MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES		
CÓDIGO: PRCSTIC.001	**VERSIÓN:** 1.00	**PÁGINA:** 61
OFICINA GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN		

PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

ELABORADO POR:	Sara Haydee Mostajo Rojas Eder Miguel Soto Barboza Henderson Enriquez Huilca
REVISADO POR:	Miguel Gumercindo Lovaton Anticona Director General de la Oficina General de Tecnologías de la Información
APROBADO POR	Miguel Gumercindo Lovaton Anticona Director General de la Oficina General de Tecnologías de la Información

Firmado digitalmente por LOVATON ANTICONA Miguel Angel Gumercindo FAU 20336951527 soft
Motivo: Doy V° B°
Fecha: 28.11.2024 11:08:03 -05:00

Historial del Documento

Fecha de elaboración /revisión	Versión	Elaborado/ Revisado por	Naturaleza del Cambio
11/11/2024	V.1.0	Sara Haydee Mostajo Rojas / Eder Miguel Soto Barboza / Henderson Enriquez Huilca	Formulación del Plan
26/11/2024	V.1.0	Miguel Angel Gumercindo Anticona	Aprobación del Plan

ÍNDICE

I. INTRODUCCIÓN **4**
II. OBJETIVO **5**
2.1. Objetivo general 5
2.2. Objetivos específicos 5
III. FINALIDAD **5**
IV. ALCANCE **5**
V. BASE LEGAL **6**
VI. GLOSARIO DE TÉRMINOS **7**
VII. DISPOSICIONES GENERALES **9**
7.1. Del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables 9
VIII.Metodología de trabajo ¡Error! Marcador no definido.
8.1. Fase 1: Organización 9
8.2. Fase 2: Determinación de vulnerabilidades y escenarios de contingencia 16
8.3. Fase 3: Estrategias del Plan 21
8.4. Fase 4: Elaboración del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables 24
8.5. Fase 5: Definición y ejecución del Plan de Pruebas 25
8.6. Fase 6: Implementación del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables 26
8.7. Fase 7: Monitoreo 26
IX. DISPOSICIONES COMPLEMENTARIAS **26**
X. ANEXOS **27**

I. INTRODUCCIÓN

La Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables; en adelante MIMP, tiene como parte de sus objetivos prioritarios : i) Garantizar los derechos de las mujeres y poblaciones vulnerables (niñas, niños y adolescentes, personas adultas mayores, personas con discapacidad, personas desplazadas, migrantes internos y migrantes internas); y ii) Reducir la desigualdad de género, la discriminación, la violencia y otras desigualdades que afectan a las mujeres y poblaciones vulnerables.

El MIMP, a través de la Oficina General de Tecnologías de la Información (OGTI); en adelante OGTI, propone el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del MIMP como parte del proceso continuo de planificación, prueba e implementación de procesos y procedimientos para la recuperación en caso de un posible evento que pueda afectar la operación de los servicios en el MIMP.

Estas actividades y acciones, tienen como objetivo garantizar la reanudación y continuidad eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones (TIC) en el menor plazo posible y minimizando el impacto posible en todos los servicios y operaciones del MIMP.

El Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables, ha elaborado documentos que permiten la gestión, ejecución, pruebas y mantenimiento, esta disgregación de documentos permite una fácil y ágil operación por los responsables autorizados, ante situaciones de desastres y su respectiva recuperación y continuidad de los mismos.

II. OBJETIVO

2.1. Objetivo general

Establecer las actividades del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento, a fin que su restablecimiento sea en el menor tiempo posible.

2.2. Objetivos específicos

- Precisar 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 causados por siniestros tecnológicos o de índole natural o humanos.
- Establecer los procedimientos que permitan el restablecimiento de todos los servicios de TI en el menor tiempo posible.
- Organizar y coordinar al personal de TI debidamente capacitado para afrontar adecuadamente los eventos adversos que puedan presentarse.

III. FINALIDAD

Garantizar la continuidad de los servicios de tecnologías de la información y comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables, en caso de un posible evento que pueda afectar la operación de los servicios en el MIMP.

IV. ALCANCE

El alcance del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones es de aplicación para la Oficina General de Tecnologías de la Información (OGTI) de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables.

V. BASE LEGAL

5.1. Ley N° 27658, Ley Marco de Modernización del Gestión del Estado y sus modificatorias.
5.2. Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo y Desastres (SINAGERD).
5.3. Ley N° 29733, Ley de Protección de Datos Personales.
5.4. Decreto Legislativo N° 1098, Ley de Organización y Funciones del Ministerio de la Mujer y Poblaciones Vulnerables.
5.5. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
5.6. Decreto Supremo N° 030-2002-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado.
5.7. Decreto Supremo N° 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
5.8. Decreto Supremo N° 018-2017–PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
5.9. Decreto Supremo N° 050-2018-PCM, Decreto Supremo que aprueba la definición de Seguridad Digital en el Ámbito Nacional.
5.10. Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
5.11. Decreto Supremo N° 038-2021-PCM, Decreto Supremo que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
5.12. Resolución Ministerial N° 320-2021-PCM, Aprueban los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno.
5.13. Resolución Ministerial N° 140-2023-MIMP, que aprueba la Directiva N° 001-2023-MIMP, Gestión de Proyectos Normativos en el Ministerio de la Mujer y Poblaciones Vulnerables.
5.14. Resolución Ministerial N° 362-2023-MIMP, que aprueba el Texto Integrado del Reglamento de Organización y Funciones del Ministerio de la Mujer y Poblaciones Vulnerables.
5.15. Resolución Ministerial N° 005-2018-MIMP, aprobar la Directiva "Administración de Recursos Informáticos y de Comunicaciones".
5.16. Resolución Ministerial N° 165-2018/MIMP, que aprueba la “Política de Seguridad de la Información del Ministerio de la Mujer y Poblaciones Vulnerables – MIMP”.
5.17. Resolución Directoral N° 022-2022-INACAL/DN, Uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3era. Edición”.

VI. GLOSARIO DE TÉRMINOS

6.1. **Activo de información:** es cualquier información o sistema relacionado con el tratamiento de la misma, que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

6.2. **Amenaza:** es cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información, a la institución o al sistema.

6.3. **Aplicación:** es un programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.

6.4. **Base de datos:** es el conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios de selección.

6.5. **Centro de datos:** es un centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.

6.6. **Confidencialidad:** es una característica que garantiza que la información es accesible solo para aquellos autorizados a tener acceso.

6.7. **Cortafuego (firewall):** es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.

6.8. **Datos:** son todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.

