



COMISIÓN NACIONAL DE LA MICRO
Y PEQUEÑA EMPRESA

PLAN DE CONTINGENCIA INFORMÁTICO

2023

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO
Y PEQUEÑA EMPRESA

Titulo	Plan de Contingencia Informático		
Elaborado por:	Carlos Sermeño Jefe de la Unidad de Informática		
Autorizado por:	Carlos Carbajal Director de Innovación, Calidad y Tecnología		
Fecha de elaboración:	2018-11-28		
Última modificación:	2023-11-18		
Versión	Responsable	Notas	Fecha de modificación
1	Carlos Sermeño	Versión Inicial	2018-11-10
2	Carlos Sermeño	Revisión año 2021	2021-05-20
3	Guillermo Celarie	Inclusión de nuevas máquinas virtuales y servicios. Inclusión de escenario de falla de equipo de comunicaciones, falla de equipo de aire acondicionado.	2022-05-17
4	Guillermo Celarie	Ajuste para contemplar el uso de proveedor de nube, cluster alternativo y manejo preciso de máquinas virtuales.	2023-11-18



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

Contenido

Introducción	4
Definiciones	5
Objetivos	5
Alcance	5
Análisis y Evaluación de Riesgos.....	5
Escenarios contemplados para el plan de contingencia	7
Planificación	7
Estrategias para garantizar continuidad de procesos y servicios de IT.....	7
Escenario 1: Falla de Servidor	8
Escenario 2: Interrupción de servicio de corriente eléctrica.	13
Escenario 3: Pérdida de servicio de internet o enlaces de datos.....	14
Escenario 4: Incendio.	15
Escenario 5: Indisponibilidad del centro de datos.	16
Escenario 6: Falla de máquina virtual	17
Escenario 7: Ausencia parcial o permanente de personal de IT.	19
Escenario 8: Ataques informáticos.....	20
Escenario 9: Falla de equipo de comunicación	21
Escenario 10: Falla de unidad de aire acondicionado del centro de datos institucional.....	24
Escenario 11: Falla de clúster de virtualización	25
Glosario	26
Anexos.....	27
Anexo 1: tabla de contacto de proveedores.....	27



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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 host de virtualización.• Falla de equipo especializado de comunicación.	Falla de servidor
<ul style="list-style-type: none">• Corte general de servicio de corriente eléctrica.	Interrupción de servicio de corriente eléctrica
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• Terremoto.• Incendio.• Inundación.• Corto circuito.	Indisponibilidad del centro de datos (destrucción del centro)
<ul style="list-style-type: none">• Accidente.• Renuncia inmediata.	Ausencia parcial o permanente de personal de IT
<ul style="list-style-type: none">• Falla de máquina virtual.	Falla de máquina virtual
<ul style="list-style-type: none">• Falla de clúster de virtualización	Falla de clúster de virtualización





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

Definiciones

A. CONTINGENCIA:

Interrupción no planificada de la disponibilidad de recursos informáticos.

B. PLAN DE CONTINGENCIA:

Conjunto de tareas (de DETECCIÓN 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.



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

- Al devolver la máquina virtual a un estado válido en el centro de datos principal, se hará un proceso de sincronización de datos de ser necesario previo a redirigir tráfico nuevamente hacia ella, sea este de manera interna o a través de un proceso de restauración de la máquina virtual en cuestión.
- Cada máquina virtual del ambiente de producción deberá contar con una tarea de respaldo automatizado asociada.
- **Almacenamiento y Respaldo de la Información (BACKUPS)**
 - Procedimiento de Backup - definen la frecuencia de los respaldos (diario, periódico) y su tipo (incremental o total), considerando la criticidad de los datos y la frecuencia con que se introduce nueva información. Para las máquinas virtuales del ambiente de producción se deberá tener un punto objetivo de recuperación de 48 horas máximo en caso de que no estén asociadas a servicios críticos, y de 24 horas máximo para las asociadas a servicios críticos. Para todos los casos se deberá contar con un Punto de recuperación en el tiempo de 7 días.
 - Los datos se respaldarán en medios magnéticos en el repositorio local, y podrán estar respaldados adicionalmente en un sitio externo, como un proveedor de nube. Este requerimiento es obligatorio para las máquinas asociadas a servicios críticos.
- **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. Este sitio alternativo puede ser un centro de datos fuera del sitio principal, o bien, un proveedor de nube.
- **Implementación de soluciones altamente disponibles o tolerantes a fallos**
 - Para reducir el impacto de posibles fallas de recursos, ya sean estas de componentes o de equipos completos, se deberá optar por soluciones tolerantes a fallos o altamente disponibles, como el uso de arreglos RAID para los repositorios de datos como SAN, NAS por ejemplo, y el uso de soluciones como vSAN, y otras que permitan el uso de múltiples servidores de cómputo.

