo y comunicaciones, y garanticen la disponibilidad, integridad y confidencialidad de la información de la Corporación.

10. 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.

10.1. SOFTWARE

10.1.1. Aplicaciones Críticas en Producción de Desarrollo Externo

Se establecen las acciones para contingencias con los aplicativos contratados con externos.

10.1.1.1. Software Financiero

Aplicación: PCT ENTERPRISE (Tesorería, Contabilidad, Almacén y Presupuesto)

- Se contrata anualmente con el proveedor la actualización, mantenimiento y soporte técnico del sistema financiero PCT ENTERPRISE, software integrado por los módulos de Presupuesto, Tesorería y Contabilidad
- El soporte técnico por un año, se tendrá asistencia técnica a permanente a través de distintos medios.
- Mantenimiento y capacitación presencial cada año.
- Soporte para montar en los servidores de PCT las bases de datos del aplicativo, y acceso remoto a los mismos, en caso de daño en los servidores de la Corporación.

Proveedores: PCT Ltda.
Usuario: Secretaría General, Coordinación Financiera.
Riesgos Asociados: Posible incumplimiento de los contratistas, Posibles Retrasos en Procesos Administrativos, Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.
Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes soluciones:

1. Instalar en un servidor de respaldo los aplicativos y montar sobre ellos la última copia de seguridad de la base de datos. Sin embargo esto requiere un esfuerzo económico en equipos y licencias.
2. Instalar en los servidores del proveedor del aplicativo la última copia de la base de datos y dar acceso remoto al aplicativo a través de internet.
3. Para el manejo de la Contabilidad, Tesorería, Activos Fijos e Inventarios, se plantea la implementación de Hojas de Cálculo Excel, para la información crítica y de producción diaria. Actualmente, algunos de estos procesos se basan en la implementación de este tipo de herramientas.
4. Contratar el mantenimiento de los productos Oracle, para el adecuado funcionamiento de PCT ENTERPRISE.

10.1.1.2. Software Nómina y Recursos Humanos

Aplicación: SIAN.

- Se contrata anualmente con el proveedor la actualización, mantenimiento y soporte técnico del aplicativo SIAN.
- El soporte técnico por un año, se tendrá asistencia técnica a permanente a través de distintos medios.
- Mantenimiento y actualización cada año.
- Soporte para montar en los servidores de SOLREDES LTDA las bases de datos del aplicativo, y acceso remoto a los mismos, en caso de daño en los servidores de la Corporación.

Proveedores: SOLREDES Ltda.
Usuario: Secretaría General, Talento Humano

Riesgos Asociados: Posible incumplimiento de los contratistas, Posibles Retrasos en Procesos Administrativos, Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.
Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes soluciones:

1. Instalar en un servidor de respaldo los aplicativos y montar sobre ellos la última copia de seguridad de la base de datos. Sin embargo esto requiere un esfuerzo económico en equipos y licencias.
2. Instalar en los servidores del proveedor del aplicativo la última copia de la base de datos y dar acceso remoto al aplicativo a través de internet.
3. Para el manejo de la Nómina, se plantea la implementación de Hojas de Cálculo Excel, para la información crítica y de producción diaria. Actualmente, algunos de estos procesos se basan en la implementación de este tipo de herramientas.
4. Contratar el mantenimiento de los productos Oracle, para el adecuado funcionamiento del SIAN.
5. Capacitar al funcionario en la herramienta en la cual fue desarrollada la aplicación.
6. Adquirir amplios conocimientos en el área normativa y en el área de liquidación.

10.1.1.3. Software de Gestión Documental

Aplicación: SICO
Estado Actual: El programa SICO es el software con que actualmente se utiliza para los procesos de radicación de correspondencia y gestión documental.
Proveedor: SOLREDES
Usuario: Secretaria General y Comunicaciones
Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.
Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes aplicaciones o soluciones:
Se plantea la implementación de un aplicativo sencillo, en hoja Electrónica o base de datos, para garantizar la continuidad de los procesos de radicación manual, llevando una continuidad en la radicación mientras se supera la situación de contingencia.