6.9. **Datos personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

6.10. **Impacto:** es el resultado o efecto de un evento, el impacto de un evento puede ser positivo o negativo sobre los objetivos relacionados del MIMP.

6.11. **Incidente de seguridad:** Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información y datos sensibles del MIMP.

6.12. **Métodos de análisis de riesgos:** son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

6.13. **Probabilidad:** es cuando un evento determinado ocurre en circunstancias del azar.

6.14. **Riesgo:** es la posibilidad que ocurra un evento adverso que afecte el logro de los objetivos del MIMP.

6.15. **Sistemas de información:** es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para cubrir una necesidad o un objetivo.

VII. DISPOSICIONES GENERALES

7.1. Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables

El Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables pretende minimizar las consecuencias en caso de incidente de seguridad, con la finalidad de reanudar las operaciones en el menor tiempo posible de manera eficiente y oportuna.

El Plan se realiza en las siguientes etapas:

ANTES, como un plan de prevención con el objeto de prevenir y mitigar los incidentes.
DURANTE, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
DESPUÉS, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

VIII. METODOLOGÍA DE TRABAJO

Asimismo, el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables se desarrolla con la metodología[1] basada en siete (07) fases:

- **Fase 1**: Organización
- **Fase 2:** Determinación de vulnerabilidades y escenarios de contingencia
- **Fase 3:** Estrategias.
- **Fase 4:** Elaboración del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones.
- **Fase 5:** Planificación y ejecución de las pruebas del plan de recuperación y continuidad de los servicios de Tecnologías de la Información y Comunicaciones.
- **Fase 6:** Implementación del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones.
- **Fase 7:** Monitoreo.

A continuación, se detallan cada una de las fases:

8.1. Fase 1: Organización

De acuerdo con el Texto Integrado del Reglamento de Organización y Funciones del MIMP aprobado con Resolución Ministerial N° 306-2024-MIMP, la Oficina General de Tecnologías de la Información del MIMP depende de la Secretaría General y es el órgano de apoyo responsable

[1] La metodología utilizada es de elaboración propia basada en un enfoque estructurado de gestión de continuidad de negocios (BCM) y recuperación ante desastres (DRP)

del gobierno digital, así como de la planificación, implementación y supervisión de los sistemas de información, la infraestructura tecnológica de redes y comunicaciones y la seguridad de la información en el MIMP, incluyendo a los programas nacionales.

Asimismo, la Oficina General de Tecnologías de la información del MIMP, cuenta con cuatro equipos de trabajo:

i. **Desarrollo y Sistemas de Información (DSI)**.
Son responsables de realizar el análisis, diseño, desarrollo, implementación y mantenimiento de las aplicaciones y sistemas de información, en alineación con las metodologías de desarrollo aprobadas y las políticas de seguridad establecidas. Además, deben garantizar que los sistemas cumplan con los requerimientos funcionales de las unidades de organización del Ministerio de la Mujer y Poblaciones Vulnerables.

ii. **Plataforma de Atención al Usuario (PAU),** Brindan el soporte técnico a los usuarios de los equipos informáticos del Ministerio de la Mujer y Poblaciones Vulnerables, atendiendo incidencias relacionadas con fallas en el hardware, sistemas operativos o problemas ofimáticos garantizando su operatividad; Además, reciben los requerimientos por fallas en aplicaciones y/o sistemas de información.

iii. **Infraestructura Tecnológica (IT)**, Dentro de sus funciones, se encargan de administrar la integridad, confiabilidad, y seguridad en el acceso a los sistemas de información, así como también el acceso a la base de datos institucional. Esto incluye establecer mecanismos de autenticación de los usuarios, así como la auditoría y control de accesos a la base de datos; además de mantener la infraestructura tecnológica necesaria para el cumplimiento de los objetivos del MIMP, también asegurar la disponibilidad de los sistemas y servicios. Asimismo, es el encargado de la administración del Portal Web del Ministerio de la Mujer y Poblaciones Vulnerables, así como del seguimiento de las publicaciones en el portal de transparencia estándar.

iv. **Innovación, Gobierno y Transformación Digital (IGTD),** Dentro de sus funciones, se encarga de formular y proponer estrategias, planes para la gestión de gobierno y transformación digital, y la supervisión de la gestión de activos informáticos a lo largo de su ciclo de vida; el diseño y evaluación de procesos operativos para optimizar funciones usando TI; así como la seguridad de la información, brindar el apoyo técnico para la implementación, operación, seguimiento y mantenimiento del Sistema de Gestión de la Seguridad de la Información.

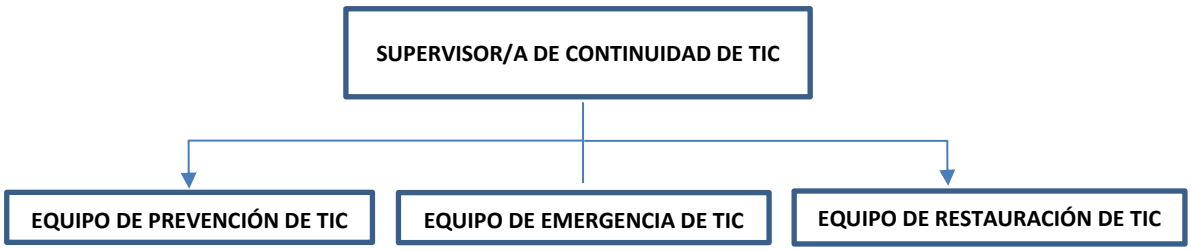
Y para la Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables, se dispone de la siguiente organización operativa:

- Supervisor de Continuidad de TIC.
- Equipo de prevención de TIC.

- Equipo emergencia de TIC.
- Equipo de restauración de TIC.

A continuación, se muestra el gráfico de la organización operativa del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables:

Cuadro N° 01



Fuente: Elaboración propia

Las actividades planificadas como parte del presente documento técnico podrán ejecutarse en forma presencial, semipresencial o en remoto, según los escenarios que puedan surgir ante los diversos eventos de mayor impacto considerados en el presente Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables; así como de acuerdo con las disposiciones vigentes.

8.1.1. Roles, funciones y responsabilidades:

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar tanto el Supervisor de continuidad de TIC, así como los distintos equipos del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables:

8.1.1.1. Supervisor/a de continuidad de TIC:

Este rol es asumido por el Director/a General de la OGTI del MIMP, que tiene la función de formular, proponer y actualizar los procedimientos y metodologías que resulten necesarios para minimizar las consecuencias en caso se produzca un evento que pueda afectar la operación de los servicios en el MIMP, entre otras funciones. Tiene a su cargo tres (03) equipos que son el de Prevención, Emergencia y de Restauración de TIC. El supervisor de Continuidad de TIC conformará a sus equipos de trabajo a través de un documento interno donde designará el rol de cada especialista como titular y alterno.

