Plan de Contingencia de Tecnologías de Información

Seguridad de Información

El presente documento cubre los procedimientos de recuperación de los servicios críticos de TI de la CAJA MUTUAL DE LOS EMPLEADOS DEL MINED en caso se den las situaciones de contingencia como las siguientes: Incendios, fallas eléctricas, terremotos, inundaciones y amenazas humanas (Ataques a infraestructura tecnológica, Bloqueo de instalaciones físicas) que provoquen una falla total del Centro de Datos de La Caja.

Unidad de Tecnologías de Información

29/11/2021

APROBADO
Acuerdo de Consejo Directivo, según punto 5.b.6 del Acta n.°108
de sesión celebrada el 28 de enero de 2022.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN

Seguridad de Información

Objetivo General:

Establecer un plan de acción y contingencia que respalde y coadyuve a iniciar las operaciones más importantes de La Caja Mutual de los Empleados del Ministerio de Educación, cuando se dé un siniestro total del centro de datos, logrando con esto la recuperación exitosa de los servicios que proporciona de Tecnologías de Información (TI), a través de procesos de respaldo y sistemas integrados paralelos.

Alcance:

En el presente documento se describen los procedimientos a realizar para la recuperación de los servicios críticos de TI, en caso de situaciones extremas por pérdida en la infraestructura y/o datos por siniestros o eventos naturales, además las siguientes condiciones:

- Cuando los sistemas de información no estén funcionando en el centro de datos y que estos no pueden ser recuperados en un periodo de 48 horas.
- Que se posean los recursos económicos, tecnológicos, para iniciar en la ejecución de este plan en caso de ser necesario.
- Poseer las copias de seguridad de los datos y software se encuentren intactos y disponibles.
- Si se posee contrato con un proveedor externo, verificar que estos se encuentren vigentes para que se puedan recuperar todos los servicios de TI.

Las amenazas comunes para las tecnologías de Información se pueden catalogar de la manera siguiente:

- Amenazas Naturales: Inundaciones, terremotos, deslaves, tormentas eléctricas, y otros eventos similares de gran magnitud que afecten la Infraestructura de TI.
- Amenazas Humanas: Eventos que son causados por personas incluyendo acciones no intencionales (errores o accidentes) y acciones deliberadamente mal intencionadas (ataques lógicos y físicos a la

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.

infraestructura, distribución de software malicioso, acceso no autorizado a la información institucional)

- Amenazas ambientales: Fallas en suministro de energía, contaminación externa, filtraciones de líquidos, químicos en el ambiente.

Justificación:

A medida que las actividades de la Caja Mutual de los Empleados del Ministerio de Educación dependen cada vez más de las computadoras y las redes para manejar dichas actividades y procesamiento de datos, la disponibilidad de los recursos tecnológicos y sistemas informáticos se ha vuelto crucial. Actualmente, se necesita un alto nivel de disponibilidad de información e incluso garantizar el mantener disponible los recursos tecnológicos.

Los procesos ejecutados en forma manual, sólo serían prácticos por un corto período durante un evento adverso ya que, La interrupción prolongada de los servicios informáticos puede significar pérdidas financieras para La Caja, afectando inclusive, la credibilidad de la institución por parte de los asegurados, teniendo consecuencias negativas.

Toda Unidad de Tecnologías de información debe cumplir con las normas plasmadas por la Corte de Cuentas, las cuales están descritas en el Reglamento para el uso y control de las Tecnologías de información y comunicaciones del Sector Público y para el Plan de Contingencia el Art. 39.- "La Unidad de Tecnologías de Información y Comunicaciones, deberá contar con un plan de contingencia autorizado por la máxima autoridad de la entidad, este plan debe ser viable, que detalle las acciones, procedimientos y recursos financieros, humanos y tecnológicos, considerando los riesgos y amenazas de Tecnologías de Información y Comunicaciones que afecten de forma parcial o total la operatividad normal de los servicios de la Entidad, categorizando el tipo de acción a realizar en cuanto a la medición en tiempo para el restablecimiento de las operaciones tecnológicas, este plan debe probarse y actualizarse atendiendo la realidad tecnológica de la entidad al menos una vez al año. Deberá ser comunicado a los niveles pertinentes".

El Art. 11 del Reglamento mencionado anteriormente, indica que "La Unidad de TIC, deberá adoptar una metodología de gestión de riesgos, debiendo documentar el proceso de identificación, análisis, administración y evaluación de riesgos de TIC", por lo que es indispensable contar con un plan que indique los procedimientos a seguir, ante amenazas que afecten la operación de la institución relacionadas con las tecnologías de información y comunicación.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.

