MINISTERIO DE ECONOMÍA

# PLAN DE CONTINGENCIA INFORMÁTICO

# TABLA DE CONTENIDO

## 1. PRESENTACIÓN

El Plan de Contingencia Informático del Ministerio de Economía contiene el establecimiento del objetivo de este tipo de documento, las definiciones o terminología empleada y la organización administrativa que soporta su ejecución. Incluye además la metodología utilizada para la identificación de escenarios y las fichas técnicas para cada escenario.

La metodología adoptada aborda la cuantificación del grado de peligrosidad de los escenarios de riesgo a considerar, en base a la evaluación de: a) el nivel de severidad de las consecuencias y b) la frecuencia de la exposición de que ocurra el riesgo.

Para cada uno de los escenarios de riesgo identificados se ha preparado una Ficha Técnica, la cual contiene la Infraestructura Tecnológica actual, la Acción de Contingencia que permitirá mantener la operatividad frente al escenario de riesgo y que minimizará la gravedad de las consecuencias negativas sobre el Ministerio de Economía; lo cual se refleja en el tiempo estimado de ejecución de la Acción de Contingencia. Asimismo, se ha incluido el detalle del personal de contacto para el reporte de fallas, comprendiendo tanto personal interno como externo.

## 2. OBJETIVO

Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por fenómenos naturales o humanos; mediante el establecimiento de un plan de acción, formación de equipos y entrenamiento para restablecer la operatividad de los sistemas en el menor tiempo posible.

## 3. DEFINICIONES Y TERMINOLOGÍA

**Contingencia**

Posibilidad o riesgo que suceda un evento o situación de emergencia que amenace la operatividad de los sistemas de una Institución.

**Plan de Contingencia Informático**

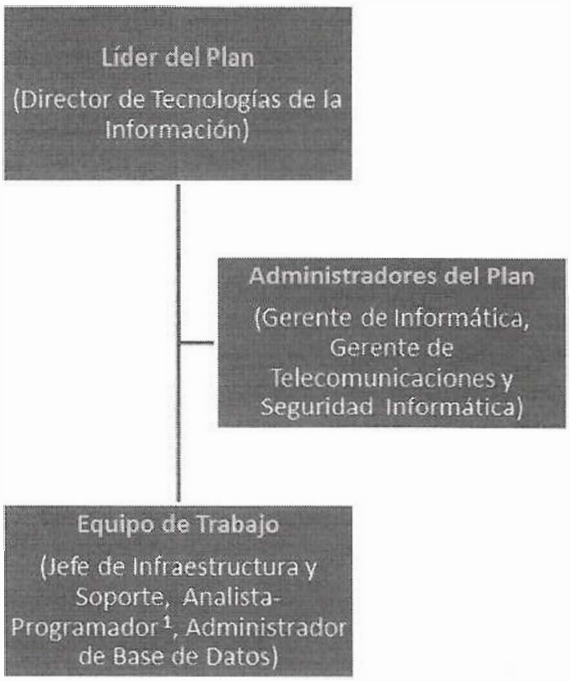
Tipo de plan preventivo y reactivo que presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.

## 4. ORGANIZACIÓN ADMINISTRATIVA DEL PLAN DE CONTINGENCIA

El diseño de un Plan de Contingencia Informático involucra el establecimiento de un grupo responsable para su elaboración, validación y mantenimiento.

### 4.1. Organización administrativa

Se propone la siguiente organización:




### 4.2. Funciones y roles de la Organización Administrativa

4.2.1. Líder del Plan:

- Dirigir el desarrollo integral del Plan de Contingencia Informático.
- Verificar el cumplimiento de las actividades encargadas a cada uno de los participantes.

4.2.2. Administradores del Plan:

- Desarrollar el Plan de Contingencia Informático establecido.
- Asignar los responsables, así como las prioridades para el desarrollo de las tareas.
- Organizar y orientar al Equipo de trabajo.
- Establecer la coordinación entre el Equipo de trabajo y el Líder del Plan.
- Verificar y efectuar el seguimiento del Plan de Contingencia Informático.
- Identificar los problemas, desarrollar las soluciones y recomendar aquellas acciones específicas.