10.1.2. Aplicaciones Críticas en Producción de Software de Desarrollo Interno

Corresponde a los aplicativos bajo la responsabilidad directa del Proceso de Gestión de las TICs.

10.1.2.1. Banco de proyectos

Aplicación: BANPROY
Estado Actual: Software que permite controlar los administrar los proyectos presentados al banco de Proyectos de la Corporación.
Ing. Desarrollador: LUIS SAEZ
Usuario: Oficina Asesora de Planeación.
Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información.
Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de la aplicación actual, se implementará la elaboración de planillas y registro de los proyectos en una en una hoja de cálculo de EXCEL.

10.1.3. Software Ofimático

Estado Actual: La entidad en la actualidad cuenta a nivel de software con:

- Software Ofimático: Microsoft Office 2000 y Microsoft Office XP, Microsoft Office 2003, Microsoft Office 2010, Microsoft Office 2013.
- Software Operativo: Windows XP, VISTA, WINDOES 7, 8, 8.1 Y WINDOWS 10

Proveedor: Varios
Usuario: Todas las dependencias de la Entidad
Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Posible falla de equipos electrónicos y Hardware fuera de inventario.
Soluciones en contingencia: Ante la posible materialización de los riesgos se plantea la utilización de los medios originales del software existente para realizar las respectivas reinstalaciones.

10.2. HARDWARE

10.2.1. Computadores personales

Estado Actual: se encuentran en funcionamiento equipos de cómputo de escritorio y portátiles que se encuentran distribuidos en las diferentes dependencias de la entidad.
Usuario: Todas las dependencias de la Entidad
Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Contratación

o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles, Posible falla de equipos electrónicos y Hardware fuera de inventario.
Soluciones en contingencia: Ante la posible materialización de los riesgos, se plantea el uso del hardware existente, desarrollando un proceso de redistribución de equipos para cubrir de manera óptima las necesidades reales y críticas de las dependencias y por ende de toda la Entidad.

10.2.2. Equipos Servidores

Estado Actual: Corpoguajira 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 Computo 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, Posible incumplimiento de los contratistas, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles.
Soluciones en Contingencia: Se debe garantizar el mantenimiento preventivo/correctivo

10.2.3. Equipos Electrónicos

Estado Actual: Actualmente se cuenta con dos (2) UPS
Proveedor:
Usuario: Todas las dependencias de la Entidad
Riesgos Asociados: Posibles retrasos en procesos administrativos, demoras en la efectividad de algunas comunicaciones, problemas en el control de asistencia del personal, 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.

11. 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

Durante los primeros 5 días de interrupción prolongada del procesamiento de datos o desastre, si la interrupción del servicio va a ser por largo tiempo luego del

desastre, se debe poner en ejecución la fase de recuperación del siniestro en el Centro de Datos alterno externo.

La estimación del tiempo en que va a durar la interrupción del servicio, se obtiene una vez se ejecute la Fase de Emergencia y una vez se halla evaluado el alcance de las fallas que se presentaron. Dicha estimación la debe obtener el Coordinador del Plan de Contingencias, apoyado en el trabajo y resultados presentados por el grupo de desarrollo del Plan.

El Plan presupone que debe utilizarse un Centro de Datos alterno externo al edificio sede de la Corporación Autónoma Regional de La Guajira, si la emergencia afecta en forma general (en un 60% o más) las instalaciones físicas y técnicas con que se cuenta.

Durante los 5 días siguientes al desastre, deberán prepararse las copias de respaldo de aplicaciones y procedimientos automatizados utilizados por las diferentes oficinas usuarias afectadas. El plan busca que las capacidades del servicio inicial del procesamiento de datos sean restauradas en el sitio alternativo en el 5º día siguiente al desastre. La reestructuración total de las capacidades del procesamiento para la red en línea está contempladas en fases durante 5 días a 28 días hábiles.

