MANUAL PLAN DE CONTINGENCIA DE LOS SISTEMAS DE INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCION

Los Planes de Contingencia permiten mantener la continuidad de los sistemas de información frente a eventos críticos, y minimizar el impacto negativo. Son parte integral de la organización y sirven para evitar interrupciones y prepararnos para fallas potenciales generando soluciones automáticas.

El alcance de este plan guarda relación con la infraestructura informática, así como los procedimientos relevantes de la Sección de Desarrollo de TIC con la plataforma tecnológica.

Este Plan debe ser parte integral de la organización y servir para evitar interrupciones y prepararnos para fallas potenciales generando soluciones automáticas.

El Plan de contingencia es una estrategia planificada con una serie de procedimientos que nos facilitan o nos orientan a tener una solución alternativa que permita restituir rápidamente el estado normal de los servicios y/o funcionamiento de la organización ante la eventualidad de todo lo que pueda paralizar, ya sea de forma parcial o total el sistema y los procesos de la Corporación.

Pese a todas las medidas de seguridad que se implementen, puede ocurrir un desastre ya sea natural o provocado, por tanto, es necesario que en este Plan de Contingencia se incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio en forma rápida, eficiente y con el menor costo y pérdidas posibles.

El plan de contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos informáticos y la información contenida en los diversos dispositivos de almacenamiento, reduciendo su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

REVISO:	**APROBO:**
Nombre y Firma: **FIRMADO EN ORIGINAL** Amilkar Correa Ojeda	Nombre y Firma: **FIRMADO EN ORIGINAL** Yancy Estella Hinojosa Ruiz
Fecha: 02 de enero de 2025	Fecha: 02 de enero de 2025

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un plan de contingencia lo más completo posible.

Lo más importante para una corporación y más para La Caja de Compensación Familiar de Arauca Comfiar, es el valor que tiene cada una de las personas que laboran en la Gran Familia Comfiar, por encima de cualquier equipo informático, información, infraestructura, (ACTIVO).

1. OBJETIVOS

Garantizar la continuidad de las operaciones de los elementos considerados como críticos que componen los sistemas de información de la Caja, tales como Servidores, redes de datos, infraestructura, etc.

Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen el sistema de información.

Establecer la normatividad correspondiente y los procedimientos necesarios para la recuperación rápida y confiable de la información contenida en los sistemas críticos del sistema de información.

Identificar los riesgos a los cuales pueden estar expuestas las personas e instalaciones de la Caja

1.1 CONCEPTOS GENERALES

- **Activo**: cualquier cosa que tiene valor para la Corporación.
- **Amenaza:** causa potencial de un incidente que puede producir daño a un sistema u organización
- **Análisis del riesgo**: procesos sistemáticos para estimar la magnitud de los riesgos.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni se divulgue a individuos, entidades o procesos no autorizados.

- **Evaluación del riesgo**: proceso total de identificación, control y eliminación o minimización de eventos inciertos que pueden afectar los recursos de los sistemas de tecnología de la información y comunicaciones.

- **Sistema informático:** Utilización de computadores para almacenar datos de una organización, procesarlos y ponerlos a disposición de la misma.

- **Sistema de información:** Conjunto de personas, equipos de cómputo, software, datos y procedimientos que interactúan para satisfacer las necesidades de información y la toma de decisiones.

- **Switch**: Es un elemento activo de comunicación que utiliza Comfiar, el cual es un elemento que permite la transmisión de tramas (paquetes de datos) desde la tarjeta de Red del Transmisor a la tarjeta de Red del Receptor.

- **Router**: Dispositivo que permite interconectar redes con el mismo o distinto prefijo en su dirección IP, estableciendo la mejor ruta de destinará a cada paquete de datos para llegar a la red y al dispositivo de destino.

- **Acces Point**: O punto de acceso inalámbrico WAP, es un dispositivo que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas.

- **Sistema de recuperación de energía eléctrica:** Utilización de UPS en los equipos con mayor preponderancia dentro de nuestro sistema.

- **Servidor**: Equipo de cómputo central encargado de suministrar servicios informáticos a otros computadores, como por ejemplo programas y datos.

- Backup: es una copia de seguridad que se realiza frecuentemente a los datos, archivos o información CRITICA, el cual se use los mecanismos o tecnología adecuadas para salvaguardarla y restaurarla en caso de requerirse.

2. INVENTARIO DE RECURSOS INFORMATICOS DE CONSIDERACIÓN CRÍTICA EN COMFIAR

2.1 DEFINICIÓN DE RECURSOS INFORMÁTICOS

Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento y la Optimización del trabajo con Ordenadores y Periféricos, tanto a nivel Individual, como Colectivo u Organizativo, sin dejar de lado el buen funcionamiento de los mismos.

En resumidas cuentas, cuando hablamos de hardware nos referimos a todos esos componentes físicos y palpables de los cuales se compone un PC, como por ejemplo una tarjeta de memoria, monitor, un Disco Duro, o la Placa Base (que junto con el procesador forman parte del corazón de un computador).

Por otro lado, Software sería todo aquello de lo que compone el Sistema Operativo, o dicho de otra manera, todos los programas del entorno Windows, Linux, etc (Windows, Office, antivirus, etc.)

2.2. INFRAESTRUCTURA TECNOLÓGICA.

2.2.1. SERVIDORES (HARDWARE)

- **Servidor Aplicativos Internos Sisu**

    - Hardware: HP Proliant ML350 G6: Servidor Aplicaciones de módulos SYS: Asamblea, tesorería, activos, presupuesto, servicios, suministros, conciliación, contabilidad, créditos, fosfec, generales, Aportes, Subsidios. Nomina, promoción, fovis,suministros vivienda Comfiar, vivienda gobernación, Colegio, auditoria, asamblea, estadística, xml y SAT.

    - IBM xSeries 226 Serve: Servidor Aplicaciones SYS de contingencia con todos los módulos nombrados anteriormente

    - **Sistema Operativo:** Ububtu 18.04 (sistema operativo de libre distribución)

    - **Bases de Datos:** MySQL Database Version 5.7 y PHP 5.3 (software de libre distribución)

➢ **Procesos**

- **Aportes y Subsidio:** Liquidación de Subsidio Familiar monetario, Recaudo de aportes parafiscales, Afiliación de empresas, trabajadores y beneficiarios, Generación estadística poblacional, etc.

- **Contabilidad:** Causación y contabilización, pagos a proveedores, activos, cartera, facturación, recaudos, etc.

- **Nómina:** Liquidación nómina mensual de empleados, procesos de liquidación, dependencias, niveles, cargos, grupo familiar, pagos, reportes, liquidación, etc.

- **Asamblea:** Creación asambleas, temas de votación, datos de los concejeros, registro de poderes, registro de asistencias, reportes generales, etc.

- **Créditos:** Mantenimiento datos básicos, mantenimiento de créditos, abonos a créditos, mantenimiento de movimiento, reportes de cartera, consulta de movimientos, etc.

- **Fosfec:** Radicación de formularios, Registro de empresas y trabajadores, Microcréditos pequeñas y medianas empresas, Subsidio para trabajadores y desempleados, Servicios para trabajadores y desempleados, etc.

- **Tesorería:** Datos básicos, recibos de caja, facturas, recibos y egresos, reportes, terceros, consignación, cheques, transferencias electrónicas, etc.

- **Activos:** Activos, tipos de activos, clases de activos, áreas y dependencias, permisos, cambio de terceros, bajas, traslados, traslados masivos por trabajador, deterioro individual, inventarios, cargue inventario por trabajador, reclasificación activo no corriente, reportes contables, reportes de baja, reportes generales, etc.