Definiciones:

Contingencia: Interrupción, no planificada, de la disponibilidad de recursos informáticos.

Plan de Contingencia: Conjunto de medidas (de detección y de reacción) a poner en marcha ante la presentación de una contingencia.

Recursos: Lugar alternativo de trabajo, computadora con "hardware" y "software" apropiados, impresoras, copias de seguridad actualizadas.

Pruebas: Validez de las copias de seguridad, simulacros de emergencia (una vez por año como mínimo), formación y reciclaje del personal.

Riesgos Identificados

Entre los principales riesgos encontrados tenemos:

- Equivocaciones, que dañen los archivos.
- Acción de virus, que dañen los equipos y archivos.
- Fallas (hardware o software) en los equipos, que dañen los archivos.
- Variaciones de fluido eléctrico.
- Accesos no autorizados, filtrándose datos no autorizados.
- Robo de datos, difundiéndose los datos sin cobrarlos.
- Vandalismo, que dañen los equipos y archivos.
- Robo común, llevándose los equipos y archivos.
- Fuego, que puede destruir los equipos y archivos.
- Terremotos, que destruyen el equipo y los archivos.

Factores de Riesgo.

A cada uno de los tipos de riesgos, mencionados en el punto anterior, se le ha asignado un factor de simple entendimiento. De acuerdo a la experiencia rescatada de los usuarios de la institución y el equipo de la Unidad de Tecnologías de Información Institucional se ha llegado al siguiente cuadro:

TIPO DE RIESGO	FACTOR DE RIESGO	Tiempo estimado de recuperación por tipo de riesgo.
Virus	Bajo	3 – 5 días
Accesos	Bajo	3 – 5 días
Robo de datos	Bajo	3 – 5 días
Vandalismo	Bajo	3 – 5 días

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.

Robo común	Bajo	3 – 5 días
Equivocaciones	Medio	6-10 días
Fallas en equipos	Medio	6-10 días
Terremotos	Medio-Alto	10 - 12 días
Inundaciones	Medio-Alto	10 - 12 días
Al fuego	Medio-Bajo	10 - 12 días
Variaciones de fluido eléctrico	Alto	13 - 15 días

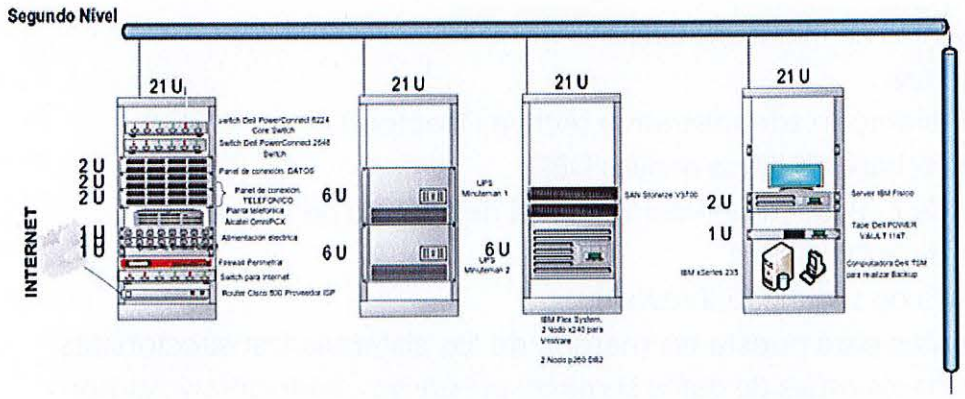
Descripción de los factores de riesgo:

- Bajo: Factor de riesgo de menor nivel de incidencia, posible a producirse.
- Medio: Factor de riesgo producido no muy a menudo, pero de presencia constante.
- Alto: Factor de riesgo de mayor probabilidad o incidencia.