Escenario 1: Falla de Servidor

Descripción:

Este escenario contempla la posibilidad de que un equipo servidor se dañe de manera que interrumpa los servicios provistos por este. Nótese que aplica exclusivamente a servidores físicos, y no a máquinas virtuales, en tanto que el aspecto de hardware no aplica a estas.

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

Escenarios contemplados para el plan de contingencia

1. Falla de Servidor.
2. Interrupción de servicio de corriente eléctrica.
3. Pérdida de servicio de internet o enlaces de datos.
4. Incendio
5. Indisponibilidad del centro de datos
6. Falla de máquina virtual
7. Ausencia parcial o permanente de personal de IT.
8. Ataques informáticos
9. Falla de equipo de comunicación
10. Falla de unidad de aire acondicionado del centro de datos institucional
11. Falla de clúster de virtualización

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 con este plan, se procederá a la activación de la máquina virtual, primero desde un clúster secundario local, y luego desde un proveedor de nube.



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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.
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:

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

Como prerequisite, los servidores con carga de entorno de producción deberán contar con un plan de soporte y garantía al día, con un plan de soporte que cubra al menos respuesta de soporte y partes al siguiente día hábil. En el caso de los servidores que no manejan procesos o datos de entorno de producción podrán hacer uso de las actividades planteadas en la resolución de contingencia.

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

Resolución de la contingencia:

Servidores con plan de soporte y mantenimiento activo:

Al momento de recibir alerta de falla de componente, se deberá contactar al personal de soporte contratado, informando de la falla, y solicitando soporte de acuerdo con el SLA contratado. Mientras se resuelve la contingencia:

- En caso de host de virtualización:
 - Se procurará no utilizar el recurso con nuevas cargas, y se migraran las cargas a otros hosts.
 - Si funciona como host de vSAN deberá ponerse en modo mantenimiento, de manera que los datos se encuentren debidamente respaldados en otros hosts.
- En caso de servidor de almacenamiento:
 - Verificar el correcto funcionamiento del arreglo de discos, y la configuración necesaria para su rearmado en caso de falla total.

Servidores sin plan de soporte, mantenimiento o garantía activo:

Al momento de recibir la alerta de falla, deberá notificar a las áreas que pudieran ser afectadas por la falla. Posteriormente se realizarán las siguientes acciones dependiendo el caso que aplique:



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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.

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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 crítica se ejecuta desde el sitio de contingencia, que por su naturaleza debe estar fuera de las oficinas de CONAMYPE.

CASO D: Falla de transferencia eléctrica automática.

Si después de los 10 minutos posteriores al corte de suministro el generador eléctrico no entra en funcionamiento automáticamente, se deberá acceder presencialmente al generador e iniciarlo de manera manual. En caso de que el generador de emergencia haya entrado en funcionamiento, pero no se restablezca la alimentación a los UPS en el centro de datos, se deberá activar la transferencia eléctrica de manera manual. Si ninguno de estos procesos funciona, deberá seguirse el proceso como un caso C, de acuerdo a lo allí establecido.

Escenario 3: Pérdida 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:

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

- 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.
- Falla de proceso de transferencia eléctrica automática.

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



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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 alternativo. El uso del centro de datos alternativo 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
Clúster de servidores de Base de Datos	No se tendrá acceso a ningún sistema informático que haga uso de bases de datos relacionales no configuradas localmente	3 horas
Servidores Web	No se tendrá acceso a ERP desde fuera de la institución ni sitio web	8 horas
Servidor DNS	No se podrá realizar navegación a internet	3 horas





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

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 24 horas hábiles, 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.

Luego 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 alternativo de contingencia, en la cual pasan las máquinas virtuales.