- **Presupuesto**: Movimiento CDP, formulación presupuestal, ejecución presupuestal, ejecución estado resultado, listado de reserva presupuestal, presupuestos proyectos, CDP´s, etc.

- **Servicios:** Parametrización de servicios, asignación de roles y permisos, capturas básicas, captura de servicios, ventas de servicios, registro masivo, reportes, etc.

- **SAT**: configuración SAT, configuración CCF, servicio aportes SAT, servicio aportes CCF, servicios subsidio SAT, servicios subsidio CCF, etc.

- **Conciliación**: cargar extractos, consultar extractos, proceso de cruce parcial, proceso de deshacer parcial, conciliación personalizada, revertir transacción, proceso de conciliación, reportes, etc.

- **Fovis:** Parametrización básica, fondo de vivienda, oferta de subsidio de vivienda, demanda de subsidio de vivienda, cruce y retiro de postulaciones, calificación y asignación de subsidios, novedades de los subsidios, reportes generales de vivienda, interface contable, consulta de subsidios, reportes, Régimen especial de aportes, etc.

- **Generales:** Mantenimiento de países, departamentos, ciudades Mantenimiento de opciones, usuarios y trabajadores Mantenimiento de los datos generales básicos Mantenimiento aplicativos, consecutivos, impresoras Datos generales de la empresa que utiliza módulos, etc.

- **Promoción:** Niveles de satisfacción, Clientes para promoción, Servicios para promocionar, Regalos para clientes, Cotizaciones de servicios, Calificación de ventas y visitas, Reportes generales de promoción, etc.

- **Suministros:** Áreas de suministro, Artículos, Consulta el movimiento de un artículo, Proveedores, Órdenes de compra, Movimiento de artículos, Listados generales de artículos, Interfaz contable y otros procesos, Ordenes de servicios generales, etc.

- **Vivienda – Fovis:** Fondo de vivienda fovis, Oferta de subsidio de vivienda, Cruce y retiro de postulantes, Novedades de los subsidios de vivienda, Reportes generales de vivienda, etc.

- **Colegio**: Ingreso de matrículas, dirección general, dirección académica y disciplina, docentes, tesorería, menú reportes, generación de estadísticas, reportes estadísticos y formatos Xml, boletín del alumno, menú migración, reportes, etc.

- **Servidor Firewall**

  - **Hardware**: RouterBoard Mikrotik RB4011iGS+este elemento de software y hardware utilizado para la protección de la red, según políticas definidas por la sección de sistemas en función a las necesidades de esta corporación.

  - **Sistema Operativo**: Sistema Operativo Mikrotik Versión v 5.5 on x86

  - **Procesos**: Firewall, PPPOE, NAT, PAT, Lista de acceso, Protocolo Layer 7, Web Proxy, Servidor DHCP, Servidor Procesos Varios.

- **Servidor de Respaldo**

  - Hardware: HP ProLiant DL160 G5

  - Sistema Operativo: servidor con sistema operativo Linux Version Ubuntu 18.04

  - Procesos: Backup's, Antivirus Karpersky Business Space Security.

- **Servidor Voz IP - Asterix**

  - Hardware: Elastix ELX-3000: servidor digital de VozIp que permite administrar una centralita telefónica.

  - Procesos: Gestionar extensiones y efectuar llamadas sin pasar por el operador telefónico, dando así servicios de telefonía inteligente mediante reconocimiento de voz utilizando el protocolo IP, los cuales brinda servicios como PBX, FAX, E-MAIL, Reportes, agenda, mediante la utilización de teléfonos IP o *softphone* y el protocolo SIP.

- **Servidor CCTV – Circuito Cerrado de Televisión (CCTV)**

  Hardware: Copumax Intel Pentium: el sistema de seguridad de COMFIAR tiene como componente fundamental el Circuito Cerrado de Televisión (CCTV) el cual está compuesto por un sistema de 14 cámaras fijas y 2

Domos con detección de movimiento, ubicados estratégicamente de acuerdo al resultado que arrojó el estudio de seguridad físico en las instalaciones de la sede administrativa de la caja.

2.2.2. DISPOSITIVOS DE INTERCONEXIÓN DE REDES

- **Switches**: CRS354-48G-4S+2Q, CRS317-1G-16S+RM, CRS328-24P-4S+RM, Cisco CATALYST2900, Cisco SF300-24P, Trendnet TK-401R, TEG-S240TX, TL-SF1016D, HPE 1420 24G, DES-1024D, RB 260GSP

- **Router**: RB3011 UIAS-RM, RB951G-2HND, LinkSys WRT300N, RB 4011IGS+RM, RB 2011VIAS-2HND-IN, CRS112-8G-4S-IN

- **Acces Point**: BASEBOX 2(ROUTER BOARD 912UAG), WAP 2.4 GHZ RBWAP2ND-BE, RB962UI-GS

2.2.3. FUENTES DE SUMINISTRO ELÉCTRICO

➢ UPS (Standby Power System)

- 1 UPS de 3 KW marca QUEST encargadas del sistema de recuperación energética de nuestro sistema.
- 1 UPS 3 KVA tripp lite encargadas del sistema de recuperación energética de nuestro sistema.

2.2.4. GENERADOR DE CORRIENTE ELÉCTRICA.

Está compuesta por los siguientes componentes

➢ Generador eléctrico PERKINS series 1000 con motor Diesel Andinos de 6 cilindros
➢ Generador Stamford.
➢ Tablero de transferencia automática con falla de suministro 704

➢ **Medidas Generales De Seguridad Para Motor Perkins**

- No cambiar las especificaciones del motor
- No fumar cuando se está llenando el dispositivo de combustible
- Limpiar cualquier derrame de combustible. Si algún material se ha ensuciado de combustible, se debe poner en un lugar seguro.
- No llenar el depósito de combustible con el motor encendido (a menos que sea absolutamente necesario).
- No realizar algún tipo de ajuste si no sabe cómo hacerlo.
- Mantenga a una distancia segura a otras personas durante el funcionamiento del motor o del equipo auxiliar.
- Mantener alejado de piezas en funcionamiento prendas de vestir sueltas o el cabello largo.
- No poner en marcha el motor si se ha retirado alguna pieza de las defensas de seguridad.
- Desconecte los terminales de batería antes de realizar cualquier reparación en el sistema eléctrico.
- Debe haber una persona solamente a la vez al mando del motor.
- No permita que la piel entre en contacto con el aire comprimido. Si el aire comprimido penetra en la piel, buscar inmediatamente asistencia médica.
- Poner el mayor cuidado posible a la hora de realizar reparaciones de emergencia en acondiciones adversas.
- No llevar prendad de vestir que se hayan ensuciado de aceite.
- Desechar el aceite y refrigerante usado de acuerdo con la normativa local para evitar la contaminación.

➢ **Mantenimiento preventivo**

- Intervalos de mantenimiento preventivo: Estos intervalos de mantenimiento preventivo corresponden a unas condiciones de funcionamiento generales. Se debe comprobar los intervalos aconsejados por el fabricante del equipo en el cual está instalado el motor.
- Como parte de un buen mantenimiento preventivo, se debe comprobar si hay fugas o elementos de sujeción sueltos en cada revisión

➢ **Programas de mantenimiento**

- El motor debe ser controlado solamente desde el panel de control o desde la posición del operario.
- Las demás características del mantenimiento se deben aplicar de acuerdo al manual de usuario de Perkins Serie 1000

2.2.5. SOFTWARE

El software instalado por la Caja de Compensación Familiar de Arauca es licenciado para cada equipo de cómputo o servidor instalado, también se usa sistema operativo de software (libre distribución – GNU).

- En servidores: Linux distribución Ubuntu y Centos. Windows Server.
- Equipos de cómputo: Linux, Windows (últimas versiones).
- Ofimática: Office Profesional (últimas versiones).
- Antivirus: Kaspersky Endpoint Security.