La relación del personal de la OGTI que forma parte del presente Plan debe ser actualizada de manera permanente, el responsable de actualizarla será el/la Supervisor/a de continuidad de TIC y deberá ser socializada al siguiente personal:

- Personal de la TI
- Personal de la Alta Dirección.
- Personal de Seguridad de la Entidad.

El/la supervisor(a) de Continuidad de TIC y tiene las siguientes funciones:

- Supervisar, dirigir y aprobar las acciones y/o estrategias a seguir en un evento dado.
- Activar el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables.
- Guiar y supervisar a los equipos de prevención, emergencia y recuperación en el desarrollo de sus actividades.
- Evaluar el impacto del evento y sus consecuencias potenciales sobre la infraestructura tecnológica.
- Notificar y mantener informados, a los miembros del Grupo de Comando de Continuidad Operativa acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- Monitorear y supervisar la recuperación de los procesos y recursos críticos de TI que forman parte del alcance del plan.
- Informar a los miembros del Grupo de Comando de Continuidad Operativa sobre las lecciones aprendidas y oportunidades de mejoras para la actualización del plan.
- Declarar el término de la ejecución del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables, cuando las operaciones de los sistemas y servicios del MIMP hayan sido restaurados.

8.1.1.2. De los equipos de prevención, emergencia y restauración de TIC:

Los miembros de cada equipo señalado deben disponer de un dispositivo móvil para las comunicaciones pertinentes, siendo necesario que los supervisores de cada equipo cuenten con línea abierta disponible; y de acuerdo a competencia, deban comunicarse con proveedores especializados. De igual manera, los correos electrónicos registrados deben estar alojados en una plataforma, que garantice la disponibilidad de este servicio. Todos los equipos están compuestos por el personal de TI de la OGTI (titular y alterno).

A. Equipo de prevención de TIC:

Es el equipo encargado de ejecutar acciones preventivas, antes que ocurra un evento que pueda afectar la operación de los servicios en el MIMP y en caso ocurriese, tener todos los medios requeridos para realizar la recuperación de los servicios de tecnologías de la información y comunicaciones, en el menor tiempo posible.

El equipo de prevención de TIC está compuesto por los siguientes miembros:

a. Supervisor/a del Equipo de Prevención de TIC.
b. Un/Una representante del equipo de Desarrollo y Sistemas de Información.
c. Un/Una representante del equipo de Plataforma de Atención al Usuario.
d. Un/Una representante del equipo de Infraestructura Tecnológica.
e. Un/Una representante del equipo de Innovación, Gobierno y Transformación Digital.

Tienen entre sus principales funciones las siguientes actividades:

- Formular, registrar, evaluar, documentar y mantener actualizado los procedimientos necesarios para el restablecimiento de los procesos y recursos críticos de TI.
- Realizar el análisis y evaluación de riesgos de seguridad y efectuar el tratamiento de los riesgos de acuerdo a competencia.
- Hacer seguimiento y participar de la ejecución del desarrollo de las pruebas y simulacros del plan de recuperación.
- Notificar y mantener informado al supervisor/a de continuidad de TIC, acerca de las pruebas y simulacros realizados.
- Informar al supervisor/a de continuidad de TIC sobre las lecciones aprendidas y oportunidades de mejoras para la actualización del plan.
- Mantener actualizado la documentación de los diagramas de red, servidores, conexiones físicas y ubicaciones de los equipos.
- Asegurar la programación y ejecución de las copias de respaldo (Backup) de los equipos de telecomunicaciones y de los sistemas de información críticos.
- Asegurar la programación y ejecución del mantenimiento preventivo y/o correctivo de infraestructura tecnológica del Centro de Datos y/o servidores de aplicaciones y/o servicios sobre tecnologías de contendedores y Dockers.
- Coordinar y supervisar la ejecución de pruebas de restauración de hardware y software.
- Verificar de manera trimestral que las estaciones de trabajo de la institución cuenten con los Sistemas Operativos y antivirus actualizados.
- Realizar y mantener actualizado el inventario hardware y software utilizado en el Centro de Datos del MIMP, equipos de cómputo, equipos de telecomunicaciones, teléfonos IP y anexos del personal del MIMP.

- Coordinar y reportar las medidas correctivas del análisis y evaluación de riesgos.
- Realizar el monitoreo de los servicios y de la infraestructura tecnológica.

B. Equipo de Emergencia de TIC:

Es el equipo encargado de ejecutar las acciones necesarias, cuando se suscita un evento que afecte la operación de los servicios en el MIMP.

El equipo de Emergencia de TIC está compuesto por los siguientes miembros:

a. Supervisor/a del Equipo de Emergencia de TIC.
b. Un/Una representante del equipo de Desarrollo y Sistemas de Información.
c. Un/Una representante del equipo de Plataforma de Atención al Usuario.
d. Un/Una representante del equipo de Infraestructura Tecnológica.
e. Un/Una representante del equipo de Innovación, Gobierno y Transformación Digital.

Tienen entre sus principales funciones las siguientes actividades:

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de determinar el impacto del evento en la continuidad de las operaciones del MIMP.
- Notificar y mantener informado al supervisor/a de continuidad de TIC, acerca de las evaluaciones realizadas.
- Contactar a los proveedores en caso de reemplazo de hardware, software y/o activación de servicios para la infraestructura tecnológica y/o sistemas afectados.
- Ejecutar los procedimientos que resulten pertinentes para minimizar el impacto del evento y dar continuidad a las operaciones de los recursos críticos del MIMP.
- Notificar y mantener informado al supervisor/a de continuidad de TIC, las acciones de emergencia ejecutadas.
- Brindar asistencia técnica en las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones.
- Informar al supervisor/a de continuidad de TIC sobre las lecciones aprendidas y oportunidades de mejoras para la actualización del plan.

C. Equipo de Restauración de TIC

Es el equipo encargado de asegurar la restauración del Centro de Datos una vez superado el evento que afectó la operación de los servicios; y dadas las condiciones necesarias para la vuelta a la operatividad en las instalaciones del MIMP.

El equipo de restauración de TIC está compuesto por los siguientes miembros:

a. Supervisor/a del Equipo de Restauración de TIC.
b. Un/Una representante del equipo de Desarrollo y Sistemas de Información.
c. Un/Una representante del equipo de Plataforma de Atención al Usuario.
d. Un/Una representante del equipo de Infraestructura Tecnológica.
e. Un/Una representante del equipo de Innovación, Gobierno y Transformación Digital.