---

[1] La persona que desempeña este cargo realiza funciones de Jefe de Desarrollo de Sistemas en la práctica; sin embargo, debido a la Política de Ahorro y de Eficiencia en el Gasto del Sector Público 2017, no ha sido posible solicitar una reclasificación de esta plaza ante el Ministerio de Hacienda.

- Informar al Líder del Plan, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

4.2.3. Equipo de trabajo

- Ejecutar las acciones especificadas en el Plan de Contingencia Informático.
- Comunicar oportunamente a los Administradores del Plan, sobre la realización de las tareas asignadas, así como dificultades encontradas y la identificación de los riesgos.
- Identificar e informar sobre aspectos operativos no contemplados.
- Ejecutar acciones correctivas, coordinando con los Administradores del Plan.

## 5. METODOLOGÍA

Para la identificación de escenarios de riesgos en el Plan de Contingencia Informático se aplicará una adaptación de la metodología de Análisis del Riesgo FINE[2], en la cual se calcula el grado de peligrosidad de cada escenario de riesgo mediante la fórmula siguiente:

$$Grado\ de\ Peligrosidad\ (GP)\ o\ Magnitud\ del\ Riesgo = Consecuencia\ (C)\ x\ Exposición\ (E)$$

En donde:

**Consecuencia:** Son los resultados más probables de un escenario debido al riesgo que se considera, incluyendo daños materiales y humanos. Este concepto está relacionado con la gravedad.

| Grado de severidad de las Consecuencias | Valor |
|---|---|
| Catastrófica (Daños desde US$ 500,000.01 hasta quebranto de la actividad) | 100 |
| Desastrosa (Daños desde US$ 250,000.01 a US$ 500,000.00) | 40 |
| Muy Seria (Daños desde US$ 50,000.01 a US$ 250,000.00) | 15 |
| Seria (Daños desde US$ 500.01 a US$ 50,000.00) | 7 |
| Importante (Daños desde US$ 50.01 a US$ 500.00) | 3 |
| Leve (Daños hasta US$ 50.00) | 1 |

**Exposición:** La frecuencia con que se presente el escenario de riesgo.

| Frecuencia de la Exposición | Valor |
|---|---|
| Continua (Se presenta muchas veces al día) | 10 |
| Frecuente (Se presenta aproximadamente una vez al día) | 6 |
| Ocasional (Se presenta semanalmente) | 3 |
| Poco Usual (Se presenta mensualmente) | 2 |
| Rara (Se presenta unas pocas veces al año) | 1 |
| Muy Rara (Se presenta anualmente) | 0.5 |
| Inexistente (No se presenta nunca) | 0 |

[2] Establecida por Williams T. Fine en el documento "Evaluación matemática para el Control de Riesgo".

## 6. ESCENARIOS DE RIESGO

La priorización de los escenarios de riesgos a abordar en el presente Plan de Contingencia Informático se efectuará aplicando la metodología descrita en el numeral anterior, y se presenta a continuación:

| Escenario de Riesgo | Consecuencia (C) | Exposición (E) | Grado de Peligrosidad (GP) |
|---|---|---|---|
| Escenario 1: Fallo en suministro eléctrico en Centro de Datos | 40 | 1 | 40 |
| Escenario 2: Fallo en sistema de enfriamiento del Centro de Datos | 40 | 1 | 40 |
| Escenario 3: Perdida de enlace de comunicación (Internet) | 7 | 1 | 7 |
| Escenario 4: Fallo de Servidores de bases de datos SQL Server y Oracle | 7 | 1 | 7 |
| Escenario 5: Fallo de Firewall Central | 7 | 0.5 | 3.5 |
| Escenario 6: Fallo de Controlador de Dominio | 7 | 0.5 | 3.5 |

# 7. FICHAS TÉCNICAS DE ESCENARIOS DE RIESGO

## 7.1. Ficha Técnica de Escenario 1: Fallo en suministro eléctrico en Centro de Datos

| **Escenario:** | Fallo en suministro eléctrico en Centro de Datos |
|---|---|

**Infraestructura Tecnológica:**
Se cuenta con un Centro de Datos el cual contiene todos los Servidores y dispositivos de comunicación que permiten brindar servicios a usuarios, público en general e Instituciones. Este debe mantenerse en condiciones eléctricas óptimas para su correcto funcionamiento y evitar interrupciones o daños en los equipos.