2.2.6. LICENCIAS

- Windows para equipos de cómputo y servidores
- Office Profesional o Enterprise.
- Kaspersky Endpoint Security
- Certificados de seguridad Web SSL
- Hosting de Dominios Corporativos

3. ANÁLISIS DE RIESGOS

Es difícil determinar con precisión la totalidad de los riesgos que pueden afectar la continuidad de las operaciones en cada una de las sedes con las que cuenta la Caja de Compensación Familiar de Arauca Comfiar.

El análisis de riesgos al cual se enfrenta la corporación, supone más que el hecho de observar la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos.

Se tiene en cuenta la probabilidad de que sucedan cada uno de los problemas posibles, de esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ¿Qué se intenta proteger?

  - Los activos
  - La información
  - Infraestructura

- ¿Frente a qué se intenta proteger?

  - Al fuego, que puede destruir los equipos y archivos.
  - Al robo común, llevándose los equipos y archivos.
  - Al vandalismo, que dañen los equipos y archivos.
  - A fallas en los equipos, que dañen los archivos.
  - A equivocaciones, que dañen los archivos
  - A la acción de virus, que dañen los equipos y archivos.
  - A terremotos, inundaciones que destruyen los equipos y los archivos.

Tomando como referencia uno de los ítems (Al robo común, llevándose los equipos y archivos). Se pueden realizar las siguientes preguntas:

- ¿En qué tipo de vecindario se encuentra el centro administrativo?

  - La caja de compensación familiar de Arauca “COMFIAR” se encuentra ubicada en una zona comercial y residencial, pero en las horas nocturnas es en muy poco el flujo de tránsito y de personas.
  - No se encuentra en el anillo de seguridad dispuesto por las entidades de control y seguridad del municipio de Arauca.
  - La Estación de Policía de Arauca está ubicada a 300 metros aproximadamente.
  - A una distancia aproximada de 800 mts, se encuentra ubicado El Comando Departamental de la Policía Nacional.
  - La brigada 18 del Ejercito Nacional se encuentra ubicada a una distancia aproximada de 1 kilómetro de distancia
  - Las instalaciones de SALUDCOOP se encuentra ubicada a tres (3) minutos de recorrido, centro médico de nivel 1.
  - Se localiza el Hospital San Vicente de Arauca la cual brinda atención médica de nivel 1, a 300 metros.

- ¿Las computadoras se ven desde la calle?

Si, principalmente los que están ubicados en la primera planta, en las oficinas con ventanas externas que tienen visibilidad hacia la calle frontal

- ¿Hay personal de seguridad en la Institución?

Se cuentan con un servicio de vigilancia privada que garantiza la seguridad a los activos, trabajadores y visitantes de las instalaciones, y así poder tener suficiente cubrimiento, completo, efectivo y eficiente del cúmulo de funciones que se le han asignado.

- ¿Cuántos vigilantes hay?

Existen tres vigilantes con dos turnos diarios, de 12 horas cada uno, uno por turno
¿Los vigilantes, están ubicados en zonas estratégicas?

Se ubican en la entrada principal de la corporación, con fácil movilidad en toda la infraestructura.

- ¿Existe Circuito Cerrado de Televisión CCTV?

Se cuenta con un sistema de circuito cerrado de televisión (CCTV) monitoreado por personal capacitado cubriendo todas las áreas necesarias para mantener vigiladas las instalaciones.

- ¿Existen planes de emergencia y/o de evacuación?

Al momento se cuenta con un plan de emergencia, evacuación, en el interior o exterior de la edificación se encuentran señalizaciones, luces de emergencia, rutas diseñadas y demarcadas para una evacuación en caso de alguna eventualidad, en razón a esto se han realizado simulacros de evacuación y emergencia.

- ¿Cuáles son los delitos más comunes en la zona?

  - El hurto.
  - Lesiones personales.
  - Robo de residencias.
  - Robo de establecimientos comerciales.

Observaciones

- Los vehículos que ingresen al parqueadero no son sometidos a inspección de seguridad con todas las medidas del caso y todos los medios logísticos necesarios para el cabal cumplimiento de esa función.

- No posee detectores de metales de arco, no tienen detectores manuales ni un guarda de seguridad que puede manipular dichos elementos.

- Los funcionarios que laboran en esta corporación portan su identificación a la vista que los identifique como servidores de la caja de compensación familiar de Arauca COMFIAR

- Se recomienda realizar un programa permanente de verificación de instalaciones eléctricas, por ningún motivo en ningún sitio las instalaciones se debe permitir la improvisación de instalaciones eléctricas.

- El personal de vigilancia debe mantener siempre las llaves de las puertas de emergencia y conocer los respectivos procedimientos a realizar en casos de emergencia (antes - durante - después de la emergencia).

4. PROTECCIONES ACTUALES

La Caja de Compensación Familiar de Arauca Comfiar tiene las siguientes protecciones:

4.1. Respaldo de la información: Backup

Se realizan diariamente copias de respaldo de la información y de software.

- Se tiene servidor de copias de seguridad (Backup) local, donde se guarda toda la información que es generada por los trabajadores (ofimáticos y otros) y las fuentes y datos de las diferentes plataformas que tiene Comfiar en propiedad y o terceros.
- Se tiene servicio en la Nube donde se envían en manera inmediata las copias generadas en el servidor local de Copias de Seguridad.

Las copias de seguridad tendrán como consideración los siguientes lineamientos:

- El respaldo de los datos del aplicativo interno de la Caja, se realiza diariamente de la base datos y cada viernes de las fuentes del software.
- Se Clasificó y definió los niveles necesarios para la información de respaldo. Con excepción a los funcionarios de recreación y deportes, publicidad y mercadeo, eventos y programas especiales, ningún otro funcionario tendrá derecho a realizar el respaldo de imágenes, música y videos (contenido multimedia), el restante de funcionarios solamente se les salvaguardará archivos tales como documentos con extensiones (doc, docx, docm, txt, pdf, ppt, pptx, ppsx, sldx, xls, xlsx, csv).
- No se debe guardar respaldo de archivos personales

Se usará el siguiente método de copias de seguridad:

- Primero se crea una carpeta dentro del disco local (D:) la cual contenga todo el contenido a realizar el proceso de copia de seguridad según las consideraciones y clasificaciones vistas anteriormente.
- La primera copia o Backup es completo. Se crea una copia de resguardo de todas las carpetas y archivos que contenga la carpeta del disco D en la herramienta para hacer el Backup. Es ideal para crear la primera copia de todo el contenido de una unidad o bien de sus archivos de datos solamente.
- Después procedemos a realizar el Backup diferencial el cual compara el contenido de los archivos a la hora de determinar cuáles se modificaron de manera tal que solamente copia aquéllos que hayan cambiado realmente y no se deja engañar por las fechas de modificación de los mismos.
- Esta copia de seguridad se realizará diariamente una vez sea creado el archivo o que registre alguna novedad.
- Ningún documento magnético que tenga información de interés institucional podrá ser difundido, distribuidos o comercializados.

4.2. Robo Común

Para evitar el robo de activos e información de personas ajenas a los que trabajan en las oficinas de esa corporación, se aseguran todos los cajones de los escritorios, se mantienen las puertas cerradas con llaves y se apagan los computadores tan pronto termine el horario laboral.

4.3. Falla de los Equipos

Al inicio de cada año se realiza un cronograma de mantenimiento preventivo para el primer semestre y se repite el mismo en el segundo semestre, estableciéndose dos mantenimientos anuales para cada equipo, así mismo si en algún momento ocurre algún daño con esta herramienta de trabajo, se procede a realizar mantenimiento correctivo.

