GOBIERNO DE
EL SALVADOR

MINISTERIO
DE ECONOMÍA

Plan de Contingencia Informática

Julio de 2020

Contenido

1. Introducción

El presente documento es el Plan de Contingencia Informático del Ministerio de Economía en materia de Riesgos de Tecnología de Información (IT).

Establece el alcance, objetivo y metodología desarrollada. Incluye además las definiciones utilizadas, políticas de seguridad, análisis de impacto, análisis de información, identificación de riesgos y controles y la clasificación de activos de TI.

La metodología comprende: Identificación de riesgos, clasificación de la probabilidad que ocurra un siniestro, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencia.

Permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y entidades asociadas, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

2. Definiciones

- **Contingencia:** Posibilidad o riesgo que suceda un evento.
- **Plan de contingencia:** Tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

3. Objetivos

- Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- 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.

4. Análisis y evaluación de riesgos

Los desastres causados por un evento natural o humano, pueden ocurrir, en cualquier parte. Se han identificado contingencias como:

- Riesgos naturales: tales como mal tiempo, terremotos, etc.
- Riesgos Tecnológicos: fallas de energía y accidentes de transmisión y transporte.
- Riesgos sociales: como siniestros humanos y desordenes.

Dentro del presente documento se han cubierto los riesgos tecnológicos que se presentan en el siguiente cuadro.

Causas	Escenarios
Falla de UPS(Suministro eléctrico)	Corte eléctrico
Corte general de suministro eléctrico	Interrupción del fluido eléctrico durante la ejecución de los procesos
Fallas en el software de acceso a internet Pérdida de comunicación con proveedores de internet	Perdida de servicio de internet

5. Escenarios

5.1. Perdida de enlace de comunicación (Internet)

El Ministerio de Economía cuenta con un enlace de comunicaciones de internet con la empresa DIGICEL de 95Mbps, el cual es utilizado para publicar servicios que el Ministerio brinda a otras entidades, usuarios y público en general, entre los cuales podemos mencionar sitios web, correo electrónico, VPN, consultas GLP, Hidrocarburos y minas. Además, se utiliza para brindar servicio de internet a los usuarios internos ubicados en el Ministerio como en la Dirección General de Estadísticas y Censos y CENADE.

Plan de acción

En caso de fallar el enlace principal se ha contratado un enlace secundario con la empresa CLARO de 10Mbps para que la comunicación pueda ser restablecida automáticamente, ya que se ha configurado la función "Fail Over" en los equipos de seguridad. Esta función permite el monitoreo constante de los enlaces y al detectar la caída de alguno, automáticamente dirige todo el tráfico al enlace redundante.

Tiempo estimado de ejecución

Basado en pruebas realizadas, el tiempo que tarda en activarse el enlace secundario al detectarse la caída del enlace primario es de menos de 1 minuto.

Contactos para el reporte de fallas

Para fallas del enlace primario se debe contactar al proveedor de acuerdo a la siguiente pirámide de escalamiento:

Área técnica	
1er. Nivel de Contacto	NOC DIGICEL
Tel.	(503)2285-5252
Email	Soporte.4G@digicelgroup.com
1 Hora 2do. Nivel de Contacto	María Elena Quintero Ejecutiva de Cuenta
Cel.	+503 7398 7577
Email	maria.quintero@escuchagroup.com
2 Horas 3er. Nivel de Contacto	Edwin Vasquez
Tel.	+503 22855252
Cel.	
Email	Edwin.Vasquez@digicelgroup.com

Para fallas del enlace secundario se debe llamar a CLARO al siguiente número de contacto:

Área técnica	
ID de enlace	1037152
Contacto	Contact Center
Tel.	(503)2250-3333
Email	clientescorporativos@claro.com.sv

