1 Objetivo General

Garantizar la capacidad de respuesta y la continuidad de los servicios esenciales del Ministerio de Desarrollo Social para proteger y asistir a la población más vulnerable durante y después de los desastres naturales y eventos adversos.

Este objetivo general busca asegurar que el Ministerio esté preparado para enfrentar situaciones de emergencia, minimizando el impacto en las comunidades y programas de atención social. Se busca establecer mecanismos efectivos de coordinación, asignación de roles y responsabilidades, así como la identificación de recursos necesarios para mantener la operatividad de los servicios críticos del Ministerio en momentos de crisis.

El objetivo del documento incluye la implementación de medidas de mitigación y acciones preventivas para reducir el riesgo de desastres en las áreas de intervención del Ministerio. También guardar la capacidad del Ministerio para brindar asistencia y protección a las personas más necesitadas en situaciones de desastre, a través de la coordinación oportuna y efectiva, con el propósito de garantizar continuidad de los servicios esenciales.

2 Objetivos Específicos

- Identificar y clasificar los servicios y programas del Ministerio según su criticidad y complejidad para brindar apoyo a la población más vulnerable durante situaciones de desastre.
- Priorizar los servicios que presta la Subdirección de Infraestructura Tecnológica para asegurar su continuidad y asignar los recursos necesarios para su funcionamiento en condiciones adversas.
- Establecer los niveles de complejidad de las fallas del sistema y los posibles tiempos de no disponibilidad de los diferentes sistemas.

3 Antecedentes

El Ministerio de Desarrollo Social pone a disposición de la población guatemalteca diferentes programas orientados a mejorar el nivel de bienestar de las personas y grupos sociales vulnerables, que sufren y viven en situación de pobreza y pobreza extrema.

De acuerdo al Manual de Procedimientos de la Dirección de Informática en su Título VI- Plan de Contingencia Tecnológica Capítulo I- Alcance y Contenido del Plan de Contingencia. La Dirección de Informática debe asegurar la existencia de un plan

de contingencias tecnológicas aprobado, formalizado, actualizado, implementado y probado.

4 Metodología empleada para su Diseño

El ciclo de funcionamiento del modelo de operación de continuidad del negocio y su funcionamiento dentro del modelo de operación seguridad y privacidad de la información y la descripción detallada de cada una de las fases. Las cuatro (4) fases que comprenden el modelo de operación contienen objetivos, metas y herramientas que permiten que la continuidad del negocio sea un sistema de sostenible dentro de las entidades: Planificación, Implementación, Gestión y Mejora Continua:

1) **Planificación**: preparación y aprobación de esfuerzos.
2) **Identificación** de riesgos: funciones y flujo del proceso del Ministerio
3) **Identificación de Soluciones**: se evalúa riesgos y fallas o interrupciones
4) **Estrategias**: otras opciones, soluciones alternativas, procedimientos y manuales
5) **Documentación de proceso**: creación de un manual del proceso
6) **Realización de pruebas**: selección de casos soluciones que probablemente funcionen
7) **Implementación**: creación de las soluciones documentación de los casos de monitoreo.
8) **Monitoreo**: probar nuevas soluciones o validar los casos

5 Definición de Desastre

El propósito de definir desastre consiste en tener claridad del concepto durante la etapa de la creación del documento, pero también que sirva para que se tenga claro el concepto durante una interrupción de negocio y conocer si realmente la institución está sufriendo un desastre.

Podemos definir desastre como: Un evento que puede interrumpir procesos críticos de negocio y degradar los servicios asociados al punto resultante de que el impacto operativo e institucional se vuelva inaceptable.

Existen niveles de desastre de acuerdo a su impacto, los cuales se listarán a continuación:

5.1 Nivel menor de desastre

Este tipo de desastre puede ocurrir de forma más frecuente durante el día a día operativo, comparado con un desastre de nivel intermedio y/o mayor. Se considera menor porque los efectos se encuentran normalmente aislados a pequeños procesos críticos de negocio. Las unidades de negocio que dependen de ese proceso, normalmente pueden continuar operando. Muchos de estos problemas son reanudados mediante políticas de la organización y departamentos que controlan los incidentes operativos y técnicos.

5.2 Nivel Intermedio de desastre

Este tipo de desastre puede ocurrir de forma menos frecuente, pero con un mayor impacto que el de nivel menor. Este tipo de evento provoca una interrupción de operaciones normales de las instituciones, pero no de todas las áreas críticas de la empresa.

5.3 Nivel Mayor de desastre

Las posibilidades de que este tipo de desastre ocurra son muy bajas, pero el nivel de impacto de interrupción y daño puede ser muy superior a los niveles medio y menor. Cuando ocurre un evento de este tipo, la operatividad es interrumpida e inaccesible para la mayoría de los procesos críticos definidos del negocio. Un ejemplo puede ser: Terremotos, incendios, sabotaje cibernético.

6 Subdirección de Infraestructura

Responsable de planificar, coordinar y administrar puntos de conexión para la red de información, creación y configuración de buzones de correo electrónico, inventario de instalación de puntos de conexión de internet, implementación de políticas de back up y respaldo de información de las bases de datos, y la administración de los sistemas de información SICOIN, GUATE-NOMINAS, SIGES, todo esto de acuerdo a las políticas, normas y procedimientos establecidos.