11.1. 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 TICs.** 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. 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.

11.1.1. Grupo de Centro de Datos

11.1.1.1. Responsabilidades

- Mantener las especificaciones para las configuraciones de hardware que deben ser instaladas en los diferentes equipos del centro de cómputo alterno.
- Mantener y mejorar los procedimientos de recuperación de desastres del grupo de operaciones del computador.

- Evaluar la instalación del software del sistema (al momento de la recuperación) y de los datos con la asistencia del grupo de soporte técnico y de las aplicaciones en producción, en la forma usual.
- Implementar los procedimientos dados por otros grupos de recuperación para generar y/o almacenar materiales que deben estar fuera del edificio y son necesarios para la recuperación.
- Mantener la configuración de la red para todos los sistemas de comunicación de datos.
- Mantener un plano de la configuración de la red a ser implementada en el evento de un desastre.
- Evaluar los procedimientos de backup's para establecer los servicios de comunicación de datos en el evento de un desastre.

11.1.1.2. Coordinador del Grupo

El Coordinador del Centro de Datos de CORPOGUAJIRA es quien administra las operaciones de los sistemas.

11.1.1.3. Miembros del Grupo

- Grupo Centro de Datos
- Grupo de Atención a Usuarios.

11.1.2. Grupo de Atención a Usuarios

11.1.2.1. Responsabilidades Pre desastres

- Proveer procedimientos para crear copias legibles por los equipos, de todos los componentes del software del Sistema, librerías de software de aplicaciones, drivers y controladores de dispositivos, Software de instalación, actualización, utilitarios y antivirus.
- Ejecutar los procedimientos para mantener copias de respaldo en el centro de almacenamiento alterno con la información de las aplicaciones críticas, de los directorios de trabajo de cada una de las dependencias de la corporación y el recurso de software necesario para las mismas.
- Evaluar y Verificar el software de recuperación de desastres en la forma usual, en cooperación con el grupo de operaciones y el sistema de aplicaciones.
- Documentar cada evaluación de recuperación desde la perspectiva de las actividades del grupo de soporte técnico.

11.1.2.2. Coordinador del Grupo

- Coordinador del grupo de Atención a Usuarios.

11.1.2.3. Miembros del Grupo

- Grupo de Soporte de Atención a Usuarios
- Responsable de la operación de programas y comunicaciones.

11.1.3. Grupo de Análisis y Desarrollo

11.1.3.1. Responsabilidades Pre desastre

- Establecer procedimientos que permitan las revisiones de todo el software de aplicaciones en producción, para que sea almacenado y copiado rutinariamente en un sitio externo como parte de los procedimientos de backup de la operación del computador.
- Coordinar con los grupos de usuarios para asegurar que sus planes de acción en caso de desastre sean seguros, viables y actualizados con el fin de reflejar las operaciones actuales.
- Mantener una estrategia general, un plan y documentación para la evaluación de las aplicaciones luego de que la recuperación en el centro alterno se haya terminado por parte de los grupos de soporte técnico y de operaciones, pero antes de que los sistemas se coloquen de nuevo en producción.
- Coordinar con el grupo de operaciones el mantenimiento de los proyectos de las aplicaciones y la documentación en el lugar de respaldo.

11.1.3.2. Coordinador del Grupo

- Coordinador del Grupo de Análisis y Desarrollo

11.1.3.3. Miembros del Grupo

Ingenieros de planta y contratistas que hacen parte del Proceso de Gestión de las TICs, responsables de la aplicación en etapa de desarrollo y producción según esté establecido.

- Usuario final, responsable de la operación del programa.
- Funcionario Delegado de cada dependencia encargado de la supervisión de la aplicación.