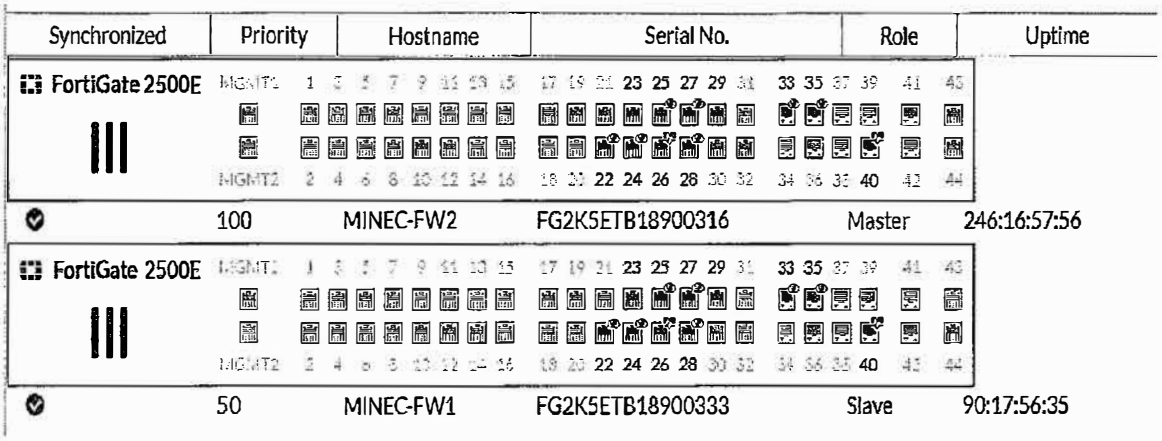
5.2. Fallo de Firewall Central

EL MINEC utiliza un Firewall Fortinet 2500E como equipo de seguridad central, el cual se encarga de las políticas de navegación de los usuarios, bloqueo de accesos no autorizados y a nivel de perímetro realiza funciones anti-spam, filtrado web, antivirus, IPSIDS, DDOS, SSL.

Todas las rutas a sitios remotos están configuradas en este equipo, por lo tanto, es crítico que este se mantenga en funcionamiento 24/7.

Plan de acción

Para realizar mantenimientos o en caso de fallo se cuenta con otro equipo de iguales características (Fortigate 2500E) que inicia su funcionamiento cuando el dispositivo principal falla y que toma todo el tráfico para mantener la continuidad en las comunicaciones.



Tiempo estimado de ejecución

Se configuró esquema en High Availability(HA) Alta Disponibilidad, lo que garantiza interrupciones mínimas y los cambios entre equipos se realizan de forma automática cuando se detecta la caída del principal. En pruebas realizadas se observaron caídas menores a un minuto.

Contactos para el reporte de fallas

Área técnica	
Contacto	Morena Castro
Tel.	(503)2246-6065
Email	morena.castro@jmtelcom.com.sv
Contacto Emergencias	Técnicos
Tel.	(503)2246-6005
Cel.	(503)7910-7529

5.3. Fallo de controlador de dominio

Los servicios de directorio se ejecutan en el servidor llamado vsrv-dc1.minec.gob.sv, cuya tarea es proveer servicios de inicio de sesión a usuarios del dominio minec.gob.sv, además contiene políticas de uso de equipos aplicadas a usuarios. El fallo de este equipo sería crítico ya que no permitiría el inicio de sesión a los usuarios perdiendo el acceso a sus configuraciones y correo electrónico.

Plan de acción

En caso de fallo en el controlador de dominio vsrv-dc1.minec.gob.sv, se ha instalado una réplica del controlador principal, llamado vsrv-dc2.minec.gob.sv, permitiendo el inicio de sesión y la entrega de políticas a los usuarios de forma automática en caso de no encontrase en línea el servidor primario. Esto permitirá la recuperación del servidor principal sin que afecte a los usuarios del dominio.

Tiempo estimado de ejecución

Ambos equipos se encuentran funcionando, y el servidor vsrv-dc2.minec.gob.sv tomará el rol de maestro cuando no se encuentre en la red al controlador primario.