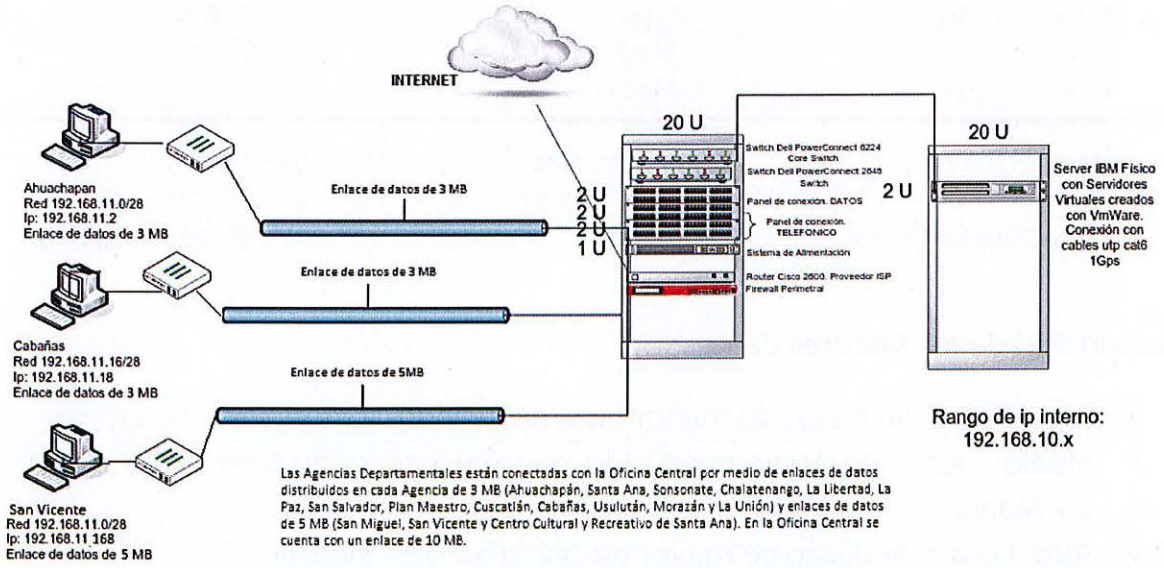
Descripción de arquitectura general de servicios de TI.

Los sistemas informáticos, servicios de conectividad, internet y correo electrónico, utilizan la infraestructura tecnológica que se describen a continuación:

Estructura de Servidores:



Estructura de Conexión de Agencias departamentales:



Principales recursos y servicios necesarios para ser restablecidos y/o recuperados en un lugar alternativo de trabajo:

Hardware y software

- Computadora con sistema operativo (Windows)
- Servicio de internet
- Correo electrónico
- Antivirus
- Herramientas de Microsoft Office

Infraestructura

- Servidor directorio administrativo (Active Directory)
- Servidor de base de datos activas DB2
- Servidor de FTP (documentación digital de sistema de préstamos)
- Servidor de aplicaciones
- Dispositivo de seguridad (firewall)

Componentes para puesta en marcha de los sistemas transaccionales

- Replicas de las bases de datos seguros, préstamos, financiera y Admon
- Ejecutables de las aplicaciones

Base de datos:

La base datos actual es DB2 11.1 para AIX, dentro de las cuales contiene las siguientes Bases de datos:

- Base de datos de Asegurados
- Base de datos de Unidad Financiera.
- Base de datos de Préstamos

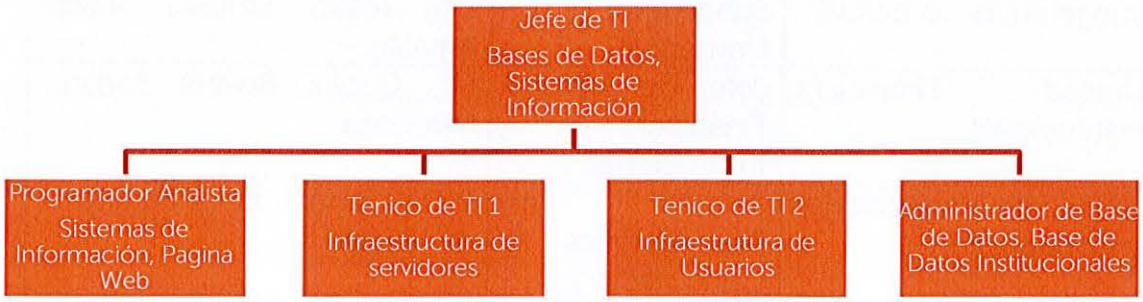
- Base de datos Admon

Sistemas de información que se utilizan actualmente:

- Sistema Integrado con sus componentes – Magic XPA 3.2 C
  - Suscripción
  - Prestamos
  - Inversiones
  - Desarrollo Humano (Pago de Planillas)
  - Mesa de Servicio
  - Logística:
    - Activo Fijo
    - Inventario y consumible
    - Carnet de parqueo
- Sistema Móvil de Asegurados – Magic XPA 2.5.
- Sistema de Pagos de Planillas – Magic Software 9.3
- Sistema de Cheques – Foxpro 2.5

Organización y Responsables.

