COMISIÓN NACIONAL DE LA MICRO
Y PEQUEÑA EMPRESA

PLAN DE CONTINGENCIA INFORMÁTICO

2021

Contenido

Introducción 3
Definiciones 4
Objetivos 4
Alcance 4
Análisis y Evaluación de Riesgos 4
Escenarios contemplados para el plan de contingencia 5
Planificación 6
Estrategias para garantizar continuidad de procesos y servicios de IT 6
Escenario 1: Falla de Servidor 7
Escenario 2: Interrupción de servicio de corriente eléctrica. 11
Escenario 3: Perdida de servicio de internet o enlaces de datos 12
Escenario 4: Incendio. 13
Escenario 5: Indisponibilidad del centro de datos. 13
Escenario 6: Problemas con sistema operativo o versión de servidor virtual 15
Escenario 7: Ausencia parcial o permanente de personal de IT. 17

Introducción

Ante el incremento de la cultura informática en todos los ámbitos derivada del creciente empleo de la Tecnología de la Información, surge la necesidad y responsabilidad de la protección de la misma, de sus medios de almacenamiento y de su ambiente de operación. La información que se maneja en CONAMYPE, por considerarse como materia prima para la propia gestión y toma de decisiones, es considerada como un activo importante y como tal, debe ser sujeta de custodia y protección para asegurar su integridad, confidencialidad y disponibilidad.

Para la CONAMYPE es indispensable recurrir a los recursos de Tecnologías de la Información y Comunicaciones (TICS) como un medio para proporcionar los servicios que la institución ofrece a la ciudadanía y es de vital importancia que dicha información sea lo más exacta y expedita posible.

Es importante resaltar que para que la CONAMYPE logre sus objetivos necesita garantizar tiempos de indisponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones; de este modo podrá mantener una productividad eficiente en todas las áreas operativas.

Es necesario, por tanto, prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo menor posible.

Definiciones

A. CONTINGENCIA:

Interrupción no planificada de la disponibilidad de recursos informáticos.

B. PLAN DE CONTINGENCIA:

Conjunto de tareas (de DETECCION y de REACCION) a poner en marcha ante la presentación de una contingencia.

Objetivos

- Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra factores exógenos y endógenos.
- Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.
- Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

Alcance

El presente plan de contingencia informático se limitará a establecer las medidas de detección y reacción a poner en marcha dentro de los activos informáticos resguardados en el centro de datos institucional central.

Análisis y Evaluación de Riesgos

Los desastres causados por un evento natural o humano, son en general poco predecibles, y para cada tipo de desastre, se generan tipos de riesgo asociados con ellos, como, por ejemplo:

• Riesgos Naturales: mal tiempo, terremotos, inundaciones, etc.

• Riesgos Tecnológicos: incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.

• Riesgos Sociales: actos terroristas y desordenes.

Todos los riesgos de factores exógenos y endógenos están estipulados en el documento de gestión de riesgos de la Gerencia de Tecnologías de la Información.

Al evaluar los riesgos antes mencionados y sus posibles consecuencias sobre los servicios prestados y la información contenida en los servidores de la Institución, se determinan los siguientes como los causales más probables y el escenario de contingencia a desarrollar para el causal:

Causal	Escenario
• **Corte de cable UTP** • **Falla de Tarjeta de Red o Punto de Acceso inalámbrico** • **Error en direccionamiento IP** • **Falla en punto de red, puerto de switch o patch panel.**	Falla de Comunicación entre equipo cliente y Servidor
• **Falla de componentes de hardware del servidor.** • **Corrupción de sistema operativo.** • **Utilización de más del 100% de espacio disponible en disco.** • **Utilización de un equipo no apropiado como servidor.** • **Efecto de virus.**	Falla de servidor
• **Corte general de servicio de corriente eléctrica.**	Interrupción de servicio de corriente eléctrica
• **Falla de equipos de comunicación del proveedor de datos.** • **Falla de equipos de comunicación internos.** • **Corte de medios externos de comunicación.**	Perdida de servicio de internet o enlaces de datos
• **Terremoto.** • **Incendio.** • **Inundación.** • **Corto circuito.**	Indisponibilidad del centro de datos (destrucción del centro)
• **Accidente.** • **Renuncia inmediata.**	Ausencia parcial o permanente de personal de IT