Como protección a los equipos se establece que el puesto de trabajo esté totalmente limpio para evitar el polvo, no se permite el consumo de bebidas, comidas ni cualquier líquido en las estaciones de trabajo.

Se tiene instalado un software antivirus licenciado con las bases actualizadas para la protección de virus que es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus pueden destruir, de manera intencionada, los datos, programas e información almacenados en los computadores. Es vital que, al introducir un dispositivo externo, ya sea Pendrive o memoria USB, discos duros externos, CD´s, etc, se escanee o vacune para eliminar cualquier amenaza de virus que altere el óptimo funcionamiento de la herramienta de trabajo.

5. PLAN DE RECUPERACIÓN

En el momento que ocurra un desastre y se active la contingencia, es necesario conocer al detalle el motivo que lo originó y el daño producido, lo que permitirá en el menor tiempo posible el proceso perdido.

Los procedimientos son obligatorios ejecutarlos bajo la responsabilidad de los funcionarios de la Sección de Desarrollo de Tic de la Caja de Compensación Familiar de Arauca Comfiar.

5.1. Actividades Previas al Desastre

Se puede identificar los siguientes bienes afectados a riesgos

- Personal
- Hardware
- Software
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de servicios de telecomunicaciones
- Infraestructura

5.2. Establecimiento del Plan de Acción

Se establece los procedimientos relativos a:

- **Equipos de Cómputo**: La sección de Desarrollo de Tic de la Caja de Compensación Familiar de Arauca Comfiar, cuenta con un inventario actualizado de todos los equipos de cómputo, especificando el propietario en ese momento.

  En caso que el daño sea a una escala mayor se procede a reemplazar temporalmente el equipo de cómputo con uno de contingencia que le será adecuado con los programas que permite el pleno funcionamiento de las labores asignadas al funcionario afectado; así mismo, con la información restaurada desde las copias de seguridad (backups)

- **Obtención y almacenamiento de los Respaldos de Información (BACKUPS):** Se tiene establecido los procedimientos para la obtención de copias de Seguridad de todos los elementos de software e información necesarios para asegurar la correcta ejecución del Software y/o sistemas operativos que posee la Caja de Compensación Familiar de Arauca. Para lo cual se debe contar con:

  - ✓ Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).
  - ✓ Backups de los Datos (Bases de Datos, passwords, y todo archivo necesario para la correcta ejecución de la Caja de Compensación Familiar de Arauca Comfiar).

5.3. Actividades durante el desastre

Es necesario saber primero cuales instituciones de socorro contamos en la ciudad y su ubicación.

- El Cuerpo de Bomberos de Arauca, está ubicado en Calle 23 Edificio Bomberos Oficiales teléfonos 6078850014 - 119, creado por Acuerdo del Concejo Municipal; por tal razón, es un Cuerpo de Bomberos Oficiales, existen 6 bomberos oficiales y 6 voluntarios, es de anotar que el cuerpo de Bomberos, funciona las 24 horas, siempre hay bomberos de turno por si hay alguna emergencia.

- Defensa Civil se encuentra ubicada en Carrera 21 No. 18-39 Línea emergencias 144, teléfono: 6078852292-Cel: 3118084428 La Defensa Civil Colombiana con los funcionarios, voluntarios y otras instituciones desarrolla planes de movilización nacional, programas de medio ambiente, prevención, atención de desastres y asistencia humanitaria para mitigar los daños causados por la naturaleza, recomponer el tejido social de los Colombianos, apoyar la seguridad ciudadana y trabajar por la convivencia social.

- Policía Nacional comandante Coronel **Freddy Ferney Pérez Pérez** Comandante Departamento de Policía Arauca. Ubicado en la Calle 15 Nro. 7-180 Vía Puente Internacional Línea Directa 112 - Línea Antisecuestro 165 Teléfono 6078853300 – 6078855540.

- Cruz Roja Seccional Arauca ubicada en la Cra 18 No. 30 - 25 / 23 San Luis Tel. 607857010, 6078852900 La Misión de la Sociedad Nacional de la Cruz Roja Colombiana es prevenir y aliviar, en cualquier circunstancia en la cual sea su deber intervenir, el sufrimiento y la desprotección de las personas afectadas por contingencias ocasionales.

- Hospital que se encuentra más cercano a las instalaciones es El hospital San Vicente de Arauca y se encuentra ubicado sobre la Vía Puente Internacional y ubicado en el Barrio Cristo Rey en la calle 15 Nº 16-17, la cual es una empresa social del estado del departamento de Arauca, que presta servicios de salud especializados a la población de los llanos colombo-venezolanos; con los recursos humano y tecnológico necesarios para la atención y del mejoramiento de la calidad de vida de la ciudadanía.

Una vez presentada la contingencia, falla o siniestro, se ejecutará las actividades planificadas previamente:

5.3.1. Plan de Emergencias

Se toma la acción que se encuentra establecida por el comité paritario de salud ocupacional COPASO, el cual establece los procedimientos necesarios para tomar acciones durante los desastres, el cual incluye la participación y actividades a realizar por todas y cada una de las personas que laboran en las diferentes sedes de la corporación, ya que, un en un siniestro no se sabe que personal se pueda encontrar en el área donde ocurra el desastre, lo cual se detalla:

- Vías de salida o escape
- Plan de evacuación del personal (incluye empleados, usuarios y visitantes)
- Ubicación y señalización de los elementos contra el siniestro si los hubiere (extintores, cobertores contra agua, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefe de Seguridad y de personal nombrado para operar en estos casos.

5.3.2. Entrenamiento

Se han realizado programas de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal, para minimizar costos se puede aprovechar fechas de recarga de extintores, charlas de los proveedores, etc.

Se ha hecho hincapié en que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la dirección otorga a la Seguridad Institucional de La Caja de Compensación Familiar de Arauca.

5.3.2. Actividad Después Del Desastre O Falla

Después de ocurrido la contingencia, falla, siniestro o desastre es necesario realizar las actividades que se detallan, las cuales están especificadas en el Plan de Acción:

- **Evaluación de Daños.**

Inmediatamente después que la contingencia, falla, siniestro o desastre ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Los daños pueden referirse a:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes afectados, sea por causas naturales o humanas.
- Imposibilidad de acceso a recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, sea por ejemplo, cambio de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- Divulgación de información a instancias fuera de las instalaciones de la corporación y que afecte el patrimonio ya sea mediante robo o infidencia.

- **Evaluación de Resultados.**

Una vez concluidas las labores de Recuperación del equipo que fue afectado, se debe de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados, el La Caja De Compensación Familiar de Arauca, debe realizar dos tipos de recomendaciones, una que es la retroalimentación del plan de Contingencias para las diferentes sedes y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro o la falla.

- **Retroalimentación del Plan de Acción.**

Con la evaluación de resultados, se optimiza el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

6. AMENAZAS MÁS COMUNES QUE PUEDEN AFECTAR EL FUNCIONAMIENTO

- **Daños causados por El Fuego**

El fuego es un elemento comprendido dentro de las principales amenazas contra el funcionamiento de los sistemas de información. El fuego es un problema crítico en un centro de cómputo por varias razones: primero, porque el centro está lleno de material combustible como papel, cajas, etc, el hardware y el cableado estructurado pueden ser también fuente de serios incendios.

Desgraciadamente los sistemas anti fuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en las instalaciones donde se encuentran los sistemas de información.
El fuego es considerado el principal enemigo del Hardware, ya que puede destruir fácilmente los archivos y programas.