**Acción de Contingencia:**
En caso de fallo en el controlador de dominio, se ha instalado una réplica del controlador principal, llamado vsrv-dc2, 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 vsrv-dc1. Esto permitirá la recuperación del servidor principal sin que afecte a los usuarios del dominio.

**Tiempo estimado de ejecución de la Acción de Contingencia:**
Ambos equipos se encuentran funcionando, y el servidor vsrv-dc2 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 3 horas, lo cual no afectaría a los usuarios porque estaría funcionando el controlador secundario.

| **Contactos para el reporte de fallas-Planta de Emergencia[3]:** | |
|---|---|
| **Personal interno** | |
| 1er Nivel de Contacto: | Sr. Miguel Quintanilla |
| Teléfono: | (503) 2590-5694 |
| Celular: | (503) 7070-6048 |
| 2° Nivel de Contacto: | Ing. Leonel Jiménez |
| Teléfono: | (503) 2590-5530 |
| Celular: | (503) 7070-6000 |

| **Contactos para el reporte de fallas-Cuarto de Potencia[2]:** | | | |
|---|---|---|---|
| **Personal interno** | | **Personal externo** | |
| Contacto: | Ing. Leonel Jiménez | Contacto: | GBM |
| Teléfono: | (503) 2590-5530 | Teléfono: | (503) 2268-6600 |
| Celular: | (503) 7070-6000 | | |

[3] Para acceder al área de la Planta de Emergencia y el Cuarto de Potencia, se deberá gestionar el ingreso respectivo con el Coordinador de Seguridad del Ministerio de Economía.

## 7.2. Ficha Técnica de Escenario 2: Fallo en sistema de enfriamiento del Centro de Datos

| **Escenario:** | Fallo en sistema de enfriamiento del Centro de Datos | | |
|---|---|---|---|
| **Infraestructura Tecnológica:**<br>Se cuenta con un Centro de Datos el cual contiene todos los Servidores y dispositivos de comunicación que permiten brindar servicios a usuarios, público en general e Instituciones. Este debe mantenerse en condiciones de enfriamiento óptimas para su correcto funcionamiento y evitar interrupciones o daños en los equipos. | | | |
| **Acción de Contingencia:**<br>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. | | | |
| **Tiempo estimado de ejecución de la Acción de Contingencia:**<br>Basado en pruebas realizadas, el tiempo que tarda en activarse el aire acondicionado redundante al detectarse la falla del aire acondicionado primario es de menos de 1 minuto. | | | |
| **Contactos para el reporte de fallas:** | | | |
| **Personal interno** | | **Personal externo** | |
| Contacto: | Ing. Leonel Jiménez | Contacto: | Electrotecnia |
| Teléfono: | (503) 2590-5530 | Teléfono: | (503) 2529-3130 |
| Celular: | (503) 7070-6000 | | |

### 7.3. Ficha Técnica de Escenario 3: Perdida de enlace de comunicación (Internet)

| **Escenario:** | Perdida de enlace de comunicación (Internet) |
|---|---|

**Infraestructura Tecnológica:**

Se cuenta con un enlace de comunicaciones de internet de 50Mb, el cual es utilizado para publicar servicios que el MINEC brinda a usuarios, público en general y a otras entidades; entre los cuales podemos mencionar sitios web, correo electrónico, VPN, consultas GLP, consultas de Hidrocarburos y Minas. Además se utiliza para brindar servicio de internet a los usuarios internos ubicados en MINEC como en la Dirección General de Estadísticas y Censos, Consejo Nacional de Calidad, CENADE y CIM.

**Acción de Contingencia:**

En caso de fallar el enlace principal, se ha contratado un enlace secundario de 8Mb 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 de la Acción de Contingencia**:

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-Enlace Principal:**

| **Personal interno** | | **Personal externo** | |
|---|---|---|---|
| 1er Nivel de Contacto: | Ing. Mario Pastori | 1er Nivel de Contacto: | Centro de Operaciones de la Red (NOC) IBW |
| Teléfono: | (503) 2590-5522 | Teléfono: | (503) 2529-4800 |
| Celular: | (503) 7070-6030 | E-Mail: | callcentersv@ibw.com y nocsv@ibw.com |
| 2° Nivel de Contacto: | Lic. Ericka Chacón | 2° Nivel de Contacto: | Alan Pérez (Gerente de NOC) |
| Teléfono: | (503) 2590-5638 | Teléfono: | (503) 2278-5068 |
| Celular: | (503) 7070-6162 | Celular: | (503) 6200-1058 |
| Email: | ericka.chacon@minec.gob.sv | Email: | |
| 3er Nivel de Contacto: | Ing. Orlando Arbaiza | 3er Nivel de Contacto: | Miguel Franco (Gerente de la Cuenta) |
| Teléfono: | (503) 2590-5519 | Teléfono: | (503) 2278-5068 |
| Celular: | (503) 7070-6305 | Celular: | (503) 7874-1085 |
| Email: | oarbaiza@minec.gob.sv | Email: | |

| Contactos para el reporte de fallas-Enlace Secundario: | | | |
|---|---|---|---|
| **Personal interno** | | **Personal externo** | |
| 1er Nivel de Contacto: | Ing. Mario Pastori | 1er Nivel de Contacto: | Centro de Operaciones de la Red (NOC) TELECOMODA |
| Teléfono: | (503) 2590-5522 | Teléfono: | (503) 2250-3333 |
| Celular: | (503) 7070-6030 | E-Mail: | clientescorporativos@claro.com.sv |
| 2° Nivel de Contacto: | Lic. Ericka Chacón | 2° Nivel de Contacto: | Rafael Enrique León (Ejecutivo de Servicio asignado) |
| Teléfono: | (503) 2590-5638 | Teléfono: | (503) 2271-7469 |
| Celular: | (503) 7070-6162 | Celular: | (503) 7868-4047 |
| Email: | ericka.chacon@minec.gob.sv | Email: | leon.rafael@claro.com.sv |
| 3er Nivel de Contacto: | Ing. Orlando Arbaiza | 3er Nivel de Contacto: | Nassaretth Mariona (Ejecutivo de Ventas asignado) |
| Teléfono: | (503) 2590-5519 | Teléfono: | (503) 2271-7335 |
| Celular: | (503) 7070-6305 | Celular: | (503) 7740-0067 |
| Email: | oarbaiza@minec.gob.sv | Email: | mariona.nassaretth@claro.com.sv |

## 7.4. Ficha Técnica de Escenario 4: Fallo de Servidores de bases de datos SQL Server y Oracle

| **Escenario:** | Fallo de Servidores de bases de datos SQL Server y Oracle | | |
|---|---|---|---|
| **Infraestructura Tecnológica:**<br>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 constituye un incidente crítico de seguridad. | | | |
| **Acción de Contingencia:**<br>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 de la Acción de Contingencia:**<br>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. | | | |
| **Contactos para el reporte de fallas:** | | | |
| **Personal interno** | | **Personal externo (Bases de datos Oracle)** | |
| 1er Nivel de Contacto: | Ing. Ernesto Lizano | Contacto: | Syntepro |
| Teléfono: | (503) 2590-5521 | Teléfono: | (503) 2223-4809 |
| Celular: | (503) 7070-6031 | | |
| E-Mail: | elizano@minec.gob.sv | | |
| 2° Nivel de Contacto: | Ing. Jorge Guevara | | |
| Teléfono: | (503) 2590-5432 | | |
| Celular: | (503) | | |
| E-Mail: | jorge.guevara@minec.gob.sv | | |