Si el controlador primario sufriera algún daño de hardware, se estima que la reinstalación tomaría 45 minutos, lo cual no afectaría a los usuarios porque estaría funcionando el controlador secundario.

Contactos para el reporte de fallas

Área técnica	
Contacto	Alex Lemus Jefe de Soporte y de Infraestructura
Tel.	(503)2590-5522
Email	alex.lemus@minec.gob.sv
Cel.	(503)7070-6030

5.4. Fallo de servidor DHCP para red inalámbrica

El Ministerio utiliza el equipo FORTINET 2500E para brindar servicio de internet inalámbrico tanto a usuarios internos como invitados, este se encuentra funcionando en DATA CENTER.

Si este presentara alguna falla, entra inmediatamente la High Availability(HA) Alta disponibilidad.

Plan de acción

Automáticamente entra a funcionar otro FORTIGATE 2500E.

Tiempo estimado de ejecución

Inmediatamente.

Contactos para el reporte de fallas

Área técnica	
Contacto	Alex Lemus Jefe de Soporte y de Infraestructura
Tel.	(503)2590-5522
Email	alex.lemus@minec.gob.sv
Cel.	(503)7070-6030

5.5. Fallo en servidores de bases de datos SQL Server y Oracle

Los servidores de bases de datos son los contenedores de todos los sistemas desarrollados por el Ministerio de Economía, la perdida de estas bases de datos sería un incidente crítico de seguridad, por lo tanto debe existir un plan de contingencia.

Plan de acción

En caso de fallas en estos servidores, se tendrá la opción de recuperarse desde archivos de respaldo generados por el motor de base de datos diariamente y que se almacenan en un equipo dedicado a guardar respaldos. Estos respaldos incluyen archivos de respaldo completos (MDF) así como del archivo de logs (LDF). También se cuenta con la opción de recuperar todo el servidor mediante un archivo de imagen (v2i) realizado con la herramienta Backup Exec System Recovery 2011. En ambos casos podemos recuperar hasta 2 meses atrás que es lo que se resguarda en el sitio remoto de almacenaje.

Tiempo estimado de ejecución

En caso de daño severo en los servidores de base de datos, el tiempo estimado para que los usuarios vuelvan a acceder a la base de datos es de aproximadamente 4 horas, siguiendo el procedimiento descrito a continuación:

a) Restauración de base de datos en el mismo servidor. De no ser posible se realiza el paso2. (Aproximadamente 30 minutos)

b) Revisar si se trata de daño físico y si se cuenta con la parte a remplazar, de no ser así se procede con el paso 3. (Aproximadamente 30 minutos)

c) Seleccionar equipo con similares características para montar imagen o reinstalar sistema operativo con motor de base de datos, en caso contrario se procede con el paso 4. (Aproximadamente 120 minutos)

d) Se convierte la imagen del servidor en equipo virtual y se monta en cualquier servidor de máquinas virtuales que utilice actualmente el MINEC y que cuente con características

mínimas necesarias para ejecutar la imagen del o de los servidores de base de datos. (Aproximadamente 60 minutos)

Contactos para el reporte de fallas

Área técnica	
1er. Nivel de Contacto	Mario Hernández
Tel.	(503) 2590-5431
Cel.	(503) 7070-6260
Email	mario.hernandez@minec.gob.sv
1 Hora 2do. Nivel de Contacto	Jorge Guevara DBA
Tel.	(503) 2590-5432
Cel.	(503) 7070-6266
Email	jorge.guevara@minec.gob.sv

5.6. Fallo en plataforma Miempresa.gov.sv

El sistema MiEmpresa.gob.sv permite que los comerciantes individuales y las sociedades realicen sus trámites empresariales en línea.

Plan de acción

En caso de reportes sobre fallas del sistema o que las personas que ingresan al portal MiEmpresa.gob.sv no les llegan correos electrónicos automáticos de respuesta, se debe crear un ticket enviando un correo a jira@miempresa.atlassian.net, esto crea una incidencia en la mesa de ayuda dispuesta por la UNCTAD.