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



COMISIÓN NACIONAL DE LA MICRO
Y PEQUEÑA EMPRESA

Recurso	Prioridad de Recuperación
VM Clúster de Base de Datos	Alta
VM Web Publico	Alta
VM ERP	Alta
VM de ActiveDirectory / DNS Privado	La más alta
VM de Hipervisor o Supervisor	La más alta
VM WAF	Alta
VM FECAMYPE	Media
VM EXPORTA.SV	Baja
VM base de datos EXPORTA.SV	Baja
VMs PKI (CAs, OCSP)	Media
VM API publica	Media
VM de autenticación regional	Media
VM repositorio de código	Baja
VM de integración continua	Baja
VM revista MYPE	Baja
VM de administración biométricos	Baja
VM de respaldo ActiveDirectory	Alta
VM nube privada	Baja
VM de gestión de proyectos IT	Baja
VM API privada	Media
VM base de datos serv. Públicos	Alta
VM base de datos postgresql	Baja
VM SSO GlobalProtect	Media
VM herramientas CI/CD	Media
VM EXPOMYPE.SV	Baja
VM SMODASV.COM	Baja

Descripción:

Este escenario contempla la posibilidad de una falla critica en el funcionamiento de una máquina virtual, ya sea por una actualización de versión, tanto de sistema operativo como del software en particular que provoque un daño irreparable debido a una actualización, o corrupción de datos ente otras.

Resolución de la contingencia

En caso de que una reparación de paquetes o sistema sea imposible, se recurre al último respaldo de máquina virtual disponible y se verifica el problema presentado en un ambiente controlado. Para

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

	No se tendrá servidor de correo No se tendrá acceso al ERP	
Equipo Firewall	No existirá comunicación externa No habrá navegación hacia internet No habrá comunicación entre las subredes conectadas al equipo.	5 horas
Servidores de Backup	En caso de emergencia no se tendrá acceso a los respaldos	8 horas
Equipo Balanceador de enlaces	No se tendrá acceso a los recursos institucionales desde Internet	8 horas
Servidor virtual WAF	No se tendrá acceso a los recursos protegido actualmente por el appliance	8

Recursos de Contingencia

Los recursos de contingencia son los siguientes

- Máquina virtual ERP
- Servicio de Base de Datos de producción
- Máquina virtual de Active Directory
- Máquina virtual del sitio web
- Máquina virtual FECAMYPE
- Servicio de base de datos para aplicativos expuestos al público.
- Repositorio de código

Los servicios son trasladados al sitio alternativo de ser posible, o en su defecto inicializados desde la última copia de respaldo disponible.

Después de inicializar las máquinas virtuales críticas, deben realizarse los ajustes IP correspondientes en las mismas para garantizar accesibilidad, así como en los DNS correspondientes.

Escenario 6: Falla de máquina virtual

Impacto:

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

- Control y Monitoreo de servidores
- Soporte técnico a usuarios
- Administración de Bases de datos
- Soporte a sitio web

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.

Escenario 8: Ataques informáticos

Descripción: Uno de los servidores virtuales se ve comprometido por un ataque informático, que lo vuelve infraestructura oscura o vuelve ilegibles los datos contenidos en él. El siguiente caso que se tratara es la denegación de servicio para un servicio en línea.

Resolución de la contingencia:

1. Aislamiento de la máquina virtual comprometida.
2. Copia de los archivos contenidos a un servidor de archivos Linux, sin copiar los permisos, eliminando así la ejecución de archivos.
3. Correr antivirus y corrector de vulnerabilidades sobre los archivos posiblemente expuestos.
4. Reinstalación y reactivación de los servicios, configuraciones y otros en un nuevo servidor virtual, con una IP diferente.
5. Instalación de un servidor en la IP del servidor comprometido de manera que se registren todas las llamadas hacia esa IP en un periodo de 3 meses, buscando así otras partes de la infraestructura que pudieran estar comprometida.
6. Analizar y revisar los equipos que salgan comprometidos del paso anterior de acuerdo a este proceso.
7. Apagar los servidores honeypot y documentar la nueva infraestructura.

En caso de un ataque de denegación de servicio hacia un servicio en línea:

- Mover el registro DNS hacia una plataforma especializada, como CloudFlare.
- Configurar una comunicación privada entre la plataforma y el servicio.
- Activar las restricciones de DDoS en la plataforma y registrar los eventos.