## 7.5. Ficha Técnica de Escenario 5: Fallo de Firewall Central

| **Escenario:** | Fallo de Firewall Central | | |
|---|---|---|---|
| **Infraestructura Tecnológica:**<br>Se utiliza un Firewall Fortinet 1240B 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, IPS-IDS, DDOS, SSL.<br>Todas las rutas a sitios remotos están configuradas en este equipo, por lo tanto es crítico que este se mantenga en funcionamiento 24/7. | | | |
| **Acción de Contingencia:**<br>Para realizar mantenimientos o en caso de fallo, se cuenta con otro equipo de iguales características (Fortigate 1240B) 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 de la Acción de Contingencia:**<br>Se ha configurado un esquema en clúster, 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 al lapso de 1 minuto. | | | |
| **Contactos para el reporte de fallas:** | | | |
| **Personal interno** | | **Personal externo** | |
| 1er Nivel de Contacto: | Ing. Mario Pastori | 1er Nivel de Contacto: | Técnicos (Contacto de Emergencias) |
| Teléfono: | (503) 2590-5522 | Teléfono: | (503) 2246-6005 |
| Celular: | (503) 7070-6030 | Celular: | (503) 7910-7529 |
| 2° Nivel de Contacto: | Lic. Ericka Chacón | 2° Nivel de Contacto: | Sra. Morena Castro (Área Técnica) |
| Teléfono: | (503) 2590-5638 | Teléfono: | (503) 2246-6065 |
| Celular: | (503) 7070-6162 | | |
| Email: | ericka.chacon@minec.gob.sv | Email: | morena.castro@jmtelcom.com.sv |
| 3er Nivel de Contacto: | Ing. Orlando Arbaiza | | |
| Teléfono: | (503) 2590-5519 | | |
| Celular: | (503) 7070-6305 | | |
| Email: | oarbaiza@minec.gob.sv | | |

## 7.6. Ficha Técnica de Escenario 6: Fallo de Controlador de Dominio

| **Escenario:** | Fallo de Controlador de Dominio |
|---|---|
| **Infraestructura Tecnológica:**<br>Los servicios de directorio se ejecutan en el servidor llamado vsrv-dc1, 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 es crítico, ya que no permitiría el inicio de sesión a los usuarios perdiendo el acceso a sus configuraciones y trabajos. | |
| **Acción de Contingencia:**<br>En caso de fallo en el controlador de dominio, se ha instalado una réplica del controlador principal, llamado vsrv-dc2, 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 vsrv-dc1. Esto permitirá la recuperación del servidor principal sin que afecte a los usuarios del dominio. | |
| **Tiempo estimado de ejecución de la Acción de Contingencia:**<br>Ambos equipos se encuentran funcionando, y el servidor vsrv-dc2 tomará el rol de maestro cuando no se encuentre en la red al controlador primario.<br>Si el controlador primario sufriera algún daño de hardware, se estima que la reinstalación tomaría 3 horas, lo cual no afectaría a los usuarios porque estaría funcionando el controlador secundario. | |
| **Contactos para el reporte de fallas:** | |
| **Personal interno** | |
| 1er Nivel de Contacto: | Ing. Mario Pastori |
| Teléfono: | (503) 2590-5522 |
| Celular: | (503) 7070-6030 |
| E-Mail: | mpastori@minec.gob.sv |
| 2° Nivel de Contacto: | Lic. Ericka Chacón |
| Teléfono: | (503) 2590-5638 |
| Celular: | (503) 7070-6162 |
| Email: | ericka.chacon@minec.gob.sv |

## 8. CONTROL DE CAMBIOS

| VERSIÓN | FECHA DE LA VERSIÓN | DESCRIPCIÓN DE MODIFICACIÓN |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| Responsables de la elaboración: | Responsables de la revisión: | Aprobó: |
|---|---|---|
| Mario Pastori<br>Jefe de Infraestructura y Soporte-DTI | Leonel Antonio Jiménez<br>Gerente de Informática-DTI | |
| Rafael Ernesto Vaquerano<br>Técnico de Desarrollo Institucional-GPDI | Orlando Ernesto Arbaiza<br>Gerente de Telecomunicaciones y Seguridad Informática-DTI | Mario Hernández Rodríguez<br>Director de Tecnologías de la Información-DTI |

**REF: GPDI-061-05-2017**

**MEMORÁNDUM**

PARA: Mario Hernández Rodríguez
Director de Tecnologías de la Información

DE: Bertha Figueroa de Castillo
Gerente de Planificación y Desarrollo Institucional

MINISTERIO DE ECONOMIA
GERENCIA DE PLANIFICACION Y DESARROLLO INSTITUCIONAL
SAN SALVADOR

ASUNTO: Remisión del documento "Plan de Contingencia Informático" (Versión 1.0)

FECHA: 23 de mayo de 2017

---

De la manera más cordial, le remito el documento "Plan de Contingencia Informático" (Versión 1.0), para su consideración y efectos pertinentes.

Sin otro particular, aprovecho la oportunidad para saludarle y expresarle mis más sinceras muestras de consideración y estima.

Atentamente,