Contingencia

- **Extinguidores Manuales**: cuando no se cuenta con sistemas automáticos anti fuego y se vea o perciba señales de fuego, entonces se debe actuar con rapidez para poder sofocar el incendio. Para ello, se debe tener en cuenta el material que está siendo consumido por el fuego. Para cada tipo de situación hay un agente anti fuego ideal, esto se observa en el plan de acción de COPASO que ha capacitado al personal para su uso, pero siempre tener presente la mejor ayuda de los expertos, se debe llamar a la línea de Bomberos.
- Si se enciende la ropa, no correr, tirarse al piso y rodar hasta apagarlas. Correr sólo hará que las llamas aumenten.
- Si la puerta está fría, escape de inmediato. Esté preparado para arrastrarse. El humo y el calor suben y el aire es más claro y frío cerca del suelo.
- No entrar a una edificación dañada por fuego a no ser que las autoridades lo permitan.
- Cuando entre a una edificación quemada, busque signos de calor o humo.
- Hacer que un electricista chequee las instalaciones antes de reconectarlas. No intentar reconectarlas por personas inexpertas. Se debe dejar esto al departamento de bomberos u otras autoridades.

- Tener cuidado con los daños estructurales. El techo y los pisos pueden estar debilitados y pueden necesitar reparación.
- Contactarse con el servicio de asistencia para desastres local, tales como la Cruz Roja, la Defensa Civil o Bomberos,

➢ **Daños Causados por el Agua**

Daños por agua pueden ocurrir como resultado de goteos del techo, goteos de tuberías de techo, inundaciones que comprometan el buen funcionamiento del equipo, así como los muebles y periféricos.

➢ **Terremotos**

Los terremotos pueden desarrollarse en cualquier momento, por lo que es de suma importancia incluir en el plan de emergencia de la Caja de Compensación Familiar de Arauca Comfiar el plan a utilizar en los sistemas de información en especial en el cuarto de servidores, dando prioridad a salvaguardar la vida de los funcionarios de la Caja de Compensación Familiar de Arauca Comfiar.

En medio de un terremoto se debe mantener la calma y quedarnos donde estamos. La mayor parte de las heridas producidas durante un terremoto se deben a objetos que caen sobre las personas mientras salen o entran a edificaciones.

Si nos encontramos dentro de una edificación, debemos cubrirnos debajo de una mesa o escritorio fuerte o contra una pared interior y sostenernos, mantenernos alejados de vidrios, ventanas, puertas o paredes exteriores y de todo lo que pueda caer, tales como lámparas de techo o muebles.

Si estamos a la intemperie, mantenernos donde estamos. Alejémonos de edificaciones, postes de electricidad y cables.
En un lugar público lleno de gente, no correr hacia una salida, otras personas tendrán esa misma idea. Cubrámonos y alejémonos de objetos que puedan caer.
En un edificio alto, meternos bajo un escritorio fuerte, lejos de ventanas y paredes exteriores. Manténgase en el mismo piso en que está dentro del edificio; puede que no sea necesaria una evacuación. tengamos en cuenta que puede cortarse el servicio de electricidad y activarse los sistemas y alarmas de incendio.

Contingencia

- Estar preparado para temblores secundarios. Estas ondas de choque secundarias son usualmente menos violentas que el terremoto principal, pero pueden ser lo suficientemente fuertes para causar daños adicionales que debiliten las estructuras.
- Chequear si hay heridas. No intentar mover a personas seriamente heridas a no ser que haya peligro de inmediato de muerte o de mayores daños. Si tiene que mover a una persona inconsciente, primero estabilice su cuello y espalda, y pida ayuda de inmediato.
- Si la víctima no respira, pero tiene un buen reflejo pupilar, posicionarla cuidadosamente para brindarle respiración artificial, liberar las vías respiratorias y comenzar la resucitación boca a boca.
- Mantener la temperatura corporal de la víctima usando cobijas. Hay que tener cuidado de no sobrecalentarla mucho.
- Nunca tratar de dar líquidos a una persona inconsciente.
- Si la electricidad falla, usar linternas de batería. No use velas ni fósforos u otros fuegos abiertos dentro de la casa debido a la posibilidad de salideros de gas.
- Usar zapatos fuertes en áreas donde haya desechos y vidrios rotos.
- Chequear los daños estructurales de la corporación. Si hay alguna duda haga que un profesional la inspeccione antes de entrar.

7. FALLAS EN INFRAESTRUCTURA: SERVICIOS

7.1. Red Eléctrica.

Para que funcionen adecuadamente, las computadoras personales necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

Por lo general las computadoras personales toman la electricidad de los circuitos eléctricos domésticos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte, siendo una corriente alterna (AC), ya que alterna el positivo con el negativo. La mayor parte de las computadoras personales incluyen un elemento denominado fuente de alimentación, la cual recibe corriente alterna

de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes de la computadora.

La fuente de alimentación es un componente vital de cualquier computadora personal, y es la que ha de soportar la mayor parte de las anomalías del suministro eléctrico. Actualmente existe el concepto de fuente de alimentación redundante, la cual entrará en operación si se detecta una falla en la fuente de alimentación principal.

Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras, monitores, las impresoras y los demás periféricos.

Un corte de la alimentación de la unidad principal puede:

- Hacer que desaparezca la información que hay en la RAM.
- Los datos recién introducidos o recién editados que no se hayan grabado, se pierden.
- Se interrumpe el proceso de escritura en el disco.
- Se puede perder información de importancia que necesita el sistema operativo, como puede ser la localización de un archivo, dando como resultado que pierdan o desorganicen archivos.
- Interrumpir impresión: cuando vuelva la tensión se han de continuar los procesos de impresión. En algunos casos se ha de volver a comenzar este proceso.
- Se interrumpen las comunicaciones: cuando vuelve la corriente, los datos que se estaban transfiriendo entre las computadoras deben de ser comprobados para tener exactitud, y los archivos que se estaban transmitiendo puede que haya que volver a transmitirlos.
- El sistema queda expuesto a picos y subidas de tensión: cuando vuelve la tensión. Normalmente se desconectan los equipos cuando se va la corriente, pero esto no siempre es posible. Cuando la empresa de distribución eléctrica restaura el servicio, a menudo viene con picos que pueden dañar los aparatos que no se hubieran desconectado.

Determinación de fallas

Las fallas de tipo eléctricos son muchas, las cuales se pueden mencionar a continuación:

- Problemas con transformador: Este problema posiblemente sea el de mayor envergadura, por lo que la falla se determina prácticamente con la

falta de suministro eléctrico, una forma de verificar el problema es que en un sitio cercano llegue el suministro de energía eléctrica y en las instalaciones de la Caja de Compensación Familiar de Arauca Comfiar no exista tal fluido, en este caso, llamar inmediatamente a la sección de Desarrollo de TIC de esta corporación.

- Problemas del tablero general: Se recomienda que el tablero este adecuadamente rotulado de acuerdo a los circuitos que protege, en el caso de la sede principal de Comfiar, el tablero de distribución general (TDG) se distingue con facilidad (es una caja color gris empotrado en la pared), que está ubicada al lado izquierdo de la entrada principal, atrás del puesto de trabajo de la recepcionista, la cual tiene como objetivo proteger de un cortocircuito a los dispositivos conectados a él. El tablero general es el que alberga los denominados térmicos los cuales de disparan para proteger al circuito de un pico de voltaje provocado por un cortocircuito. Será necesario verificar qué ocasiono el cortocircuito antes de accionar en modo normal, se recomienda acudir a un electricista al menos con categoría tres para que realice un diagnóstico preventivo. Es posible que el térmico llegue a tener un daño irreversible, por lo que se sugiere reportar a La sección de Desarrollo de TIC de la Caja de Compensación Familiar de Arauca Comfiar para realizar el cambio respectivo.