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

el caso de los equipos como firewall y balanceador de enlaces 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 de la maquina en el centro de datos primario, se activa el centro de datos alterno. El uso del centro de datos alterno se mantiene hasta la restauración de los servicios y la disponibilidad en el centro de datos primario.

Identificar Impacto de la Caída y Tiempos Aceptables de Caída		
Criticidad del recurso	Impacto	Tiempo de Caída Aceptable
La más alta	No se tendrá acceso a ningún sistema informático, afectando incluso navegación.	3 horas
Alta	No se tendrá acceso a servicios de aplicaciones vitales para el desempeño diario de funciones	8 horas
Media	Algunas funcionalidades de aplicativos no estarán disponibles. La navegación a internet para usuarios podrá verse comprometida.	72 horas
Baja	Servicios no vitales podrán encontrarse no accesibles, como sitios web de proyectos. El despliegue de software podrá verse parado o limitado.	120 horas

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

Descripción:

La Gerencia de Tecnología de la Información pierde talento humano, ya sea de manera parcial o permanente.

Impacto:

Impacto	Área Afecta
Interrupción de funciones de la persona ausente	Todas las Áreas de la Institución
<ul style="list-style-type: none">Ajustes de programas críticos en producción	



COMISIÓN NACIONAL DE LA MICRO
Y PEQUEÑA EMPRESA

	redundante, se asume falla de conectividad. Si no es parte de un clúster, se pierde conectividad de los equipos conectados a este switch.	
Switch de capa de distribución	Degradación de la calidad del servicio de conectividad de los equipos conectados de manera redundante a otros integrantes del clúster, incluyendo la comunicación de switches inferiores. En el caso de equipos sin conexión redundante, se asume falla de conectividad. Si no es parte de un clúster, se pierde conectividad de los equipos conectados a este switch.	8 horas
Switch de capa de acceso	No existirá comunicación entre los equipos conectados a la red institucional o internet en caso de los equipos regionales	24 horas
Media converter, router de proveedor externo	No existirá comunicación externa No habrá navegación hacia internet	8 horas

Resolución de la contingencia:

Para resolver la falla de equipos de comunicación, se resolverá la contingencia dependiendo del tipo de equipo. Sin embargo, en el caso de los switches de núcleo y distribución, se deberán mantener las siguientes consideraciones previas:

- Contratos de soporte y garantía vigentes para los equipos.
- Las capas núcleo y distribución deberán ser parte de clusters, de manera que sean parte de un conjunto tolerante a fallos.
- Los equipos estarán conectados a la alimentación eléctrica de 2 baterías de respaldo diferentes, a través de sus fuentes redundantes.

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

- Al finalizar la contingencia, almacenar los registros y devolver el registro al balanceador de enlaces de ser necesario.

Escenario 9: Falla de equipo de comunicación

Descripción:

Uno o varios de los equipos de comunicación falla de manera que compromete el throughput del mismo, la calidad del servicio o el acceso a los recursos conectados a él. Dependiendo la ubicación del mismo y si forma parte de un clúster, el riesgo y el impacto son elevados correspondientemente de la siguiente manera:

Identificar Impacto de la Caída y Tiempos Aceptables de Caída		
Recurso	Impacto	Tiempo de Caída Aceptable
Router-Firewall	Si el equipo es parte de un cluster: Degradación de calidad del servicio para los equipos conectados de manera redundante. Pérdida de conectividad para los equipos no conectados a otro integrante del cluster Si no es parte de un cluster: Pérdida de la conectividad entre las redes conectadas al mismo. Pérdida de acceso a internet o proveedor de nube	3 horas
Balanceador de enlaces	Pérdida de accesibilidad a servicios desde el exterior.	3 horas
Switch de capa de núcleo	Si es parte de un clúster: Degradación de la calidad del servicio de conectividad de los equipos conectados de manera redundante a otros integrantes del clúster, incluyendo la comunicación de switches inferiores. En el caso de equipos sin conexión	3 horas



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

En el caso de falla de router-firewall:

- Informe inmediato al proveedor local de soporte para iniciar el trámite de garantía y soporte con el fabricante.
- Si la contingencia no se puede resolver en un periodo aceptable de acuerdo con la tabla anterior y se configura el equipo remanente de la siguiente manera:
 - Trasladar las interfaces que no poseen redundancia del clúster hacia el equipo activo.
 - Habilitar las políticas relacionadas a esas interfaces.
 - Al finalizar la contingencia se devuelve la configuración a su estado anterior.