Tienen entre sus principales funciones las siguientes actividades:

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de restaurar las operaciones en su totalidad.
- Notificar y mantener informado al supervisor/a de continuidad de TIC, acerca de las evaluaciones de las condiciones realizadas.
- Ejecutar los procedimientos que resulten pertinentes para la restauración de los procesos y recursos críticos del MIMP.
- Brindar asistencia técnica en las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones.
- Informar al supervisor/a de continuidad de TIC sobre la culminación de la restauración de los procesos y recursos críticos del MIMP.

Los equipos deben ejecutar sus actividades paralelamente, de acuerdo al siguiente orden de operación:

FIGURA N°01
FLUJO DEL ORDEN DE OPERACIÓN DE LOS EQUIPOS DE TI

FUENTE: ELABORACIÓN PROPIA

8.2. Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

En esta fase se identifican las aplicaciones críticas, los recursos necesarios y el periodo máximo de recuperación de los servicios de tecnologías de la información y comunicaciones. Se tomarán en cuenta todos los factores que puedan provocar eventos que requieran la activación del plan.

8.2.1. Procesos y recursos críticos

El proceso, aplicaciones y recursos críticos, cuentan con una expectativa del tiempo de recuperación, que se detalla a continuación:

TABLA N°01
PROCESOS Y RECURSOS CRÍTICOS DE TI

PROCESO CRÍTICO	APLICACIONES Y/O RECURSOS CRÍTICOS	TIEMPO DE RECUPERACIÓN (RTO*)
Gestión de las TIC	Equipos de Comunicaciones	10 h
	Equipos de protección eléctrica del centro de datos (UPS)	24 h
	Sistema de aire acondicionado de precisión del Centro de Datos	24 h
	Cableado de red de datos	12 h
	Internet corporativo	12 h
	Transmisión de datos	12 h
	Plataformas: hipervisores, contenedores, base de datos, aplicaciones	48 h
	Servicios: directorio activo, software de backup, correo electrónico	48 h
	Sistema de almacenamiento (storage)	24 h
	Medios de respaldo (cintas de backup)	24 h
	Certificado Digital para firma	96 h
	Líneas de emergencia de atención al ciudadano	24 h
	Sistemas de Gestión Administrativa: Sistema de Gestión Documental, Sistema de Gestión Administrativa, Sistema de Administración Financiera, Sistema de Tesorería, Sistema de Recursos Humanos (Planillas)	48 h
	Sistemas de Información enfocados para la atención al Ciudadano	48 h
	Personal crítico responsable de los procesos de TIC.	24 h
	Estaciones de trabajo para el personal crítico (computadoras personales y portátiles)	48 h

*El RTO: Tiempo de Recuperación Objetivo, es determinado por el criterio del personal de la OGTI

Fuente: Elaboración propia.

En base al cálculo de los cuadros del Anexo 01, se muestran los siguientes resultados:

8.2.2. Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios TIC del MIMP, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos, así como la percepción del juicio de expertos.

TABLA N°02
AMENAZAS A LOS SERVICIOS DE TI

N°	AMENAZAS (EVENTO)	TIPO
1	Terremoto / Sismo	Siniestros
2	Inundación en el Centro de Datos	
3	Incendio en el Centro de Datos	
4	Ciberdelito informático	Tecnológicos
5	Falla de hardware de la infraestructura tecnológica	
6	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Físico y ambiental
7	Ausencia o no disponibilidad del personal crítico de TI	Humanos
8	Sabotaje	
9	Pandemia y/o Epidemia	

Fuente: Elaboración propia.

Una vez determinadas las amenazas que pueden afectar los recursos críticos de Tecnologías de la Información, se calcula el nivel de probabilidad estimada, a fin de identificar las amenazas que serán consideradas en la evaluación de los riesgos.

A continuación, se detalla el resultado obtenido, de la **TABLA N°01**.

TABLA N°03
PROBABILIDAD ESTIMADA DE LAS AMENAZAS A LOS SERVICIOS DE TI

N°	AMENAZAS (EVENTO)	OCURRENCIA	PERCEPCIÓN	NIVEL PROBABILIDAD ESTIMADA
1	Terremoto / Sismo	1	2	Menor
2	Inundación en el Centro de Datos	1	2	Menor
3	Incendio en el Centro de Datos	1	2	Menor
4	Ciberdelito informático	3	4	Moderado
5	Falla de hardware de la infraestructura tecnológica	3	3	Moderado
6	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	4	4	Moderado
7	Ausencia o no disponibilidad del personal crítico de TI	3	3	Moderado
8	Sabotaje	2	2	Moderado
9	Pandemia y/o Epidemia	1	2	Menor

Fuente: Elaboración propia.

8.2.3. Identificación de controles existentes

La identificación de los controles existentes es un mecanismo que permite evaluar qué tan protegidos están los recursos de Tecnologías de la Información. En el MIMP se identificaron los siguientes controles para determinar el grado de protección frente a cada amenaza:

- Acuerdos de niveles de servicio con proveedor de servicio de Internet
- Acuerdos de niveles de servicio con proveedor de enlace de comunicación entre la Sede Central y las Sedes remotas del MIMP.
- Cámaras de vigilancia en el interior del Centro de Datos.
- Grupo electrógeno compartido con el Centro de Datos y oficinas de la Alta Dirección en el MIMP.
- Mantenimiento de grupo electrógeno y UPS. El mantenimiento de generadores (grupo electrógeno está a cargo de la Oficina de Abastecimiento) y el mantenimiento de UPS está a cargo de la Oficina General de Tecnologías de la información.
- Mantenimiento para equipos de aire acondicionado de precisión del Centro de Datos.
- Redundancia en los enlaces de comunicaciones (fibra óptica) y de internet, pero con el mismo proveedor.
- Respaldo de información.
- Solución antivirus instalada en los servidores de red y computadoras.
- Portal web alojado en la Plataforma única del estado de la Presidencia de Consejo de Ministros.
- Solución web para detección y protección de amenazas a las aplicaciones publicadas hacia internet.
- Sistema de detección y extinción de incendios en el centro de datos.
- Redundancia de Switch Core.
- Redundancia del Sistema de Almacenamiento del Centro de Datos.
- Solución de respaldo con características avanzadas de protección contra ransomware.
- Plataforma de virtualización consolidada y centralizada.
- Arquitectura de contenedores para una gestión y despliegue eficiente de servidores.
- Redundancia de la Base de Datos institucional.
- Redundancia de los equipos de aire acondicionado de precisión del Centro de Datos.
- Uso de conexiones remotas seguras con VPN.