Escenarios contemplados para el plan de contingencia

1. Falla de Servidor.
2. Interrupción de servicio de corriente eléctrica.
3. Perdida de servicio de internet o enlaces de datos.
4. Indisponibilidad del centro de datos
5. Ausencia parcial o permanente de personal de IT.
6. Desastres naturales (Inundaciones y/o terremotos).
7. Incendios y/o conatos de incendio
8. Ataques Informáticos

Planificación

Para la creación de planes de manejo de incidentes, se manejarán como indicadores importantes los siguientes:

- Tiempo máximo de la contingencia
- Recurso humano necesario
- Soporte técnico especializado por proveedores (Garantías)

Estrategias para garantizar continuidad de procesos y servicios de IT

Como parte general de este plan de contingencia, se consideran como requisitos base la implementación de las siguientes estrategias:

- **Estrategia de Respaldo y Recuperación**
  - Respaldo continuo de los servidores virtuales de acuerdo a su criticidad, primero en un servidor físico local, además de la replicación a un sitio alterno.
  - Uso de los respaldos locales para intentar una recuperación a un punto previo.
  - En caso de que la situación no pueda ser resuelto en un tiempo determinado como aceptable de acuerdo a este plan, se procederá a la activación de la maquina virtual desde el centro de datos de contingencia.
  - Al devolver la maquina virtual a un estado valido en el centro de datos principal, se hará un proceso de sincronización de datos de ser necesario previo a redirigir tráfico nuevamente hacia ella.
- **Almacenamiento y Respaldo de la Información (BACKUPS)**
  - Procedimiento de Backup - definen la frecuencia de los backup (diario, periódico, incremental o total) considerando la criticidad de los datos y la frecuencia con que se introduce nueva información.
  - Los datos se respaldarán en medios magnéticos u ópticos.
  - Es una buena práctica contar con lugar alternativo externo para el almacenamiento de la información más importante.
- **Sitios Alternos para el Centro de Datos**

- El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; en el cual estarán alojadas las máquinas virtuales de servidores más importantes

Escenario 1: Falla de Servidor

Impacto:

Impacto	Área Afectada
Paralización de sistemas o aplicaciones contenidas en el servidor, o que dependan de la información contenida en este	Todas las áreas.
Posible pérdida de hardware o software	Gerencia de Tecnologías de la Información.
Perdida del proceso automático de respaldo y recuperación	Gerencia de Tecnologías de la Información.
Interrupción de operaciones	Todas las áreas

Descripción:

Este escenario contempla la posibilidad de que un equipo servidor, se dañe de manera que interrumpa los servicios provistos por este.

En el caso de la CONAMYPE, este es un caso de alto riesgo, pues para minimizar el uso de recursos económicos y de espacio, se utilizan máquinas virtuales, que permiten la instanciación de múltiples servidores "virtuales" en un solo equipo. En caso de un fallo de hardware en dicho equipo físico (como disco duro, fuentes de poder, RAM) esto inutilizaría todas las máquinas virtuales alojadas en el mismo.

Para minimizar el riesgo ante un fallo de esta índole se debe de contar con servidores en arreglo lo cual permita que ante un fallo de uno de los servidores en los cuales se alojan servicios críticos como base de datos, correo electrónico sitio web, etc. De manera que tal que si un servidor falla el otro tenga la misma capacidad para poder migrar las máquinas virtuales de forma automática.

En cuanto al servidor de base de datos de las aplicaciones de producción se deberá realizar un respaldo diario.

Respecto a las máquinas virtuales en sí, se deberá llevar un respaldo al menos 2 veces a la semana de las que se consideren críticas, usando criterios de importancia de datos o procesamiento para su elección. En el caso de los aplicativos en producción, se deberá mantener actualizado el repositorio de código de manera que se pueda servir como recuperación de código en caso de ser necesario.

El tiempo de vida de los respaldos será semanal, es decir en una semana se guardar todos los archivos diarios y en un mes todos los archivos semanales y un año todos los archivos mensuales.