En la siguiente matriz se identifican activos críticos y las acciones relacionadas a la recuperación de caso de ocurrencia de un desastre:

ACTIVO	ACCIONES A REALIZAR EN CASO DE UN DESASTRE	CLASIFICACIÓN	PRIORIDAD DE ATENCIÓN
Core Switch y Distribution Switch	En la actualidad, los Distribution Switches enfrentan la vulnerabilidad de estar accesibles a los usuarios, lo que incrementa el riesgo de daños físicos. Con el fin de mitigar este riesgo, se está realizando la transición hacia gabinetes con cerradura. En caso de que se produzca algún daño físico al dispositivo, se requiere la generación de una orden de compra para su recuperación y garantizar la continuidad del negocio. Es importante señalar que estos equipos carecen de garantía y no cuentan con contratos de mantenimiento proporcionados por los proveedores. No obstante, se han implementado respaldos de las configuraciones para posibilitar la restauración de la información técnica y la documentación necesaria.	Crítica	1
Firewall	En el caso de un daño físico el equipo no proporciona continuidad del servicio con alta disponibilidad, es necesario realizar el cambio del equipo completamente. En el caso de pérdida de configuración, se realiza una copia de seguridad cuando existan cambios significativos dentro de la configuración, la cual se puede recuperar y configurar el equipo nuevamente.	Crítica	1

Servidor de Active Directory Servidor de Antivirus Servidor de BDD Servidor de aplicaciones (dos) Servidor de impresión Servidores de servicios críticos a mapear Enclusoure (4 servidores, ambiente de virtualización)	Se cuenta con un cluster de servidores donde se encuentran alojados todos los servidores. En caso de que alguna máquina virtual se infecte con un virus, el proceso de recuperación consiste en aislar la máquina virtual afectada y restaurarla utilizando el respaldo del que disponemos. Solo los servidores considerados críticos cuentan con copias de respaldo frecuentes (en este caso, todos los mencionados). Se cuenta con un datacenter (Barracuda) donde se realizan los respaldos en la nube. Esta herramienta es capaz de levantar la máquina virtual en la nube o descargar el respaldo para instalarlo localmente (esto puede llevar más tiempo). La frecuencia de los respaldos depende del servidor en particular. Por ejemplo, los servidores de Active Directory y las aplicaciones se respaldan tres veces por semana.	Crítica	1
Servicios de DNS (nube)	Se dispone de una Red de Entrega de Contenido (CDN) donde se generan los registros de las direcciones IP públicas del ministerio. El proveedor brinda soporte en la gestión de este servicio, y está integrado dentro del servidor de Active Directory. CONTACTO Devel security soporte@develsecurity.com Nelson Leonel Ruiz Diaz	Crítica	1
Internet (principal y redundante)	Los proveedores actuales, GUATEL e INNOVA, son responsables de brindar servicios de enlaces, proveedores de servicios de internet (ISP), así como realizar revisiones de configuraciones y conexiones.	Crítica	1
Enlaces de Datos (Finanzas, Bodega)	La comunicación se lleva a cabo a través de los enlaces contratados, y generalmente los proveedores se encargan de gestionar dichos enlaces. Se administran los puntos finales de entrada y salida.	Alta	2
Wifi	En caso de que un dispositivo sufra un daño físico, no es posible garantizar la continuidad del negocio en ese punto, ya que no se cuenta con dispositivos similares almacenados en inventario.	Alta	2

	Se debe realizar una orden de compra para gestionar y continuar con los servicios.		
SAN (san switch) NAS	Se realiza backup de la información, sin embargo, no se cuenta con un balanceador de carga para poder ofrecer continuidad del negocio.	Crítica	1
BARRACUDA (seguridad) BARRACUDA (backup, 2 equipos)	Para el servicio de Barracuda como se menciona anteriormente se posee acceso por medio de credenciales y en él se almacenan copias de seguridad de los servidores, el alcance del servicio abarca la seguridad y la continuidad de operaciones.	Alta	2
UPS Datacenter	En caso de daño físico se debe de reemplazar el dispositivo, se asegura la continuidad del negocio al activar la planta eléctrica automáticamente con un rango de 3 días de disponibilidad, aproximadamente, sin embargo, los UPS se deben reemplazar. Actualmente poseen acceso ciertos usuarios de la subdirección de infraestructura: José Alejandro Ramírez (tarjeta de acceso) Rene Bernal Mazariegos (biométrico) José Fernando Obando (biométrico) Dany Estuardo Jiménez (biométrico)	Crítica	1
Servicedesk	Para estos servicios se realizan copias de seguridad con una frecuencia específica dentro de los servidores y la nube de Barracuda.	Alta	2
Correo Electronico		Alta	2

Equipo de respuesta

Avería o falla	Contacto 1	Email	Contacto 2	Email
Base de datos	Rogelio Alvarez	ralvarez@mides.gob.gt	Jose Manuel Gonzalez	josemanuel.gonzalez@mides.gob.gt
Servidores	René Mazariegos	rbmazariegos@mides.gob.gt	Dany Jimenez	Dany.jimenez@mides.gob.gt
Red de datos	Jose Obando	jobando@mides.gob.gt	Alejandro Ramirez	jramirez@mides.gob.gt
Enlaces de internet	Alejandro Ramirez	jramirez@mides.gob.gt	Jose Obando	jobando@mides.gob.gt

Medidas Preventivas:

Monitoreo constante de la disponibilidad y el rendimiento del servicio por medio de la herramienta PRTG y SnapShot del Servidor Virtual donde está instalado el Sistema de Mesa de Ayuda, administrado por el personal de la Subdirección de Infraestructura Tecnológica de la Dirección de Informática.

Incidentes

Riesgo o Incidente	Probabilidad de Ocurrencia	Impacto en el Servicio	Prioridad	Consecuencias
Falla de todos los servicios en la granja de Servidores	Baja	Alto	Alta	Imposibilidad de acceso al sistema mesa de ayuda y generar ticket para solicitar ayuda

Perdida del Servidor donde está instalada la herramienta	Baja	Alta	Alta	Baja total del servicio.