8.2.4. Evaluación del nivel de riesgo

Para determinar el Nivel de Riesgo de un recurso crítico de Tecnologías de la Información del MIMP, se consideraron los controles existentes que permitan mitigan las amenazas descritas en el numeral 8.2.2. De acuerdo con la aplicación de la metodología de riesgos, descrita en el **ANEXO N°01**, se obtuvo el siguiente resultado.

TABLA N°04

RESULTADO DE LA EVALUACIÓN DE RIESGOS DE LOS SERVICIOS DE TI

N°	APLICACIONES Y/O RECURSOS CRÍTICOS	Terremoto / Sismo	Inundación en el Centro de Datos	Incendio en el Centro de Datos	Ciberdelito Informático	Falla de hardware de la infraestructura tecnológica	Falla del suministro eléctrico en el Centro de Datos y gabinetes de	Ausencia o no disponibilidad del personal crítico de TI	Sabotaje	Pandemia y/o Epidemia
1	Equipos de comunicaciones									
2	Equipos de protección eléctrica del centro de datos (UPS)									
3	Sistema de aire acondicionado de precisión del Centro de Datos									
4	Cableado de red de datos									
5	Internet Corporativo									
6	Transmisión de datos									
7	Plataformas: hipervisores, contenedores, base de datos, aplicaciones									
8	Servicios: directorio activo, software de backup, correo electrónico									
9	Sistema de almacenamiento (storage)									
10	Medios de respaldo (cintas de backup)									
11	Certificado Digital para firma									
12	Líneas de emergencia de atención al ciudadano (1810)									
13	Sistemas de Gestión Administrativa: Sistema de Gestión Documental, Sistema de Gestión Administrativa, Sistema de Administración Financiera, Sistema de Tesorería, Sistema de Recursos Humanos (Planillas)									
14	Sistemas de información enfocados para la atención al ciudadano									
15	Personal crítico responsable de los procesos de TIC									
16	Estaciones de trabajo del personal crítico (computadoras personales y portátiles									

Fuente: Elaboración propia.

Escenarios de riesgo

Los escenarios de riesgo que se presentan ante un desastre son:

- Destrucción e indisponibilidad de las plataformas (Hipervisores, contenedores, base de datos, aplicaciones) por un ciberdelito informáticos (Ransomware, Malware, etc).
- Falla en el funcionamiento de los servicios (Directorio activo, software de backup, correo electrónico) por fallas en el hardware de la infraestructura tecnológica y/o sabotaje.
- Interrupción de las comunicaciones de las líneas de emergencia de atención al ciudadano (1810) por un terremoto/sismo.
- Falla del equipo de protección eléctrica del centro de datos (UPS) debido a una falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.

A continuación, se presenta el consolidado de los escenarios de riesgo y su impacto para la activación del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables.

TABLA N°05
ESCENARIOS DE RIESGOS

ESCENARIO DE RIESGO	DESCRIPCIÓN	IMPACTO
Destrucción e indisponibilidad de las plataformas (Hipervisores, contenedores, base de datos, aplicaciones) por un ciberdelito informáticos (Ransomware, Malware, etc).	Este escenario consiste que las plataformas (Hipervisores, contenedores, base de datos, aplicaciones), se ven afectado en su funcionamiento, como resultado de un ataque informático (Ransomware), generando la paralización o interrupción de los servicios de infraestructura y las aplicaciones.	**EXTREMO**
Falla en el funcionamiento de los servicios (Directorio activo, software de backup, correo electrónico) por fallas en el hardware de la infraestructura tecnológica y/o sabotaje.	Este escenario se refiere a la falla físico o lógico (servidor virtual) de los servicios (Directorio activo, software de backup, correo electrónico) que se encuentran en la infraestructura de TI, generando la indisponibilidad de los servicios infraestructura y las aplicaciones.	**EXTREMO**
Interrupción de las comunicaciones de las líneas de emergencia de atención al ciudadano (1810) por un terremoto/sismo.	Este escenario se refiere al corte del servicio de las comunicaciones de las líneas de emergencia de atención al ciudadano (1810) y/o su infraestructura, produciendo la interrupción en las comunicaciones de los usuarios	**ALTO**
Falla del equipo de protección eléctrica del centro de datos (UPS) debido a una falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Este escenario consiste en el sobrecalentamiento del equipo de protección eléctrica del centro de datos (UPS) debido a una falla de sobretensión que origino que un componente mecánico se sobrecalentara y estallara, esto origino un amago de incendio y daño la infraestructura tecnológica.	**ALTO**

FUENTE: ELABORACIÓN PROPIA.

8.3. Fase 3: Estrategias del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones.

Las estrategias para la contingencia operativa en caso de un evento que pueda afectar la operación de los servicios en el MIMP, Se definen en tres tipos de estrategias:

8.3.1. Estrategia para la prevención:

Las estrategias para la prevención ante un evento que pueda afectar la operación de los servicios en el MIMP, teniendo dentro de sus principales actividades a realizar las siguientes:

A. Almacenamiento y respaldo de la información (backups):

La verificación de estas actividades, como parte de las estrategias de prevención del Plan, se deberá mantener actualizada. Las actividades son las siguientes:

- Gestionar copias y respaldo (Backup) de la información almacenada y procesada en el Centro de Datos, considerando la criticidad de los datos, así como los criterios de identificación de los medios, la frecuencia de rotación y transporte al sitio externo.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y la comprobación de los medios de respaldo.
- Realizar copias de fuentes de sistemas de información, de software base, sistema operativo, utilitarios, etc.
- Custodiar los medios magnéticos (cintas de backup) de almacenamiento de copias de respaldo a través de un proveedor externo.

B. Evaluación y gestión de proveedores:

La verificación de estas actividades, como parte de las estrategias del Plan, se deberá mantener actualizada. Las actividades son las siguientes:

- Mantener actualizado el listado y numero de contacto de proveedores de aplicaciones y recursos críticos de TI.
- Mantener actualizada la lista de los procesos y recursos críticos de TI, necesarios para garantizar la operación de los servicios en el MIMP, en caso se suscite un evento que pueda afectarlos.
- Si es necesario, adquirir o habilitar hardware y software, así como transportarlos al sitio alterno de ser el caso; las estrategias básicas para disponer de equipo de reemplazo serán:

  - Acuerdos con proveedores: Establecer acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.
  - Equipos de respaldo: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa.

En el **ANEXO N°02** se detalla la relación de los proveedores de aplicaciones y/o recursos críticos de TI y **ANEXO N° 03** componentes de la infraestructura tecnológica de contingencia.