11.2. RECUPERACIÓN DEL DESASTRE: PLAN DE ACCION

El Plan presupone que debe utilizarse un Centro de Datos alterno externo al edificio sede Principal de CORPOGUAJIRA 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.

11.2.1. 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.

11.2.1.1. Procedimientos de Emergencia en el Centro de Datos.

Si la naturaleza del desastre no da tiempo para apagar y evacuar, la prioridad más alta es la seguridad de las personas. Ellos deben salir inmediatamente del Centro de datos o del área afectada. En un caso de éstos, el siguiente paso es notificar inmediatamente al grupo de administración de emergencia (Grupo de Salud Ocupacional o sus delegados).

Si hay tiempo para apagar, se deben realizar las siguientes actividades, en el orden especificado:

1. Inicializar procedimientos de emergencia organizacional estándar (los establecidos por el Grupo de Salud Ocupacional).
2. Ejecutar procedimientos de apagado para los servidores y demás dispositivos del centro de datos.
3. Apagar luces y bajar tacos en las cajas de distribución
4. Notificar al grupo de Administración de Emergencia

11.2.1.2. Grupo de Administración de Emergencia de Gestión de las TICs.

- Jefe de la Oficina encargada del proceso de Gestión de las TICS.

- Coordinador Grupo de Análisis y Desarrollo
- Coordinador Grupo Línea de Atención a Usuarios
- Grupo Centro de Cómputo

11.2.1.3. Árbol telefónico de emergencia

El grupo de emergencia, o su designado, llamará a los líderes de grupo de recuperación de desastre con información actualizada de la situación del desastre, junto con la localización y hora de reunión del Grupo de Administración de Emergencia.

11.2.1.3.1. Líderes de Grupo

- Coordinador del Plan de Contingencias
- Grupo de Administración de la Emergencia
- Coordinador Centro de Datos

Estos líderes de grupo tendrán copias del Plan para el grupo, con la lista de las personas que lo conforman. El líder iniciará un árbol telefónico para contactar todos los miembros del grupo.

El Administrador asumirá la responsabilidad total del grupo de administración de emergencia. El Grupo de Administración de Emergencia hará una apreciación inicial de la extensión del desastre tan rápido como sea posible.

Será decisión del Grupo de Administración de Emergencia, si se inicializa el resto del Plan o no (Si se activa el Centro Alterno o no). Se espera que esto ocurra en un lapso de 4 horas después del desastre.

11.2.2. SEGUNDA FASE: Procedimientos 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.

11.2.2.1. Acciones

Dentro de las 6 horas siguientes al desastre se debe:

- Notificar a los usuarios la interrupción del servicio.
- Notificar al Centro de Cómputo Alterno, Administrador, Servicios de Soporte, Director y otros.
- Activar el procesamiento manual de las aplicaciones (si es necesario)
- Efectuar una evaluación de daños e identificar el equipo reusable para transferirlo al Centro de Datos Alterno.
- Notificar al Proveedor las configuraciones de Hardware y alistar los requerimientos.
- Notificar a todos los funcionarios del Área de Gestión de las TICs que están involucrados en el Plan.
- Seleccionar y catalogar las oficinas de servicio para el procesamiento de los reportes de respaldo.
- Inicializar las preparaciones ambientales en el Centro de Datos o Centro de Respaldo. (Eléctrica, protección contra incendio, extractores).
- Ordenar los circuitos para comunicación de datos en el Centro Alterno, si es necesario.
-

Dentro de las 24 horas siguientes al desastre debe:

- Contactar con el proveedor y ordenar el soporte tanto de hardware como de software
- Iniciar y coordinar los procedimientos de preparación del lugar para el Centro Alterno.
- Iniciar el ensamblaje de la documentación y medios magnéticos en el lugar de almacenamiento externo.
- Confirmar el soporte dado por el proveedor.
- Complementar el procesamiento de los reportes seleccionados en el Centro Alterno.