Contactos para el reporte de fallas

Área técnica	
1er. Nivel de Contacto	Ernesto Lizano
Institución	UNCTAD
Cel.	(503)7940-3648
e-mail	ernestoa.lizano@gmail.com
2do. Nivel de Contacto	Carlos Zelaya
Empresa	JM TELCOM
Software	FortiMAIL
Fijo	2246-6065
Cel.	(503)7910-7759
3er. Nivel de Contacto	Jorge Guevara
Fijo	(503) 2590-5432
Cel.	(503) 7070-6266
e-mail	jorge.guevara@minec.gob.sv

5.7. Fallo en plataforma de entrega de subsidio al GLP

La plataforma de entrega del subsidio al GLP permite que los beneficiarios se acerquen a un punto autorizado de venta de cilindros de GLP, presenten su Tarjeta Solidaria y se les descuenta el subsidio del precio de mercado, el beneficiario únicamente debe pagar la diferencia. Con este sistema se busca destinar el subsidio a la compra del gas, apoyando a las familias salvadoreñas que más lo necesitan; y racionalizar el gasto del subsidio, mediante un nuevo mecanismo que permite sostenibilidad financiera.

Plan de acción

En caso de reportes sobre fallas del sistema o que los beneficiarios no pueden cobrar su subsidio, se debe llamar al centro de llamadas al (503) 2565-5555.

Contactos para el reporte de fallas

Área técnica	
1er. Nivel de Contacto	Mario Hernández
Cel.	(503)7070-6260
e-mail	mario.hernandez@minec.gob.sv
2do. Nivel de Contacto	Marvin Melara
Fijo	(503) 2590-5435
Cel.	(503) 7070-6140
e-mail	marvin.melara@minec.gob.sv
3er. Nivel de Contacto	Jorge Guevara
Fijo	(503) 2590-5432
Cel.	(503) 7070-6266
e-mail	jorge.guevara@minec.gob.sv

5.8. Fallo en suministro eléctrico de Centro de Datos

El ministerio de Economía cuenta con un Centro de Datos el cual contiene todos los servidores y dispositivos de comunicación que permiten brindar servicios a Instituciones, usuarios y público en general. Este debe mantenerse en condiciones eléctricas óptimas para su correcto funcionamiento y evitar interrupciones o daños en los equipos.

Plan de acción

El Ministerio cuenta con 2 UPS en clúster de 30KVA cada uno que permiten un tiempo de respaldo de 3 horas, además 4 UPS de 20 KVA en clúster que permiten 3 horas de autonomía en caso de corte eléctrico. Paralelo a esto el Ministerio de Economía cuenta con una planta eléctrica de 500KVA. Al presentarse fallas en el suministro eléctrico, se han configurado alertas desde los UPS, enviando mensajes a los equipos móviles de los encargados de la red y Centro de Datos

sobre las interrupciones y el estado de los equipos, permitiendo monitorear en tiempo real su funcionamiento.

La planta de eléctrica de emergencia está programada para entrar en funcionamiento de forma automática ante la falla del suministro eléctrico. En caso que esto no ocurriera y que además sucediera en hora no hábiles, el supervisor de turno de vigilantes deberá contactar al coordinador de seguridad del Ministerio de Economía quien a su vez contactara al Jefe del departamento de Mantenimiento y al Gerente de Informática.

Tiempo estimado de ejecución

Los UPS se encuentran conectados directamente al Centro de Datos por lo tanto son los encargados de regular la energía que entra a los equipos y gracias a la autonomía permitida por estos, garantizan un suministro contante ya que la planta eléctrica entra en funcionamiento 30 segundos después de un corte eléctrico, protegiendo así los equipos del Centro de Datos.