- Problema con la tierra: Si existe problemas con la tierra, es decir, hay inducción de corriente parásita, la cual se puede medir con un Ohmiómetro, por lo que la medición deberá hacerlo personal capacitado. En muchas ocasiones, una caída de un rayo cerca del sector del centro administrativo puede generar inducción de corrientes parásitas alterando la calidad de la tierra por lo que el responsable de la sección de Desarrollo de TIC deberá reportarlo para efectuar mediciones y tener la certeza que la tierra es la adecuada y está dentro del parámetro especificados por las normas que lo rigen. Por esta razón la sede administrativa adecuó un pararrayos situado en la parte más alta y conectado con el sistema de puesta a tierra (SPT).

- Problemas con el interruptor de las lámparas fluorescentes: En muchas ocasiones, el interruptor de las lámparas fluorescentes de las instalaciones de Comfiar puede fallar, una prueba sencilla es que al accionar en modo encendido y no encienden las lámparas existiendo fluido eléctrico al interior de las instalaciones de COMFIAR, entonces se puede deducir que el interruptor está fallando, favor verifique que los térmicos están en ON (encendido) y realice nuevamente la prueba. En caso que se mantiene la falla, será necesario reemplazar el interruptor, esto lo puede realizar una persona competente en el área.

- Problema con los tomas eléctricos: Si la salida en el toma es de 0 Vac, significa que no hay fluido eléctrico en el toma, esto se debe a variables tales como falta de fluido eléctrico en la zona, se dispararon los térmicos por algún pico de voltaje o existe un circuito abierto entre la caja de distribución y el toma eléctrico. Si hay fluido eléctrico en la zona se descarga la primera variable y se necesitará verificar si se han disparado los térmicos, si es así, entonces, se debe observar que ocasiono que los térmicos se activaran, antes de encender un equipo eléctrico/electrónico, realizar la inspección con personal capacitado; en el caso de que persista el problema, entonces acudir a personal capacitado para verificar si el toma eléctrico está mal instalado o existe un circuito abierto y si es posible reemplazar el toma eléctrico defectuoso.

7.1.1. Sistemas alternos de solución

Mantener en buen estado el U.P.S. (Sistema Ininterrumpible de poder): este equipo se utiliza, cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable. El UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico. Esta unidad hace transparente a las interrupciones de fracciones de segundo que inevitablemente detiene a los sistemas y le permite seguir trabajando durante varios minutos. Los pequeños sistemas UPS proveen energía de baterías por sólo unos pocos minutos. Los sistemas más sofisticados están conectados a generadores eléctricos y pueden proveer energía durante días enteros. Los sistemas UPS proveen generalmente protección contra sobrecarga y pueden proveer asimismo regulación de tensión. Es de aclarar que este sistema de poder tiene carga en las baterías para varios minutos por lo cual se debe aprovechar para terminar y guardar los procesos y apagar los equipos de cómputo hasta que se restablezca el fluido normal de energía eléctrica o se active la planta eléctrica.

Mantenimiento

Antes de instalar la unidad, se recomienda hacer una inspección visual del estado del equipo decepcionado, si no está en perfectas condiciones, deberá notificarse al proveedor respectivo (en el caso que este sea nuevo)

Escoger una localización que esté limpia y seca. No colocar el UPS en un espacio cerrado donde el flujo de aire esté restringido ni encima de otro dispositivo electrónico como la CPU. Como el flujo de aire es de interés primordial, asegurarse de que el área en que el UPS debe ser localizado no esté sujeta a la contaminación de polvo, gases corrosivos, exceso de humedad, vapor de aceite u otras sustancias combustibles.

Al limpiar el equipo, no usar líquidos o agentes de limpieza a base de aerosol. Se puede mantener el UPS limpio y fresco, aspirando periódicamente los depósitos de polvo alrededor de las rejillas de ventilación y limpiando la unidad con un paño seco.

Tablero de Control.

El tablero de control debe ser diseñado de acuerdo al voltaje y corriente que se propone soportar, y debe ser equipado con los dispositivos necesarios de protección contra fallas (térmicos) para proteger al generador de daños, cuando hay fallas o sobrecargas en el sistema. Se debe fijar parámetros los cuales fijen la carga que soporte cada braker ubicado en los tableros principales y secundarios de distribución de energía eléctrica.

Mantenimiento.

La limpieza con paño seco puede ser satisfactoria cuando los componentes son pequeños. Generalmente se recomienda soplar la suciedad con aire comprimido, especialmente en los lugares donde se ha juntado tierra y no se puede llegar con el paño.

El polvo y la tierra pueden quitarse con una escobilla de cerdas y luego aspirar. No usar escobilla de alambre. Inspeccionar que no haya conexiones sueltas o contaminadas.

7.1.2. Extensiones Eléctricas y capacidades

Las computadoras personales a veces ocupan rápidamente todas las tomas de corriente. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser autorizado, instalado y controlado por el jefe de la sección de Desarrollo de Tic. No sólo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima (especialmente con los niños). Aparte del daño físico que puede provocar engancharse repentinamente con el cable, se trata de una forma rápida y poco agradable de desconectar un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.

- Se debe utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar.se recomiendo utilizar los enchufes de pared siempre que sea posible.

- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar a limitar el daño ante fallas eléctricas.

- Adquirir toma corriente de pared y/o extensiones eléctricas mixtas, capaces de trabajar tanto con enchufes de patas planas, como cilíndricas.

- Tanto la toma corriente de pared como las extensiones eléctricas deben tener toma a tierra.

La Empresa de Energía de Arauca · ENELAR E.S.P. es la empresa de energía que suministra este servicio, se encuentra ubicada la Carrera 22 - Calle 22 - 46, Teléfono: 6072495 Horarios de Atención: lunes a viernes de 8:00 AM - 12:00 M - 2:00 PM - 6:00 PM

El suministro de energía es por las redes eléctricas comunes del municipio recibiendo corriente de 110 y 220 voltios. El área Administrativa de la caja de compensación familiar de Arauca “COMFIAR” cuenta con dos (02) postes y un (01) transformador de 75 Kva que están ubicados sobre la calle 22 y posee una una estructura eléctrica adecuada para el óptimo funcionamiento de los equipos

de la empresa que está comprendida de una central de energía donde se distribuye dicho servicio a todo el edificio y así protegiendo toda la red interna.

La red eléctrica interna está diseñada de la siguiente forma:

- Comienza por una llegada de línea de media tensión de 13.2 Kv proporcionado por la Empresa de Energía Eléctrica de Arauca ENELAR.
- Un cortacircuitos de 4 Amperios tipo HH.
- Un transformador de 75 KVA 13200/208/120V
- 4 cables 1/0 por 2 ductos de 3”
- llega al tablero general a un totalizador general de 3x3000 A
- llega a un barraje 300 AMP
- pasa por una transferencia 50 KVA de la planta eléctrica Perkins series 1000
- Se deriva a 4 Breakers de la siguiente forma; uno de 2x40 Amp, dos de 125 Amp, y otro de 3x60 Amp.
- De allí se dirigen a los tableros de distribución

Contingencia

Al momento de no haber servicio o suministro del fluido de energía eléctrica externa suministrado por la Empresa de Energía Eléctrica de Arauca ENELAR, se activa automáticamente la transferencia de la planta eléctrica Perkins series 1000 la cual enciende su motor (previa configuración), realiza transferencia de cargas y espera la normalización del fluido eléctrico de la red externa para proceder a conectarla y apaga el motor de la planta eléctrica.

7.2. Red de Datos

La red de datos es la que permite transmitir información de un computador a otro.

La estructura de red que posee La Caja de Compensación Familiar de Arauca Comfiar es cliente/servidor, por lo que los servidores son el componente más importante de la red.