La tabla con información de centros de llamada para equipos y proveedores se muestra como el Anexo 1: tabla de contacto de proveedores.

Escenario 10: Falla de unidad de aire acondicionado del centro de datos institucional

Descripción:

Uno o varios de los equipos de aire acondicionado dentro del centro de datos institucional falla.

Resolución de la contingencia:

En caso de que el aire principal falle y no haya entrado el siguiente equipo de manera automática:

1. Activar la unidad secundaria, moviendo los sets hacia On y Cool en caso que no lo estén.
2. Apagar el equipo principal en caso que se muestre como encendido, pero sin obtener resultados.
3. Notificar a la unidad de servicios generales o al proveedor del soporte para el equipo e iniciar el proceso de reparación.

En caso falle el aire acondicionado secundario o se esté en un escenario con un único equipo de aire acondicionado central:

- Apagar los equipos en caso se muestren como encendidos, pero sin obtener resultados.
- Encender los equipos de aire acondicionado incluidos en cada gabinete. Dichos equipos están en la parte inferior de todos los gabinetes de datos, y ponerlos a 20° C.

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

Con las precondiciones planteadas, los siguientes pasos serán ejecutados para la resolución de la contingencia de los equipos de núcleo y distribución:

- Informe inmediato al proveedor local de soporte para iniciar el trámite de garantía y soporte con el fabricante.
- Si fallan todos los integrantes del clúster, se deberán apagar los servidores para evitar fallas en el arreglo de vSAN en el caso de los servidores de distribución.
- Notificar inmediatamente a la cadena jerárquica en caso de escalado de la contingencia. En caso de escalar, se tomarán los pasos como fallo de servidores.

En caso de los switches de acceso se tomarán los siguientes pasos:

- Carga de la configuración más reciente del equipo dañado en uno de los equipos de contingencia.
- Remoción del switch dañado e instalación del switch de contingencia.
- Prueba de conectividad de los equipos asociados.
- Gestión de soporte y garantía del switch dañado si aplica.

En el caso de media converter o router de proveedor:

- Notificación inmediata al proveedor de soporte o garantía relacionado al equipo.
- Habilitación de enlace alternativo como canal principal en caso que el cambio no haya sido automático en el equipo balanceador de enlaces
- Gestionar la reparación del equipo o enlace
- Devolución de la carga de enlaces a su estado nominal

En el caso de falla del balanceador de enlaces:

- Informe inmediato al proveedor local de soporte para iniciar el trámite de garantía y soporte con el fabricante.
- Si la contingencia no se puede resolver en un periodo aceptable de acuerdo con la tabla anterior, se procede a habilitar un enlace de internet directamente al equipo router-firewall:
 - Habilitación de política de ruta por defecto a la interfaz conectada.
 - Inhabilitación de política de ruta por defecto tradicional.
 - Configuración de interfaz de acuerdo con el direccionamiento IP del proveedor de internet a usar.
 - Al finalizar la contingencia se devuelve la configuración a su estado anterior.



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

Resolución de la contingencia:

Este es un escenario de alto impacto, por lo que se deberá llamar inmediatamente al personal de soporte de la plataforma de virtualización para obtener apoyo lo más pronto posible. Adicionalmente, deberán realizarse las siguientes acciones:

- Trasladar máquinas virtuales críticas a clúster secundario o a proveedor de nube, dependiendo la necesidad. Esta tarea es requerida en caso se dé la pérdida de 2 o más integrantes del arreglo.
- Garantizar la disponibilidad de respaldos recientes para las máquinas virtuales del clúster.
- Evitar crear nuevas máquinas virtuales en el clúster. En caso de ser necesario, hacer uso del clúster alternativo o de proveedor de nube.
- En caso de pérdida de 2 o más integrantes, ajustar registros DNS en sitio alternativo de manera que el direccionamiento de los servicios se dé a las máquinas virtuales apropiadas.
- Al finalizar la contingencia acompañado de personal de soporte del proveedor devolver las máquinas virtuales después de garantizar pleno funcionamiento del clúster.