Previendo la posible falla de equipos físicos, se debe contar con ciertos componentes en inventario[1], para minimizar los tiempos fuera, o saltos innecesarios a la contingencia en el caso de aquellos servidores que se encuentran fuera de su periodo de garantía. Cabe agregarse que todos los servidores usados como Hosts en la infraestructura de virtualización deben estar en garantía mientras estén en uso para las máquinas virtuales críticas.

Resolución de la contingencia:

En dado caso sean múltiples servidores los que fallan de manera simultánea, o deba darse prioridad a servidores en particular, a continuación, se muestra el orden de prioridad para restablecimiento de equipos o máquinas virtuales:

Recurso	Prioridad de Recuperación
Servidor de Base de Datos	Alta
Servidor Web Publico	Alta
Servidor de Aplicaciones	Media
Servidor de Correos	La más alta
Firewall	La más alta
Servidor de Respaldos	Media
Servidor de Dominio / DNS Privado	La más alta
Servidor de Hipervision o Supervisor	La más alta

CASO A: Error Físico de Disco de un Servidor (Sin RAID).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se deben tomar las acciones siguientes:

1. Ubicar el disco dañado.

2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.

4. Bajar el sistema y apagar el equipo.

5. Retirar el disco dañado y reponerlo con otro del mismo tipo, formatearlo y darle partición.

6. Restaurar el último respaldo en el disco, enseguida restaurar las modificaciones efectuadas desde esa fecha a la actualidad.

7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.

[1] Ver anexo 1 a plan de contingencia

8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de Memoria RAM

En este caso se dan los siguientes síntomas:

• El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.

• Ante procesos mayores se congela el proceso.

• Arroja errores con mapas de direcciones hexadecimales.

• Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto, si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la Institución, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

2. El servidor debe estar apagado, dando un correcto apagado del sistema.

3. Ubicar las memorias dañadas.

4. Retirar las memorias dañadas y reemplazarlas por otras iguales o similares.

5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.

6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

7. Probar los sistemas que están en red en diferentes estaciones.

Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

2. El servidor debe estar apagado, dando un correcto apagado del sistema.

3. Ubicar la posición de la tarjeta controladora.

4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.

5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.

6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

• Caída del servidor de archivos por falla de software de red.

• Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.

Bajar incorrectamente el servidor de archivos.

• Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz.

De encontrarse este volumen con problemas, se deberá descargar también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO E: Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

• Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación

• El antivirus muestra el nombre del archivo infectado y quién lo usó.

• Estos archivos (exe, com, etc.) serán reemplazados del disco original de instalación o del respaldo.

• Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Recursos de contingencia:

- Ultimo respaldo de la terminal.
- Media de instalación de sistema operativo.

Escenario 2: Interrupción de servicio de corriente eléctrica.

Impacto:

Impacto	Área Afectada
Paralización de sistemas o aplicaciones contenidas en los servidores.	Todas las áreas.
Posible pérdida de hardware	Gerencia de Tecnologías de la Información.
Perdida del proceso automático de respaldo y recuperación	Gerencia de Tecnologías de la Información.
Interrupción de operaciones	Gerencia de Tecnologías de la Información.

Descripción:

Este escenario contempla la posibilidad de que el suministro eléctrico que llega a los servidores falle. Dependiendo de la duración y/o magnitud de dicha falla, se pueden dar 3 escenarios:

- Falla de suministro.
- Pico de voltaje que daña equipo UPS.

- Falla de planta eléctrica.

Resolución de la contingencia:

CASO A: Falla de suministro por menos de 1 hora

En este caso, el equipo UPS encargado de los servidores, deberá contar con una potencia de 9000 watts y 10kva para cada uno de los gabinetes para poder soportar que los equipos se mantengan funcionando con todos sus servicios en línea, además deberá entrar en funcionamiento la planta eléctrica exclusiva para el centro de datos institucional después de 10 minutos de corte del suministro.

CASO B: Pico de voltaje que daña equipo UPS.

Se deberá tener redundancia de UPS entre gabinetes de manera tal que si uno falla los equipos continúan en funcionamiento, se deberá de reparar o reemplazar el UPS en el menor periodo posible.

CASO C: Falla de planta eléctrica.