Existe un sistema de seguridad de red llamada Firewall el cual restringe los accesos no permitidos o intrusos a la red, y limita el acceso no permitido de navegación.

También hay un Switch de datos, el cual permite interconectar cada punto lógico de red o estación de trabajos para que se intercambie información en toda la Red.

El cableado es estructurado y topología es estrella, también existe implementada tecnología inalámbrica, para los dispositivos móviles y portátiles

La red de datos de La Caja de Compensación Familiar de Arauca Comfiar cumple con las normas de cableado estructurado expuesta por la EIA/TIA 568, donde se establecen las pautas a seguir para la ejecución de un cableado estructurado.

La totalidad de las conexiones de nuestra red LAN (Red de Área Local) se realizan con cables de pares trenzados (para aislar y disminuir la interferencia electromagnética) sin apantallar (UTP) de categoría 6, que especifica hasta 250 MHz y está concebido para redes de hasta 1 Gbps, garantizando una mejor velocidad en la transmisión de datos, voz, vídeo, multimedia, etc, constituyendo un sistemas integrado de comunicación óptimo.

La comunicación entre los diferentes servicios (servidores) de la red y la terminales de trabajo, se hace por cableado horizontal y topología en estrella (estándar TIA/EIA-568A), donde cada toma de área de trabajo se conecta a una terminación de conexión horizontal entre diferentes vías en el Rack y cada piso tiene por lo menos un Rack para el cableado como lo sugiere el estándar TIA/EIA-569 y los ductos o canaletas no son compartidos por ningún otro servicio, cumpliendo con la distancia máxima de 90 mts, 6 mts de cable de empalme que sirve como puente y 3 mts el cable perteneciente al área de trabajo.

De acuerdo a la norma, un subsistema de cableado estructurado consiste de 6 subsistemas funcionales:

- instalación de entrada, o acometida: es el punto donde la instalación exterior y dispositivos asociados entran al edificio, es decir; la entrada del cable del proveedor del servicio de Internet al dispositivo de distribución.
- El cuarto local o sala de máquinas o equipos: es el espacio centralizado para los equipos de telecomunicaciones (PBX, servidores de datos, firewall, alarmas, etc.) que da servicio a los usuarios en las instalaciones de Comfiar.
- El eje de cableado central: proporciona interconexión entre los gabinetes de telecomunicaciones, locales de equipo, instalaciones de entrada y gabinetes dentro de la misma sede de Comfiar.
- Gabinete de telecomunicaciones: es donde terminan en sus conectores compatibles, los cables de distribución horizontal, igualmente el eje de cableado central termina en los gabinetes, conectado con puentes o cables

de punteo, a fin de proporcionar conectividad flexible para extender los diversos servicios a los usuarios en las tomas o salidas de telecomunicaciones.

- El cableado horizontal. Consiste en el medio físico usado para conectar cada toma o salida a un gabinete. Se pueden usar varios tipos de cable para la distribución horizontal. Cada tipo tiene sus propias limitaciones de desempeño, tamaño, costo, y facilidad de uso.
- El área de trabajo: sus componentes llevan las telecomunicaciones desde la unión de la toma o salida y su conector donde termina el sistema de cableado horizontal, al equipo o estación de trabajo del usuario.

- Todo lo anteriormente nombrado es gestionado por el administrador de Red, y se materializa por este medio de transmisión físico.

- La red de datos inalámbrica o Wi-Fi (Wireless-Fidelity) y cumplen los estándares 802.11b/g relacionados a redes inalámbricas de área local que opera en la frecuencia 2.4 GHz (frecuencia inalámbrica licencia libre) alcanzar ya transferencias a 108 Mbps con alta seguridad y fiabilidad utilizando filtrado por la dirección MAC (*media access control*) que es la tarjeta de red que tiene un número de identificación único de 48 bits, 6 bloques hexadecimales, permitiendo el acceso únicamente a estas direcciones relacionada. Estas direcciones hardware únicas son administradas por el Institute of Electronic and Electrical Engineers (IEEE)

Ejecución de Actividades

El primer paso que se debe seguir es ir a la estación de trabajo afectada, verificar si la falla de la conexión es física, es decir, si el cable de red se encuentra desconectado o en mal estado (con un probador de cable de red), en caso de estar conectado de forma inalámbrica, verificar igualmente si la conexión de red inalámbrica se encuentra desconectada, en caso de no ser así, verificar si el adaptador de red ya se encuentra activo, de no ser así, se procede a activarlo.

Si las conexiones de red de cualquiera de los dos medios de conexión de red se encuentran activos se procede a realizar una prueba de diagnóstico de red llamado Protocolo de Mensajes de Control de Internet o ICMP, es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta *ping* y *traceroute*, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible,

el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa. Si esta prueba arroja una respuesta con tiempo de espera agotado para esa solicitud, se debe verificar la conexión física en el Pacth Panel que es el elemento encargado de recibir todos los cables del cableado estructurado, si este se encuentra bien conectado, se procede a verificar la conexión y buen estado del Patch Cord (se usa en una red para conectar un dispositivo electrónico con otro) que conecta el Patch Panel con el Switch de la red, que es un elementos activo de comunicaciones, que permite trasladar a cada nodo (host) los paquetes de datos para que se intercambien información en toda la red.

Si todo esto resulta bien, se debe verificar el estado del PC, se procede a realizar un mantenimiento correctivo ya sea que el driver no esté instalado, problemas con la board etc.

7.3. Servicio De Internet

La red Local (LAN), limita su cobertura de servicios estrictamente en la infraestructura de esta entidad, sin embargo, a través de un proveedor de servicios de Internet ISP (actualmente actualmente Movistar y Servicios Profesionales WiCom S.A.S), se puede tener acceso a la Red Internacional (Internet) para utilizar este recurso como herramienta de conexión a correo institucional, y páginas autorizadas por la directora administrativa y administradas por la sección de Desarrollo de TIC de Comfiar.

El servicio de Internet permite tener acceso a los recursos de Internet tales como correos electrónicos, páginas web, bases de datos, información en línea, etc.

El componente del servicio a Internet es el Router y conectividad dado por el ISP.

El Router es un elemento activo que permite comunicar la red a los servidores de comunicaciones del proveedor de Internet y con ello tener acceso a cualquier servidor que publique información en la Red Internacional.

Detección de fallas.

- La conectividad por parte del ISP puede generar problemas, desde su planta externa hasta el Router y este a su vez puede tener problemas de Hardware o de Firmware.

- Se procede llamar a la línea de atención al cliente de la empresa proveedora de servicio de Internet, para solicitar soporte, haciendo pruebas remotas, y si es necesario trasladar a personal técnico a las instalaciones de la corporación para realizar cambio de este dispositivo si es necesario.

- Se cuenta con dos proveedores diferentes que sirven como fail over (que levanta un servicio cuando detecta que el otro está ausente) como contingencia.

Problemas con el Servidor de Datos.

Quizá unos de los equipos de cómputo más importantes en la Caja de Compensación Familiar de Arauca Comfiar es el servidor de datos, donde se encuentra instalado el software del aplicativo de nuestra corporación, por ende se encuentran situadas las fuentes y base de datos que permite el perfecto funcionamiento de los diferentes módulos del aplicativo SYS

Detección de fallas

Los problemas en el servidor de datos pueden ser el no encendido de este, además, de agregar problemas de Hardware, tales como, problemas con los discos duros, tarjetas de Red, Motherboard, etc.

El objetivo, es poder detectar que tipo de problema posee el servidor y con ello, determinar qué acción tomar, en ese sentido, es necesario retomar algunas fallas generales que pueden darse en el Server.