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:

- 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 4 días siguientes al desastre debe:

- Completar la preparación ambiental del Centro Alterno
- Recibir la documentación y el medio magnético de los lugares de almacenamiento en el Centro Alterno.
- Asegurar el ambiente físico en el Centro Alterno y establecer la seguridad de los datos.
- Restablecer los backups de datos de producción de las cintas de backups.
- Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
- Evaluar los sistemas operacionales
- Notificar a los usuarios el estado de la recuperación

Dentro de los cinco días siguientes al desastre:

- Asegurar la operación total de los sistemas críticos.
- Continuar la implantación por fases de la red de comunicación de datos

Dentro de los 28 días siguientes al desastre:

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

11.2.3. TERCERA FASE: Procesamiento en el Centro de Cómputo Alterno

Las actividades paralelas listadas abajo caracterizan las acciones a tomar durante esta fase empiezan cuando los sistemas críticos y las redes de computación son operativas y no se ha podido completar la restauración de los datos del sistema.

Esta fase continúa hasta que los servicios de procesamiento de datos son restaurados en el lugar u otro sitio permanente. En este momento es cuando se debe informar al personal de las actividades que han sucedido y la operatividad del plan. Los logs de recuperación del desastre se deben recolectar y analizar por parte del Grupo de Administración de Emergencia del Proceso de Gestión de las TICs. Deben realizarse preparaciones en la marcha para regresar al sitio original o alternativo.

11.2.3.1. 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

11.2.4. CUARTA FASE: Recuperación en el sitio original o alterno

Mientras que las operaciones se estén ejecutando en el Centro Alterno, se harán planes para la recuperación total en el sitio original. Si hay un desastre mayor, o si está dentro de los planes de la organización, se puede realizar la recuperación en un sitio alterno improvisado. Esta fase es muy similar a la descrita en la fase 3 pero en una localización permanente.

Los siguientes son los componentes procedimentales importantes de las actividades en esta fase:

- Decisiones en el tiempo y equipo de recuperación
- Preparar restauración del lugar
- Desarrollo de los procedimientos de recuperación para la localización permanente.
- Repetir los procedimientos de recuperación
- Asegurar el ambiente físico y establecer la seguridad de los datos
- Montaje de los sistemas
- Evaluación de los sistemas
- Convertir a procesamientos en producción
- Realizar auditoría post-desastre
- Preparar reclamación de los seguros
- Reportar a la administración

11.2.5. QUINTA FASE: Mantenimiento

Parte del mantenimiento del Plan será la Programación de sistemas requeridos para mantener los programas con los cambios sobre el tiempo, del hardware, software y aplicaciones. Esta es obviamente la clave para el futuro exitoso del plan.

La actualización de nombres, responsabilidades y números telefónicos de los participantes claves es además críticamente importante. El Plan será auditado para ver que estos detalles sean actualizados rutinariamente en el Plan y en todas sus copias.

12. IMPLEMENTACION DEL PLAN

Para la implementación del Plan, deben estar formalmente documentados, y en operación, los siguientes procedimientos:

- Retención y respaldo de archivos permanente y corriente de cada dependencia,
- software específico y operativo.
- Recuperación de errores y fallas del sistema
- Seguridad física y lógica
- Mantenimiento preventivo y correctivo de equipos
- Administración de personal en lo referente a las emergencias

En primera instancia, el presente plan debe ser puesto a consideración, revisión y aprobación por parte del Comité de Informática. Seguido, debe ser probado y simulado.

En segunda instancia, desarrollar un programa de entrenamiento a los sujetos y áreas directamente involucradas, aquellas que asumen responsabilidades y funciones dentro del plan.

Finalmente, debe adoptarse a nivel institucional mediante Acto Administrativo, es decir, reglamentado por Resolución emanada del despacho del Director General. Posteriormente, se debe recopilar bimensualmente las modificaciones al plan y realizar actualizaciones periódicas al mismo.