Se designará el Jefe de Tecnologías de Información como encargado de la coordinación de este Plan de contingencia, quien será el encargado de velar por la seguridad de los sistemas de información y la ejecución de los procedimientos documentados, para el caso de una contingencia se define la siguiente estructura y equipos de trabajo para responder ante la emergencia de acuerdo con los procedimientos institucionales.



Criterio de activación del Plan de Contingencia.

El Plan de Contingencia se ejecutará cuando se cumpla al menos una de las siguientes condiciones:

- Una interrupción total de servicios de TI por más de 48 horas
- Se produzca una amenaza (Natural, humana, etc.) que impacte las oficinas administrativas de La Caja Mutual de los Empleados del Ministerio de Educación.
- Se declarase emergencia nacional en la que haya afectación a la infraestructura y servicios la oficina central de La Caja.

Procedimiento para la activación del plan de Contingencia.

De existir la necesidad de ejecutar el Plan de Contingencia, TI realizará el siguiente procedimiento:

1. Verificar la situación y catalogar el tipo de contingencia
2. Convocar al comité de contingencia el cual estará conformado por las jefaturas siguientes:

Unidad	Puesto	Nombre
Unidad de Tecnologías de Información	Jefe de Tecnologías de Información	Ing. Carlos Rafael Henríquez Romero – Coordinador de comité de contingencia de Tecnologías de Información
Planificación y Desarrollo Institucional	Jefe de Planificación y Desarrollo Institucional	Lic. Jorge Alberto Canales Blanco.
Subgerencia Operativa	Subgerente Operativa	Lcda. Dina Lariza Rivera Menjivar
Subgerencia Comercial	Subgerente Comercial	Ing. Mario Ernesto Navas Aguilar
Unidad Financiera Institucional	Jefe de Unidad Financiera Institucional	Lic. Cecilia Beatriz Soriano Mendoza
Unidad de Adquisiciones y Contrataciones	Jefe de Adquisiciones y Contrataciones	Licda. Sandra Janet Barahona de Huezo

Se consideran que son las personas idóneas porque son las unidades involucradas en los procesos y toma de decisiones.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN GERENCIA SAN SALVADOR, C.A.

3. Convocar a los equipos por vía telefónica, correo electrónico (si están activos) u otro medio de acuerdo a la circunstancia.
4. Verificar el repositorio de datos y procedimientos de contingencia específicos.

Evaluación del daño.

Se verificará el daño recibido a la infraestructura tecnológica debido al tipo de amenaza detectado:

Se evaluarán los siguientes puntos, juntamente con los equipos de trabajo:

- Estructura principal incluyendo soportes, paredes y techo.
- Problemas de seguridad y acceso (puertas, ventanas, etc.)
- Problemas en sistema de aire acondicionado, poder, iluminación.
- Daños en elementos específicos de infraestructura tecnológica
- Daños en mobiliario y equipo en centro de datos y estaciones de trabajo que se utilizan para su administración.

El equipo de Evaluación preparará un estimado del costo de reparación, sustitución y puesta en marcha en caso que hubiera daños considerables en el centro de datos de La Caja Mutual de los empleados del Ministerio de Educación, así como también, notificar al Coordinador de Contingencia y las autoridades correspondientes.

De la evaluación inicial dependerán las siguientes etapas de este Plan de Contingencia pudiendo recomendar que se detenga el proceso.

Requisitos mínimos para el sitio de contingencia recomendado:

1. Sistemas eléctricos de las instalaciones: entradas del servicio de energía debe de ser entre voltaje y frecuencia 120 / 208 VAC, 60Hz
2. Generación eléctrica de energía independiente
3. Sistema de redundancia en los sistemas de distribución y redundancia eléctrica.
4. Sistemas de aire acondicionado redundantes.
5. Detección de humo y supresión de incendio.
6. Altura del techo tiene que tener como mínimo 2.6 metros
7. Poseer piso elevado con el objetivo de exista un flujo de ventilación en los equipos instalados.
8. No debe existir ninguna exposición al agua.
9. Seguridad Física perimetral de las instalaciones donde están ubicadas los servidores.
10. Cumplir con los estándares internacionales en el diseño, electricidad, aire acondicionado, seguridad, etc. de los DataCenter

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.

Pruebas de funcionamiento.

Se deberán realizar pruebas de funcionamiento del plan de contingencia, por lo menos una vez al año, para verificar la efectividad de dicho plan.

Tiempo de desfase de los datos, respecto a la data original

El tiempo de desfase de los datos que se tendrán en el local de contingencia será de 48 Horas antes de acontecido el evento de desastre.