Si además del fallo de suministro se presenta una falla de la planta eléctrica que imposibilite su resolución en un tiempo mayor a 50 minutos, se procede a apagar las máquinas virtuales en el orden establecido de prioridad, posteriormente se apagan los servidores físicos toda la actividad critica se ejecuta desde el sitio de contingencia, que por su naturaleza debe estar fuera de las oficinas de CONAMYPE.

Escenario 3: Perdida de servicio de internet o enlaces de datos

Impacto:

Impacto	Área Afectada
Indisponibilidad de servicios de comunicación con el exterior.	Todas las áreas.
Interrupción de operaciones de comunicación externa.	Gerencia de Tecnologías de la Información.

Descripción:

Este escenario contempla la posibilidad de que un enlace de internet o datos se encuentre no disponible.

Resolución de la contingencia:

En caso de la caída de uno de los enlaces de internet asignados al centro de datos, la carga debe trasladarse por completo a los enlaces restantes, para lo cual la institución debe de contar con al menos un enlace redundante para contingencia.

En caso que la interrupción incluya a todos los enlaces de Internet del centro de datos por más de 8 horas, se pasará al sitio externo de contingencia para continuar la prestación de los servicios de correo,

y aplicaciones web, así mismo los firewalls de los centros regionales re direccionaran hacia el sitio externo de contingencia.

Escenario 4: Incendio.

Impacto:

Impacto	Área Afectada
Indisponibilidad de servicios de comunicación con el exterior.	Todas las áreas.
Interrupción de operaciones de comunicación externa.	Gerencia de Tecnologías de la Información.

Descripción:

Este escenario contempla la posibilidad de que se dé un incendio en el centro de datos.

Resolución de la contingencia:

En caso de incendio en el centro de datos si una de las dos alarmas es activada y se identifica el conato de incendio, primero desactive el sistema contra incendio presionando el botón rojo identificado como tal tome el extintor de CO2 e inmediatamente apague el incendio.

Si las dos alarmas son activadas el sistema contra incendio se activará automáticamente por lo cual no entre al centro de datos bajo ninguna circunstancia, si por fallo del sistema este no se activa jale la palanca blanca con rojo del sistema contra incendio y salga inmediatamente del mismo.

Lugo de apagado el incendio se procede a identificar los servidores afectados, se procede a gestionar la garantía o reparar el servidor según sea el caso y se pasa los recursos no disponibles a otros servidores dentro del mismo centro de datos.

Si el centro de datos se destruye por completo los servicios son trasladados al sitio de contingencia ubicado en el sitio alterno de contingencia, en la cual pasan las máquinas virtuales.

Para este caso se deberá refilar el ludido extintor en el menor tiempo posible.

Escenario 5: Indisponibilidad del centro de datos.

Impacto:

Impacto	Área Afectada
Paralización de sistemas, servicios y comunicación.	Todas las áreas.

Posible pérdida de hardware o software	Gerencia de Tecnologías de la Información.
Perdida del proceso automático de respaldo y recuperación	Gerencia de Tecnologías de la Información.
Interrupción de operaciones	Gerencia de Tecnologías de la Información.

Descripción:

Este escenario contempla la posibilidad de que el centro de datos primario este indisponible, volviéndolo inaccesible o no disponible, por caso de terremotos, inundaciones que no permitan el acceso al centro de datos.

Resolución de la contingencia:

En caso de identificar que en el centro de datos está iniciando una inundación por lluvias, u otra situación como goteras, etc., proceda a apagar todos los servidores y notifique al encargado de servicios generales sobre la situación.

En caso de indisponibilidad del centro de datos primario, se activa el centro de datos externo. El uso del centro de datos externo se mantiene hasta la restauración de los servicios y la disponibilidad del centro de datos primario.

Identificar Impacto de la Caída y Tiempos Aceptables de Caída		
Recurso	Impacto	Tiempo de Caída Aceptable
Servidor de Base de Datos	No se tendrá acceso a ningún sistema informático ni sitio web	3 horas
Servidores Web	No se tendrá acceso a ERP desde fuera de la institución ni sitio web	8 horas
Servidor DNS	No existirá comunicación entre la central y sus regionales No se podrá realizar navegación a internet No se tendrá servidor de correo No se tendrá acceso al ERP	3 horas
Servidor Firewall	No existirá comunicación externa No habrá navegación hacia internet	5 horas
Servidores de Backup	En caso de emergencia no se tendrá acceso a los respaldos	8 horas

Recursos de Contingencia
Los recursos de contingencia son los siguientes

- Servidor de Aplicaciones
- Servidor de Base de Datos
- Servidor de Correo
- Servidor de Active Directory

Los servicios son trasladados al sitio de contingencia ubicado en el sitio alterno de contigencia, en la cual pasan las máquinas virtuales.