13. PLAN EXPERIMENTAL DE PRUEBAS

El plan de contingencias comprende, finalmente, el desarrollo de un plan experimental de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o, en caso contrario, se le deben efectuar ajustes para su funcionalidad.

El mayor énfasis será ejercido sobre las pruebas o simulacros, y sobre los eventos posteriores a la emergencia relacionados con el reinicio de las operaciones normales de la **Corporación Autónoma Regional de La Guajira**.

Los siguientes son los objetivos de control y auditoria de las pruebas del plan:

- Validar la habilidad de los funcionarios y la consistencia de los procedimientos en eventos de recuperación de siniestros.

- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar y corregir fallas en el plan.
- Facilitar la divulgación y el entrenamiento en los procedimientos y guías de recuperación
- Fomentar el respeto por el plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias
- Estar preparado para evaluar las necesidades de seguros y reducir al máximo los costos en primas de aseguramiento.
- Motivar a los funcionarios involucrados en el diseño y desarrollo del plan a mantener actualizados los procedimientos inherentes

La Oficina Asesora de Control Interno evaluará que sean definidas las responsabilidades de las pruebas del plan.
La Oficina Asesora de Control Interno conocerá la frecuencia de las pruebas y la periodicidad de cambios en el ambiente informático o cualquier ajuste en el mismo.
El Jefe de la Oficina encargada del proceso de Gestión de las TICS y el Jefe de la Oficina Asesora de Control Interno, identificarán y documentarán los diferentes niveles de prueba del plan. Estos pueden ser por segmentos, por áreas relacionadas o a gran escala; éste último, como prueba global del plan, según los lineamientos que establezca el comité de Gobierno en Línea. Como métodos de prueba, se sugieren: en papel, real o a gran escala probado por segmento mediante simulacro a criterio del comité directivo con apoyo del grupo de desarrollo. La Oficina Asesora de Control Interno conocerá los períodos de prueba.

13.1. PASOS PARA CONDUCIR LA PRUEBA

El grupo de desarrollo del plan indicará a la Oficina Asesora de Control Interno el esquema ordenado de las pruebas, teniendo en cuenta:

1. Selección del sujeto de la prueba para identificar los aspectos o capítulos del plan que están siendo evaluados
2. Descripción de los objetivos de la prueba y mecanismos de medición del alcance exitoso de los objetivos
3. Reunión con el comité directivo para explicar la prueba y sus objetivos, y obtener como resultado su acuerdo y soporte
4. Comunicación formal de una prueba anunciada, de los factores críticos a considerar y el tiempo estimado de la prueba.
5. Consolidación de los resultados de la prueba al final de ésta.
6. Evaluación de resultados: progresos, inconvenientes y logros.

7. Determinación de las implicaciones de los resultados de la prueba. Se debe analizar si el resultado de un caso simple (segmento) puede tomarse como referencia para la realización satisfactoria de todos los capítulos del Plan (a gran escala)
8. Generación de recomendaciones para cambios o ajustes, definición de la fecha límite para respuesta y gestión
9. Notificación de los resultados de las pruebas al comité directivo y por su intermedio al nivel directivo de Corpoguajira.
10. Cambios en documentación o manuales, si es aplicable.