Glosario

Servidor: Computadora capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Para efectos de este plan hace referencia a equipos especializados para despliegue en centros de datos.

Máquina virtual (virtual machine, VM): Software que simula un sistema de computación y puede ejecutar programas como si fuese una computadora real.

Hipervisor: Plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora. Es una extensión de un término anterior, «supervisor», que se aplicaba a los kernels de los sistemas operativos de computadora.

SAN: Una red de área de almacenamiento (SAN) es una red de alta velocidad independiente y dedicada que interconecta y suministra depósitos compartidos de dispositivos de almacenamiento a varios servidores. Cada servidor puede acceder al almacenamiento compartido como si fuera una unidad conectada directamente al servidor. Una SAN suele montarse con cableado, adaptadores de bus de host y conmutadores SAN conectados a matrices de almacenamiento y servidores. Cada conmutador y cada sistema de almacenamiento de la SAN debe estar interconectado.





COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

- Notificar a la unidad de servicios generales o al proveedor del soporte para el equipo e iniciar el proceso de reparación.

En caso de falla total de todos los equipos de aire acondicionado:

- Apagar todos los servidores que no sean vitales de acuerdo a lo establecido en el escenario de falla de suministro eléctrico para el centro de datos.
- Apagar las máquinas virtuales no necesarias de manera que los servidores no calienten en exceso.
- Si los servidores que permanecen encendidos se alarman, tratar la contingencia como fallo de alimentación completa e iniciar el proceso de apagado total.

Escenario 11: Falla de clúster de virtualización

Descripción: El clúster de virtualización vSAN falla, perdiendo uno o más de sus integrantes, ya sea de manera parcial o permanente.

Impacto:

Subescenario	Impacto	Área Afectada
Pérdida temporal de un integrante del arreglo	<ul style="list-style-type: none">• Pérdida temporal de datos de paridad.• Maquinas que estaban funcionando desde el integrante deben ser reiniciadas en otro host.• Reducción de capacidad de tolerancia a fallos	Gerencia de Tecnologías de la información
Pérdida total de un integrante del arreglo	<ul style="list-style-type: none">• Posible pérdida de datos de paridad del arreglo.• Perdida de tolerancia a fallos.	Gerencia de Tecnologías de la información
Perdida de 2 o más integrantes del arreglo	<ul style="list-style-type: none">• Se deja de contar con tolerancia a fallos y el clúster deja de funcionar apropiadamente.• Posible pérdida/corrupción de datos de máquinas virtuales	Todas las áreas



COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

NAS: Dispositivo de almacenamiento de alta capacidad conectado a una red que permite a los usuarios y clientes autorizados almacenar y recuperar datos en una ubicación centralizada.

Anexos

Anexo 1: tabla de contacto de proveedores

EQUIPOS/SERVICIOS	NOMBRE DEL PROVEEDOR	EMAIL/ TELÉFONO DE CONTACTO
VM WAF BALANCEADOR DE ENLACES WAF IBW ROUTER-FIREWALL PALO ALTO VIRTUALIZACION VMWARE SOFTWARE DE RESPALDO DE SERVIDORES VEEAM SERVICIO DE NUBE	JMTelcom S.A de C.V IBW El Salvador ETS Consulting S.A de C.V Grupo RAF S.A de C.V Escucha Group S.A de C.V	Morena.castro@jmtelcom.com / 2246-6000 2529-4800 soporte@ets.consulting / 2234-2757 Max.barrera@gruporaf.com / 7455-5270 damaris.velasquez@escuchagroup.com/ 7308-1434
ENLACE DE INTERNET PRIMARIO ENLACE DE INTERNET REGIONALES ENLACE DE INTERNET USUARIOS-CENTRAL ENLACE CON MINISTERIO DE HACIENDA (SAFI) ENLACE DE INTERNET SECUNDARIO ENLACE DE INTERNET USUARIOS – SECUNDARIO	Cablecolor S.A de C.V GCA Telecom S.A de C.V	7988-3800 servicioalcliente@gcatelecom.com.sv / 2230-0555

Autorizado por medio de Punto 4.2.4 del Acta 111 de la sesión de Junta Directiva del 21 de diciembre de 2023