Contactos para el reporte de fallas

PLANTA DE EMERGENCIA	
1er. Nivel de Contacto	Alex Lemus Jefe de Soporte y de Infraestructura
Cel.	(503)7070-6030
2do. Nivel de Contacto	Mirna Fuentes Jefe de Mantenimiento
Cel.	(503)7070-6240
2do. Nivel de Contacto	NOC GBM
Tel.	(503) 2505-9600

5.9. Fallo en sistema de enfriamiento Data Center

El ministerio de Economía cuenta con un Centro de Datos el cual contiene todos los servidores y dispositivos de comunicación que permiten brindar servicios a Instituciones, usuarios y público en general. Este debe mantenerse en condiciones ambientales óptimas para su correcto funcionamiento y evitar altas temperaturas que provoquen daños en los equipos.

Plan de acción

El Ministerio de Economía posee 2 aires acondicionados de precisión configurados en fail over para garantizar el enfriamiento adecuado, además un sistema de alertas de estado permite monitorear las fallas que pueden surgir.

Contactos para el reporte de fallas

PLANTA DE EMERGENCIA	
1er. Nivel de Contacto	Alex Lemus Jefe de Soporte y de Infraestructura
Cel.	(503)7070-6030
2do. Nivel de Contacto	Mirna Fuentes Jefe de Mantenimiento
Cel.	(503)7070-6240
2do. Nivel de Contacto	Kevin Aldair Mejía Grupo Electrotécnica
Cel.	(503)7861-0381

6. Responsabilidades

Para el desarrollo e implementación de este plan de contingencia, se ha diseñado la siguiente estructura, definiendo las responsabilidades:

Líder del Proyecto	Director de Tecnologías de Información y Telecomunicaciones
Administrador del Proyecto	Gerente de Seguridad Informática y Telecomunicaciones Gerente de Informática
Equipo de trabajo	Jefe de la unidad de Seguridad y Soporte Técnico Informático Jefe de la unidad de Desarrollo de Sistemas

Líder del Proyecto

a) Dirigir el desarrollo integral del Plan de Contingencia, así como verificar el cumplimiento de las actividades encargadas a cada uno de los participantes.

Administrador del Proyecto

a) Desarrollar el Plan de Contingencia establecido.

b) Asignar los responsables, así como las prioridades para el desarrollo de las tareas.

c) Organizar el proyecto y orientar al equipo de trabajo.

d) Establecer coordinación entre el equipo de trabajo y el Líder del Proyecto.

e) Verificar y efectuar el seguimiento para el plan de contingencia.

f) Identificar los problemas, desarrollar las soluciones y recomendar aquellas acciones específicas.

g) Informar al líder del Proyecto, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

Equipo de trabajo

f) Identificar los problemas, desarrollar las soluciones y recomendar aquellas acciones específicas.

g) Informar al líder del Proyecto, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

Equipo de trabajo

a) Ejecutar las acciones especificadas en el Plan de Contingencia.

b) Comunicar oportunamente al Administrador del Proyecto, sobre la realización de las tareas asignadas, así como dificultades encontradas y la identificación de los riesgos,

c) Identificar e informar sobre aspectos operativos no contemplados.

d) Ejecutar acciones correctivas, coordinando con el Administrador del Proyecto.

7. Control de Cambios

Versión	Fecha de la Versión	Descripción de la modificación
2.0	Julio de 2020	Se ha revisado y actualizado la información técnica referente a los planes de acción a realizar para las contingencias, junto con los contactos a quien reportar las fallas

Responsable de la elaboración:	Responsable de la revisión:	Aprobó:
Fredy Alexander Lemus Jefe de División de Soporte Técnico e Infraestructura **Apoyo Técnico:** **Eduardo Elías Barahona** Técnico de Planificación y Desarrollo Institucional	**Nelson Armando Muñoz** Dirección de Tecnologías de la Información **Arlen Tatiana Gámez Mejía** Dirección de Planificación y Desarrollo Institucional	 **María Luisa Hayem Brevé** Ministra de Economía