13.2. **AREAS O PARTES A PROBAR**

- Recuperación del sistema aplicativo individual utilizando archivos y documentación almacenada en el sitio externo
- Habilidad para procesar en modo “degradado” o limitado
- Recarga de los discos del sistema y de los procedimientos de carga y arranque utilizando archivos y documentación almacenada en el sitio externo
- En sitios de procesamiento alterno, solución de diferencias en configuración de equipos
- Disponibilidad de equipos periféricos y de procesamiento
- Disponibilidad de equipos de soporte: aire acondicionado, unidades de potencia no interrumpida de corriente eléctrica
- Disponibilidad de soporte logístico: provisiones, transporte y comunicaciones.
- Evacuación del equipo desde el Centro de Datos de la Entidad, en respuesta a eventos tales como inundación o terrorismo.
- Habilidad de la administración y del comité directivo para determinar la prioridad de sistemas cuando se procesa con recursos computacionales limitados.
- Habilidad para recuperar y procesar en forma satisfactoria sin personal clave, asumiendo la pérdida del personal o turnos primarios.
- Habilidad para adaptar el plan a desastres menores.
- Efectividad de alternativas manuales para aquellos sistemas que confían en esa opción.
- Habilidad de entrada de datos para alimentar sistemas críticos utilizando las instalaciones del área de soporte externo.
- Habilidad de los usuarios para continuar con las operaciones normales de la entidad para los sistemas clasificados como no críticos.
- Habilidad para establecer contacto en un período definido por emergencia y de manera organizada, con el personal clave o sus designados alternos.

- Nivel de cumplimiento de los estándares normativos aprobados por la entidad.
- Identificación de los recursos utilizados durante la emergencia que son cubiertos por la póliza de seguros.
- Distribución correcta y oportuna de listados, transmisión de datos vía telefónica conmutada, servicios de correo.
- Disponibilidad de formas y cantidad mínima de papelería. Control de formas numeradas o asimilables a títulos valores.
- Adherencia nula, parcial o total a medidas de seguridad durante el período de emergencia.
- Habilidad para ejecutar tareas de evacuación y tratamiento de primeros auxilios.
- Mecanismos para recuperación de información perdida en caso de sistemas en línea.
- Análisis de tiempos y movimientos durante las pruebas.

13.3. PROCESO GENERAL PARA PRUEBA ANUNCIADA

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

13.4. PROCESO GENERAL PARA SIMULACRO

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

14. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad de información son la piedra angular de la eficacia de la seguridad de la información, sin una política sobre la cual basar los estándares y procedimientos, las decisiones tomadas serán probablemente inconsistentes y los agujeros de seguridad estarán presentes listos para ser explotados por personas internas y externas a la organización.

Esta es una primera fase en la implementación de políticas, para evaluar su aceptación y cumplimiento en la organización.

14.1. REINICIALIZAR O RESTAURAR SU SISTEMA

Los propietarios de los sistemas de información deben asegurarse de la existencia de un backup completo y que los procedimientos de recuperación de sistemas están en su sitio.

Descripción: Facilita las instalaciones para asegurar que su equipo reinicie exitosamente después de una interrupción voluntaria o involuntaria.

- No tener disponible el sistema después de una interrupción en el proceso normal puede impactar la eficiencia en las operaciones de la entidad.
- La pérdida de información después de una interrupción en el proceso normal, puede interrumpir las operaciones y retrasar los procesos de la entidad.

14.2. PANTALLA SIN INFORMACIÓN VISIBLE

- Los usuarios de los computadores de Corpoguajira deben asegurarse que su monitor o pantalla se encuentre en blanco, cuando el usuario no la esté utilizando.
- Si la pantalla es legible cuando el usuario se encuentra ausente de su escritorio o de su lugar de trabajo, esto podría dar como resultado que la información confidencial (sensible) pueda ser leída por personal no autorizado.
- Cuando el personal puede ver como un sistema confidencial es accesado, esto puede facilitar su premeditación a intentos oportunos para leer y copiar los datos cuando el computador es abandonado aunque sea por un corto periodo.

14.3. MANEJO DE BACKUPS Y PROCEDIMIENTOS DE RECUPERACION.

El backup de los archivos de información de la organización y la habilidad para recuperar información es una prioridad alta. La administración es responsable por asegurar que la frecuencia de cada operación de backup y los procedimientos de recuperación se ajusten a las necesidades de la organización.

Los procedimientos usados para iniciar una recuperación deben ser claramente documentados y probados. Si los procedimientos de restauración no han sido probados, una restauración parcial o incompleta puede corromper la integridad del sistema.

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.