Por problemas de Hardware:

- Fuente de Poder.
- Motherboard.
- Sistemas de almacenamiento.
- Tarjetas de Red
- Periféricos del Server

Por problemas de Software:

- Sistema Operativo incluyendo servicios.
    - Queryx.

Alternativas de Solución

- Fuente de poder: Si el servidor de datos no enciende y hay energía eléctrica en la toma en que está conectado el Server, es muy probable que el problema sea la fuente de poder, corroborar además si existe energía eléctrica a la salida del UPS del Server.

- Por problemas en la Motherboard: Si se ha detectado que enciende el Server (específicamente los ventiladores de la fuente de poder), entonces es muy posible que el arreglo de disco este dando problemas o en su caso la tarjeta madre (Motherboard). Si el problema es con el arreglo de disco, es muy probable que el BIOS entregue un código de error (1794), el cual, le indicara al usuario que definitivamente es problema en el arreglo de disco.

- Por problemas en el sistema de almacenamiento: Si algún Disco Duro del Server está fallando, normalmente este presenta un Led en color rojo en la parte frontal del Disco Duro, acá el controlador está detectando que existe una inminente falla en el Disco duro, por lo que será necesario reemplazarlo y se acude al backup echo anteriormente y montarlos en el servidor de contingencia y adecuarlo y ponerlo en funcionamiento en el tiempo más corto para no entorpecer los procesos diarios de la corporación.

- Por problemas de NIC: Normalmente, el Server posee dos tarjetas de Red, uno para la red de datos interna y el otro para el acceso a Internet. Una forma rápida de verificar su funcionamiento es identificar si el Led de la tarjeta de Red está funcionando, en caso contrario es posible que la NIC no esté operando adecuadamente. Otro caso probable es que este desactivado desde el sistema operativo, lo cual se procede a levantar la interface de Red.

- Por problemas de periférico: Normalmente los periféricos del Server pueden fallar, tales como el monitor, el teclado o el ratón (Mouse). Para detectar las fallas en el teclado y en el Mouse, estos pueden ser detectados desde el SO o el BIOS, y en el caso del Monitor, la falla puede ser la tarjeta de video, el cable de video o específicamente en el Hardware del Monitor.
- Problemas con el SO y sus servicios: En muchas ocasiones, los problemas no son de Hardware, sino también de Software, por lo que será necesario hacer énfasis en su diagnóstico, es por ello, que se hacen entrega al detalle de la configuración de los servicios.

- En el caso que el servidor esté en mal estado y no pueda recuperarse, se procede a tomar la última copia de seguridad (procedimiento visto en copias de seguridad Backups), compilamos las fuentes y la base de datos, este proceso se tarda en un tiempo promedio de una hora y media (90 minutos). Todo el proceso de adecuación del servidor de contingencia tardaría aproximadamente 3 horas y media (210 minutos) en caso de no tener uno como mirror.

7.4 EQUIPOS ACTIVOS DE COMUNICACIÓN

Switch: este elemento activo de comunicaciones es de suma importancia, y no debe estar apagado, ni desconectado ya que en ese momento se tendría una caída en la Red de datos. Usualmente estos elementos activos de comunicación son de 24 puertos, los cuales poseen unos Led (Diodo Emisor de Luz - indicadores visuales) que señalan el estado de funcionamiento de cada puerto, en el momento en que está activo el puerto, el Led del mismo debe estar encendido. Cada puerto conecta a un nodo o computadora por lo que una de las formas de detectar que hay falla de comunicación es observar el puerto, obviamente, cada puerto debe estar etiquetado con el punto de Red respectivo.

Detección de fallas

- Por problemas eléctricos: Si hay problemas de suministro de fluido eléctrico, posiblemente se apague el elemento activo de comunicaciones, por lo tanto, el resultado será una caída en la red de datos.

- Por problemas de puerto: es posible que por alguna variación de voltaje, se queme una cantidad limitada de puertos, se recomienda verificar los Led (Diodo Emisor de Luz) que indican conectividad.

Alternativas de solución.

- En el caso de falla en el suministro de energía eléctrica, su respaldo es la UPS dedicado para el elemento activo, se recomienda que el UPS tenga un regulador de voltaje integrado para evitar picos de voltaje.

- Por problemas de puerto: una forma sencilla de verificar que el puerto está fallando, es verificar que el Led de la tarjeta con que está conectado el puerto esta encendido, si al realizar un ping al Server, este no contesta, entonces, es posible que el puerto está fallando, otra verificación es cambiar la conexión de la tarjeta a otro punto de red, el cual conectara a otro puerto, si al realizar un ping al Server y este contesta, entonces, se puede concluir que el puerto es el que está fallando, lo mismo se puede realizar si hay problemas con los puntos de red.

Si ninguna de las pruebas anteriores es exitosa, se procede entonces a cambiar por otro de contingencia que se debe tener para estos casos.

VERSIÓN	FECHA APROBACIÓN	PAGINA(S)	NUMERAL(ES)	CAMBIO
Versión 02	07 diciembre de 2017	5	2.1.1.1	**Hardware:** HP Proliant ML350 G6 Si**stema Operativo**: Centos releáse 5.8 **Procesos**: Servidor Aplicaciones de módulos SYS; módulos de Asamblea, Contabilidad, Tesorería, Activos, Presupuesto, Servicios, Conciliación, Créditos, Fosfec, Generales, Promoción, Mercurio, Suministros, Colegio, Auditoria, Estadística, Fovis, Xml1, Xml2, Xml3 y Xml4
		5	2.1.1.4	**Hardware:** HP ProLiant DL160 G5 **Sistema Operativo:** Servidor con sistema operativo Linux Versión Ubuntu 10.04 **Procesos:** Servidor de aplicación de mesa de ayuda GLPI
		6	2.1.1.7	**Hardware:** HP ProLiant DL180 G6 **Sistema Operativo:** Centos releáse 6.5 **Procesos:** Sistema de Gestión documental (Orfeo), permite incorporar la gestión de los documentos a los

				procesos organizacionales, con procedimientos y políticas definidas de acuerdo al AGN, reduciendo costos, tiempo y recursos y control del documento-Intranet el cual contiene toda la información pública interna de Comfiar
		8	2.2	VMware vSphere Client Para la virtualización de diferentes sistemas operativos
		8	2.3	Kaspersky Endpoint Security Antivirus (última versión)
		46	7	La red Local (LAN), limita su cobertura de servicios estrictamente en la infraestructura de esta entidad, sin embargo, a través de un proveedor de servicios de Internet ISP (actualmente es Tv Satélite Arauca) como canal principal, y Movistar como canal de contingencia, se puede tener acceso a la Red Internacional (Internet) para utilizar este recurso como herramienta de conexión a correo institucional, y páginas autorizadas por la directora administrativa y administradas por la sección de sistemas de Comfiar
Versión 03	5 de agosto de 2022	Todo el Documento	Todo el Documento	Adición tabla de contenido
		Todo el Documento	Todo el Documento	Actualización Orden nomenclatura
		5	1.1	Actualización Conceptos Generales
		7	2.2.1	Adición módulos en servidores (Servidor aplicativos internos SISU)

		10	2.2.2	Actualización dispositivos de interconexión de redes
		19	5.3	Actualización Actividades durante el desastre.
Versión 4	2 de enero de 2025	Todo el documento	Todo el documento	Se cambia el código documental de acuerdo a la creación de un nuevo proceso, de ML-GA-03 a ML-TI-02.
		Todo el documento	Todo el documento	Se modifican los cargos y la denominación de las secciones, de acuerdo a cambios en la estructura organizacional del organigrama, mapa de procesos y planta de personal.
		Todo el documento	Todo el documento	Se modifican los códigos documentales de los procedimientos y formatos referenciados de acuerdo al nuevo sufijo TI.