C. Renovación tecnológica:

La renovación es necesaria para garantizar la continuidad de las aplicaciones y/o recursos críticos de la infraestructura tecnológica. Para ello, se debe realizar lo siguiente:

- Programar dos revisiones anuales de obsolescencia tecnológica de las partes y componentes de la infraestructura tecnológica para proceder a su renovación y/o actualización.
- Registrar en el **ANEXO N°07 – FORMATO 01,** las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, con el fin de adquirir equipos de contingencia basándose en las estadísticas de este registro.

D. Entrenamiento, Capacitaciones y personal de reemplazo:

Respecto al entrenamiento, capacitaciones y personal de reemplazo, se debe de considerar las siguientes actividades:

- Todo el personal de los equipos de prevención, emergencia y restauración, deben recibir entrenamiento y capacitaciones en los procesos del plan para la restauración de aplicaciones y recursos críticos de TI del MIMP. Las mismas que deben ser planificadas, estructuradas y acordes al plan. Además, los entrenamientos deben ser supervisados y evaluados por el Supervisor/a de continuidad de TIC, para evaluar que se ha logrado con el objetivo.
- Organizar al personal de TI de la OGTI, a fin de garantizar la presencia y disponibilidad de los equipos de respuesta del plan.
- Documentar y elaborar un repositorio de conocimiento de ciertos procedimientos que sean necesarios para la ejecución de procesos del plan, en caso el personal asignado no se encuentra disponible o presentes y así se pueda disponer de la información necesaria.
- Evaluar la posibilidad de incorporar personal de reemplazo a los equipos de respuesta del plan, para contar con especialistas disponibles en caso sea necesario ante un evento o contingencia para la restauración de aplicaciones y recursos críticos de TI del MIMP.

E. Activación de Teletrabajo (Plan de teletrabajo MIMP):

La activación del teletrabajo se llevará a cabo cuando no se den las condiciones de trabajo adecuadas para el personal. Se debe considerar lo siguiente:

- Verificar y validar el acceso seguro remoto a los sistemas y servicios TICs.
- Activar redes virtuales VPN, siempre que el equipo a conectarse cuente con los mecanismos de seguridad informática necesarios.

- En caso un usuario no dispone de un equipo para realizar su trabajo remoto, se le habilitará el equipo asignado en la sede Central del MIMP para entregárselo en su domicilio, siguiendo los protocolos establecidos por el equipo de Control Patrimonial de la Oficina de Abastecimiento.
- Realizar el trámite de certificados digitales y distribución de token de seguridad a los usuarios fuera de la entidad.
- Activar el desvío de las llamadas telefónicas a los usuarios encargados de la atención de las líneas de emergencia de atención al ciudadano (1810).

8.3.2. Estrategia frente a la Emergencia:

Las estrategias del equipo de emergencia de TIC frente a un evento critico que pueda afectar la operación de los servicios en el MIMP, que permitan controlar, mitigar y/o reducir los efectos producidos durante y después de un evento crítico, se definen las acciones que permitan la continuidad de las aplicaciones y/o recursos críticos:

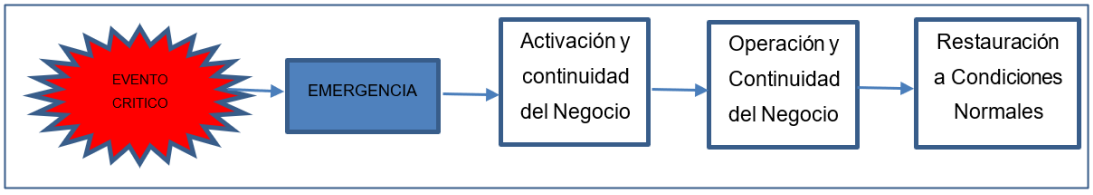
- Evaluar el alcance del desastre de acuerdo a las competencias de cada especialista.
- Notificar y reunir a los integrantes del equipo de Emergencia y Restauración de TIC.
- Informar al Supervisor/a de continuidad de TIC, sobre la situación presentada y solicitar la activación de las acciones definidas en plan para controlar, mitigar y/o reducir los efectos del evento crítico.
- Determinar si el área afectada es segura para los equipos de respuesta de la contingencia.
- Evaluar la proporción de los daños a las aplicaciones y/o recursos críticos, a fin de formular un informe del nivel de afectación sobre los mismos.
- Facilitar los recursos necesarios al personal encargado de la recuperación, para asegurar la realización de las actividades asignadas en los procesos del plan.

8.3.3. Estrategia para la restauración:

El alcance de las estrategias para la restauración del plan, incluye las acciones a realizar después de un evento crítico que pueda afectar la operación de los servicios en el MIMP, teniendo como objetivo la restauración de las aplicaciones y/o recursos críticos del MIMP. Para ello, se definen las acciones que permitan al personal de la OGTI garantizar la continuidad de las operaciones en la entidad.

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

FIGURA N° 02
CICLO DE LA ESTRATEGIA DE RECUPERACIÓN DE TI



FUENTE: ELABORACIÓN PROPIA

La priorización para la restauración de las aplicaciones y/o recursos críticos del MIMP, se ejecutará de acuerdo a lo indicado en la siguiente Tabla de información:

TABLA N°06
PRIORIDAD DE ATENCIÓN DURANTE LA RESTAURACIÓN DE TIC

PRIORIDAD DE ATENCIÓN	DESCRIPCIÓN
1	**ATENCIÓN PRIORITARIA:** Aplicaciones y/o recursos críticos que requieran alta disponibilidad de atención a usuarios, que brinden asistencia a la población vulnerable. Ejemplo: Sistema de Gestión Documental (SGD), Sistema Administrativo Financiero (SIAF), Sistema de Gestión Administrativa (SIGA), servidores de aplicación, servidores de bases de datos, entre otros.
2	**ATENCIÓN NORMAL:** Aplicaciones y/o recursos no relacionados con la atención de usuarios y población vulnerable. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.
3	**ATENCIÓN BAJA:** Aplicaciones y/o recursos de uso interno, poco uso y/o que manejan bajo volumen de información. Asimismo, equipos de apoyo. Ejemplo: Intranet, sistema de visitas, etc.

FUENTE: ELABORACIÓN PROPIA

En el **ANEXO N°04** listado de aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación de TI, con la respectiva prioridad de atención, en caso de activarse la el plan de recuperación y continuidad.

Acciones después de la contingencia

- Evaluar el trabajo de los equipos durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables, así como de las condiciones y recursos brindado para la ejecución del plan.