- Modificaciones maliciosas, de los resultados de la secuencia diaria del backup dentro de una falla para proteger todos los datos requeridos.

14.4. ARCHIVAR INFORMACIÓN

Los medios de almacenamiento usados para archivar la información deben ser apropiados de acuerdo a las expectativas de vida de la información. El formato en el cual es almacenada la información debe ser cuidadosamente considerado, especialmente cuando los formatos propios están implicados.

Se hace referencia a la información la cual no es requerida en el día a día, pero la cual necesita ser guardada por un cierto periodo y también información la cual debe ser guardada perpetuamente. Los datos que son removidos del procesamiento cotidiano, reducen los niveles de almacenamiento y de recursos de procesamiento.
Las recomendaciones que deben ser consideradas cuando se implemente esta política incluyen lo siguiente:

- Las debilidades en la longevidad de los medios usados para archivar, pueden causar fallas en la restauración de los datos cuando eventualmente sean requeridos.
- Los datos archivados pueden ser conservados a menudo en un formato del usuario que sea apoyado solamente por los sistemas actuales, así intentos frustrados de acceso.

14.5. ENVIO DE CORREO ELECTRONICO

El e-mail se debe utilizar solamente para los propósitos institucionales, usándolo en términos que sean consistentes con otras formas de comunicación de la Entidad.
Los archivos adjuntos a un e-mail se pueden adjuntar solamente después de confirmar la clasificación de la información que es enviada y después de explorar y verificar que el archivo no posee virus o código malévolo.

Descripción

- El uso de correos electrónicos se ha hecho tan popular hasta el punto donde es obligatorio para todas las compañías ser acusadas a través de este medio. La carencia inherente de seguridad para enviar mensajes, información, archivos o instrucciones aparentemente es ignorado por muchos usuarios que utilizan este servicio.

- Enviar e-mail usando firmas digitales (opcionalmente encriptado) es una forma de asegurar su validez e integridad. El contenido de correos electrónicos recibidos sin autenticación podría ser considerado poco fiable.
  1. La transmisión de un virus puede no solamente causar daño en los equipos sino que puede dañar permanente la reputación de la organización.
  2. Enviar un e-mail vía líneas públicas (por ejemplo internet) puede comprometer la confidencialidad e integridad de la información que está siendo transmitida. Esto es similar a una carta postal porque cualquiera que la pueda abrir, la puede leer.
  3. Archivos confidenciales podrían ser transmitidos por e-mail como adjuntos, rompiendo así la confidencialidad y potencialmente ocasionando pérdidas financieras.
  4. Enviar una copia de archivos a los colegas dentro de la red interna, crea duplicados innecesarios y también compromete la integridad del documento o archivo original.

15. CONCLUSIONES

- En el presente Plan de Contingencias se describen los métodos y procedimientos a seguir en la Corporación Autónoma Regional de La Guajira – Corpoguajira en caso de presentarse desastres que destruyan, modifiquen o alteren la información y los equipos de cómputo que la procesan, con el propósito de proteger la información y asegurar la continuidad del procesamiento de la información necesaria para el adecuado cumplimiento de sus Objetivos Institucionales.
- Lograr integración de las diferentes sedes de la Corporación de tal forma que se ofrezca apoyo en sus centros de datos con la implementación de aplicaciones de propósito común, compatibles entre sí, garantizando el desempeño y continuidad en cada una de sus funciones.
- Concientizar a los funcionarios de la Entidad acerca de la seguridad de la información, labor que no es sólo del proceso de Gestión de las TICs, sino que debe comprometer a toda la organización.
- Con el desarrollo de este trabajo en CORPOGUAJIRA se establecen los perfiles acerca de las labores que ha de cumplir el grupo encargado del seguimiento del Plan de Contingencias.

16. RESPONSABLE DEL DOCUMENTO

Profesional Especializado de la Oficina Asesora de planeación Líder del Proceso Gestión de las TICS