Procedimientos de recuperación

Prioridad de recuperación de servicios.

1. Base de datos de seguros y préstamos.
2. Sistemas Informáticos Institucionales
3. Servidor de dominio

Los procedimientos de recuperación se detallan en tres áreas: infraestructura tecnológica, Sistemas Informáticos y equipo cliente.

Principales servicios que deberán ser restablecidos

- Software Base
    - Bases de DB2
    - Ejecutables de las aplicaciones.
- Respaldo de la Información
    - Copia de la Base de Datos DB2
    - Copia de la Plataforma de Aplicaciones (Sistema)
    - Copia del Servidor controlador de Dominio.

Sistemas Informáticos

Como precondición al proceso de recuperación de los sistemas, se asume que existe una infraestructura disponible y ha sido puesta en operación quedando en este apartado la recuperación de:

- Base de datos Institucional
- Sistemas Informáticos Institucionales.

CAJA NACIONAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
SAN SALVADOR, C.A.

- Servidor de dominio

Restauración de Base de Datos

El proceso de restauración de la base de datos se dará de acuerdo a los procesos definidos por el fabricante de dicho software, contratado La Caja Mutual de los Empleados del Ministerio de Educación, detallándola:

- DB2 11.1 para AIX.

Restauración de sistemas

Existen dos tipos de arquitectura y por lo tanto dos tipos de restauración de los servicios:

- Arquitectura Web
- Arquitectura Cliente Servidor

Para el caso de La Caja es:

Cliente Servidor

La restauración de los sistemas informáticos de este tipo de arquitectura asume únicamente la necesidad de un servidor de base de datos que contenga la información manejada por los mismos.

Debido a lo anterior, la restauración de estos sistemas únicamente requiere que se restaure la base de datos correspondiente al sistema y se instale el sistema en el equipo cliente disponible para dicho propósito. La instalación podrá realizarse con los instaladores de los sistemas correspondientes según los pasos determinados por el manual de usuario o de instalación de cada sistema.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.

Procedimiento de Recuperación para Equipos Clientes.

El personal de soporte técnico apoyará en los casos de desastres, realizando el siguiente procedimiento:

Paso	Actividad	Responsable
1	Recibe comunicación de la activación del plan de contingencia de parte del comité de contingencia, por desastres naturales u otros.	Unidad de Tecnologías de información.
2	Coordinan las acciones a seguir e identifican las zonas afectadas	Unidad de Tecnologías de información.
3	Realizan visitas a las unidades afectadas del Caja Mutual de los Empleados MINED y procuran dejar funcionando el número de equipos posible. Solicitan al encargado de cada unidad que envíen el Inventario de los equipos funcionando y los que no se pueden utilizar	Unidad de Tecnología de información
4	Envían Inventario del equipo funcionando y sin utilizar al Encargado de Soporte Técnico	Unidad de Tecnología de información
5	Toma decisiones basado en los datos recibidos y verifica opciones de áreas donde se pueda seguir operando con los equipos cliente que estén funcionando.	Unidad de Tecnologías de información.

Una vez ejecutado el o los procedimientos de contingencia específicos se verificará la funcionalidad de los servicios restaurados y se operará en modo de contingencia.

Determinación del RPO

El punto objetivo de recuperación (RPO) es la cantidad de pérdida de los datos que el negocio puede tolerar, esto depende de las copias de seguridad si son diarias, semanales o mensuales.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.

Servicios	RPO
Sistema de Seguros	1 día
Sistema de préstamos	1 día
Sistema de Inversiones	1 día
Correo	1 día
Sistema de respaldos	1día

Desactivación del Plan.

El plan de Contingencia se desactivará una vez se estabilicen los sistemas informáticos necesarios para las operaciones de La Caja Mutual de los Empleados del Ministerio de Educación y que se reanuden operaciones de manera normal en el Centro de Datos original o nuevo. La transición a operaciones normales dependerá del impacto de la situación de Contingencia y puede que no se alcance a tener el 100% de disponibilidad de los servicios de TI restaurados.

Recoger información y equipo luego de operaciones.

Al desactivar el plan debe recogerse y resguardarse toda la documentación, equipo, materiales, medias de software y cualquier otro elemento que haya sido utilizado en el proceso de recuperación de los servicios de TI. Debe de enviarse a la ubicación apropiada definida por el comité de contingencia.

CAJA MUTUAL DE LOS EMPLEADOS DEL MINISTERIO DE EDUCACIÓN
GERENCIA
EL SALVADOR, C.A.