8.4. Fase 4: Elaboración del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables

Una vez identificados los eventos críticos y los escenarios de riesgos, se desarrollan los Planes de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables agrupados por las categorías indicadas previamente.

El Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables abordará los eventos de mayor impacto identificados en la Matriz de Riesgo de Contingencia. Estos eventos se tratarán en formatos independientes, como se indica en el siguiente cuadro:

TABLA N°07
EVENTOS DE MAYOR IMPACTO PARA EL PLAN DE RECUPERACION DE LOS SERVICIOS INFORMÁTICOS

N°	DESCRIPCIÓN	EXPOSICIÓN AL RIESGO	FORMATO PLAN DE CONTINGENCIA
1	Terremoto/Sismo	Extremo	FPC - 01
2	Incendio en el Centro de Datos	Extremo	FPC - 02
3	Inundación en el Centro de Datos	Alto	FPC - 03
4	Ciberdelito Informático	Alto	FPC - 04
5	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Alto	FPC - 05
6	Sabotaje	Alto	FPC - 06

FUENTE: ELABORACIÓN PROPIA

En el **ANEXO N°05** se presentan los formatos del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables.

8.5. Fase 5: Definición y ejecución de Pruebas del Plan.

Está enfocado principalmente en simular situaciones de contingencia que puedan surgir debido a evento que pueda afectar la operación de los servicios en el MIMP. Estas pruebas se llevarán a cabo en condiciones simuladas y controladas, utilizando respaldos que pueden ser empleados y replicados en una situación de un evento.

Para garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por los equipos de prevención, emergencia y restauración de las TIC. Estos equipos probarán, verificarán y observarán cualquier incidencia que surja durante las pruebas, con el fin de proporcionar retroalimentación para realizar la actualización del plan si es necesario.

La información que se desarrollará seguirá el siguiente esquema:

- Metodología (descripción de la prueba a efectuarse).
- Alcances (áreas afectadas / personal involucrado).
- Resultados.

Las pruebas relacionadas con este plan deberán ejecutarse cada cuatro (04) meses, a partir de la fecha de aprobación del Plan, para evaluar la preparación de la Entidad ante la ocurrencia de un evento y realizar los ajustes necesarios. Estas pruebas deberán ser registradas en el formato detallado en el **ANEXO N°06.**

8.6. Fase 6: Implementación del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables

La implementación del presente plan se realizará a partir del primer (01) mes de su aprobación.

Para tal efecto, el Supervisor/a de continuidad de TIC, será el responsable de asegurar el cumplimento de las funciones establecidas en el **punto 8.1.1** del presente plan.

8.7. Fase 7: Monitoreo

La fase de Monitoreo asegura la actualización y mantenimiento constante de los procesos y recursos críticos, para llevar a cabo el control de cambios.

IX. DISPOSICIONES COMPLEMENTARIAS

La Oficina General de Tecnologías de la Información del Ministerio de la Mujer y Poblaciones Vulnerables, es responsable de difundir el presente Plan, así como de brindar asistencia técnica, implementar y supervisar su cumplimiento, en el marco de la competencia de sus funciones.

X. ANEXOS:

ANEXO N°01	: Metodología aplicada a la gestión de riesgos.
ANEXO N° 02	**:** Relación de proveedores de servicios y recursos de TI.
ANEXO N° 03	**:** Componentes de la infraestructura tecnológica de contingencia.
ANEXO N° 04	: Listado de aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación de TIC.
ANEXO N°05	: Formatos del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables
ANEXO N°06	: Formato de Control y certificación de las Pruebas del Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones del Ministerio de la Mujer y Poblaciones Vulnerables
ANEXO N°07	: Formato de Registro de Incidencias de Deterioro de Equipos.

ANEXO N°01
METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

1. CÁLCULO DE LA PROBABILIDAD DE OCURRENCIA DE LA AMENAZA.

Para realizar este cálculo, se toman en cuenta dos variables: "Ocurrencia" y "Percepción".

Se considera "Ocurrencia" a la frecuencia en que se presentan los eventos a evaluar, sobre la base de los registros históricos de incidentes que hayan afectado al MIMP directamente. Se consideró la siguiente tabla de valores para el cálculo:

N°	OCURRENCIA	DESCRIPCIÓN
1	Rara Vez	Se presentó al menos una vez en los últimos 20 años / Nunca se presentó
2	No Frecuente	Se presentó al menos una vez en los últimos 10 años
3	Moderada	Se presentó más de una vez en los últimos 5 años
4	Frecuente	Se presentó por lo menos una vez al año en los últimos 5 años
5	Muy frecuente	Se presentó más de una vez al mes en el último año

La "Percepción" está basada netamente en la sensación de los expertos, de que la amenaza en cuestión podría ocurrir, se consideró la siguiente tabla de valores para el cálculo:

N°	PERCEPCIÓN	DESCRIPCIÓN
1	Muy Difícil	● <= 1% probabilidad, o ● El acontecimiento requiere de circunstancias excepcionales, o ● La probabilidad es nula, incluso en un futuro a largo plazo
2	Difícil	● >1% ó <=10% de probabilidad, o ● Puede ocurrir, pero no será anticipada
3	Mediana	● >10% ó <=50% de probabilidad, o ● Puede ocurrir en el mediano plazo
4	Posible	● >50% ó <=75% de probabilidad, o ● Podría ocurrir anualmente
5	Muy Posible	● >75% ó 100% de probabilidad, o ● El impacto está ocurriendo ahora, o ● Podría ocurrir dentro de unos meses

Los valores definidos para la Ocurrencia y Percepción son promediados y consolidados a fin de obtener una Probabilidad de Ocurrencia consensuada, asociada a cada amenaza en evaluación.

2. IDENTIFICACIÓN DE LAS AMENAZAS QUE SE TOMARÁN EN CUENTA PARA LA EVALUACIÓN.

De la combinación de las variables descritas se obtiene la Probabilidad Estimada, que sirve como valor discriminatorio para seleccionar que amenazas se deberían evaluar para el alcance. Aquellas que resultan en un nivel de probabilidad estimada insignificante, según la tabla siguiente, no son tomados en cuenta.