Equipos de contingencia

- 1 Firewall Palo Alto PA 850
- FotiADC
- 2 Servidor DELL R830
- 1 Servidor SAN
- 2 Switch Dell de alto desempeño
- 1 Enlace de Internet
- 1 Enlace de datos entre sitio principal y sitio de contingencia.

Escenario 6: Problemas con sistema operativo o versión de servidor virtual

Impacto:

Recurso	Prioridad de Recuperación
Servidor de Base de Datos	Alta
Servidor Web	Alta
Servidor de Aplicaciones	Media
Servidor Cloud	Media
Servidor Marketplace	Alta
Servidor de Correos	La más alta
Firewall	La más alta
Servidor de Respaldos	Media
Servidor de Dominio / DNS Privado	La más alta
Servidor de Hipervision o Supervisor	La más alta

Descripción:

Este escenario contempla la posibilidad de una actualización de versión tanto de sistema operativo como del software en particular de cada servidor sufra un daño irreparable debido a una actualización, corrupción de datos ente otras.

Resolución de la contingencia

En caso de identificar que una de los servidores físicos o virtuales presenta problemas tanto en su versión como en su sistema operativo, se recurre al último respaldo de máquina virtual disponible y se verifica el problema presentado en un ambiente controlado. Para el caso de los equipos como firewall y DNS se notifica a la empresa que brinda el soporte para resolver o gestionar el cambio del equipo según sea el caso.

En caso de indisponibilidad del centro de datos primario, se activa el centro de datos externo. El uso del centro de datos externo se mantiene hasta la restauración de los servicios y la disponibilidad del centro de datos primario.

Identificar Impacto de la Caída y Tiempos Aceptables de Caída		
Recurso	Impacto	Tiempo de Caída Aceptable
Servidor de Base de Datos	No se tendrá acceso a ningún sistema informático ni sitio web	3 horas
Servidores Web	No se tendrá acceso a ERP desde fuera de la institución ni sitio web	8 horas
Servidor DNS	No existirá comunicación entre la central y sus regionales No se podrá realizar navegación a internet No se tendrá servidor de correo No se tendrá acceso al ERP	3 horas
Servidor Firewall	No existirá comunicación externa No habrá navegación hacia internet	5 horas
Servidores de Backup	En caso de emergencia no se tendrá acceso a los respaldos	8 horas

Recursos de Contingencia
Los recursos de contingencia son los siguientes

- Servidor de Aplicaciones
- Servidor de Base de Datos
- Servidores web
- Servidor de Correo
- Servidor de Active Directory

Los servicios son trasladados al sitio de contingencia ubicado en el sitio alterno de contingencia, en la cual pasan las máquinas virtuales.

Equipos de contingencia

- 1 Firewall Palo Alto PA 850

- 1 Application Delivery Controller FortiADC
- 2 Servidor DELL R830
- 1 Servidor SAN
- 2 Switch Dell de alto desempeño
- 1 Enlace de Internet
- 1 Enlace de datos entre sitio principal y sitio de contingencia.

Escenario 7: Ausencia parcial o permanente de personal de IT.

Impacto

Impacto	Área Afecta
Interrupción de funciones de la persona ausente • **Ajustes de programas críticos en producción** • **Control y Monitoreo de servidores** • **Soporte técnico a usuarios** • **Administración de Bases de datos** • **Soporte a sitio web**	Todas las Áreas de la Institución

Resolución de la contingencia:

Para resolver una falta de una de las personas de la Gerencia de Tecnologías de la Información deberá de definirse por la jefatura de la Unidad de Infraestructura y Seguridad Informática o la Unidad de Desarrollo de Software quien cubrirá a esta persona de manera temporal.