Nivel de Probabilidad Estimada	Interpretación
Extrema	Probabilidad de ocurrencia alta (Evaluación de prioridad alta)
Moderado	Probabilidad de ocurrencia intermedia (Evaluación de prioridad baja)
Menor	Probabilidad de ocurrencia muy baja (Evaluación sin prioridad)
Insignificante	No se cree que ocurra (Desestimar evaluación)

3. CÁLCULO DE LA PROBABILIDAD DE AFECTACIÓN DEL RECURSO.

Se utiliza la siguiente tabla de valores para el cálculo:

N°	PROBABILIDAD	DESCRIPCIÓN
1	IMPROBABLE	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados
2	BAJA	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas
3	MODERADA	Se cuenta con controles que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas, pero no son suficientes
4	ALTA	Algunos controles se prueban esporádicamente, debido a que no cuentan con un programa definido o de existir no se cumple con el mismo
5	MUY ALTA	Bajo nivel de controles o los controles existentes no son efectivos o eficientes

4. CÁLCULO DEL IMPACTO DEL RECURSO.

Se utiliza la siguiente tabla de valores para el cálculo:

N°	IMPACTO	DESCRIPCIÓN
1	NO SIGNIFICATIVO	Tiene un efecto nulo o muy pequeño en las operaciones de la sede evaluada
2	MENOR	Afecta hasta en 6 horas las operaciones de la sede evaluada
3	MODERADO	Afecta hasta en 24 horas las operaciones de la sede evaluada
4	MAYOR	Afecta hasta en 48 horas las operaciones de la sede evaluada

N°	IMPACTO	DESCRIPCIÓN
5	CATASTRÓFICO	Afecta por más de una semana las operaciones de la sede evaluada

5. CÁLCULO DEL NIVEL DE RIESGO

Se calcula considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Probabilidad de Afectación		Impacto				
		No Significativo (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
MUY ALTA	(5)	Alto	Alto	Extremo	Extremo	Extremo
ALTA	(4)	Moderado	Alto	Alto	Extremo	Extremo
MODERADA	(3)	Bajo	Moderado	Alto	Extremo	Extremo
BAJA	(2)	Bajo	Bajo	Moderado	Alto	Extremo
IMPROBABLE	(1)	Bajo	Bajo	Moderado	Alto	Alto

Interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación:

Nivel de Riesgo	Interpretación
EXTREMO	Riesgo no deseable, se requiere acción correctiva inmediata
ALTO	Riesgo no deseable que requiere de una acción correctiva, pero se permite alguna discreción de la gerencia sobre los plazos y compromisos
MODERADO	Riesgo aceptable con revisión de la dirección
BAJO	Riesgo aceptable sin revisión

ANEXO N°02
RELACIÓN DE PROVEEDORES DE SERVICIOS Y RECURSOS DE TI

N°	DESCRIPCIÓN	PROVEEDOR	TELÉFONO
1	SERVICIO CERTIFICADO DIGITAL SSL PARA LOS SISTEMAS DE INFORMACIÓN DEL MINISTERIO DE LA MUJER	BMTECH-PERU S.A.C.	(01) 246-1991
2	SERVICIO DE INTERNET E INTERCONEXION Y DE SEGURIDAD INFORMATICA GESTIONADA	WIN EMPRESAS	(01) 500-7500
3	SERVICIO DE MANTENIMIENTO PREVENTIVO DE EQUIPO DE AIRE ACONDICIONADO DE PRECISIÓN	INTEGRITY PERU S.A.C	(01) 634-9626
4	SERVICIO DE MANTENIMIENTO PREVENTIVO DEL SISTEMA DE PROTECCIÓN DE ENERGIA ELECTRICA	INTEGRITY PERU S.A.C	(01) 634-9626
5	SERVICIO DE SOPORTE DE SOFTWARE DE BACKUP	VEEM BACKUP	(01) 18006911991
6	SERVICIO DE CUSTODIA DE CINTAS DE BACKUP	IRON MOUNTAIN S.A.	(01) 711-4000
7	SERVICIO DE CERTIFICADOS DIGITALES PARA FIRMA	RENIEC	(01) 315- 2700
8	SERVICIO DE SOPORTE DE ASISTENCIA TECNICA DEL SISTEMA DE RECURSOS HUMANOS (INTEGRIX)	LIT CONSULTING	(01) 641 9259 (funciona como celular)
9	SERVICIO DE VIDEOCONFERENCIA	PROVISIONES TECNOLOGICAS S.A.C.	(01) 969 340 543
10	SERVICIO DE ANTIVIRUS	Grupo Electrodata	(+51) 994 221 672

ANEXO N°03

COMPONENTES DE LA INFRAESTRUCTURA TECNOLÓGICA DE CONTINGENCIA

N°	TIPO DE COMPONENTE	ROL	DESCRIPCIÓN	PRIORIDAD
1	Site de Contingencia	Plataforma en la Nube	Plataforma en donde se implementará los servicios críticos	1
2	Servicio	Internet, Interconexión y Seguridad Informática Gestionada	Servicio que permitirá la conexión al Site de Contingencia, proporcionará los equipos de seguridad perimetral (firewall, antispam) y acceso vpn a usuarios remotos	1
3	Servicio	Comunicación de voz	Servicio que permitirá la disponibilidad de la línea de comunicación y atención de emergencia del MIMP	1
4	Servicio	Base de Datos	Servidor de base de datos Oracle	1
5	Servicio	Controlador de Dominio	Servidor de dominio de la entidad (AD, DNS)	1
6	Servicio	DHCP	Servidor DHCP de la entidad	1
7	Servicio	Backup	Servidor donde se encuentra instalado el software de backup	1
8	Servicio	Correo	Servidor para envió y recepción de correos	1
9	Servicio	Repositorio de información	Servidor de archivos donde se encuentra la información de todas las carpetas compartidas en la entidad	1
10	Switch	Comunicaciones	Switch Core que realiza la comunicación en toda la entidad	1

ANEXO N°04

LISTADO DE APLICACIONES CRITICAS CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Nombre del Sistema	Descripción	Unidad de organización	Base de Datos	Tipo	Prioridad
1	Sistema de gestión documental	Sistema que permite el registro, atención y derivación del acervo documentario del MIMP utilizando firmas y certificados digitales para la emisión de documento, mostrando la Iniciativa del cero papel.	Oficina de Atención a la Ciudadanía y Gestión Documental	Oracle	Web	1
2	Sistema de Recursos Humanos (Integrix)	Sistema que permite la gestión de pago de planillas, registro de asistencia y legajos del personal del MIMP	Oficina General de Recursos Humanos	Sql Express	Web/Cliente-Servidor	2
3	Sistema Integrado de Administración Financiera (SIAF)	Sistema de Administración Financiera del MEF para la gestión presupuestal del MIMP	Oficina General de Administración / Oficina General de Planeamiento, Presupuesto y Modernización	Visual Fox Pro	Web / Cliente - Servidor	3
4	Sistema integrado de consultas pide	Permite hacer consultas Integradas de los servicios de la PIDE.	Oficina de Tecnologías de la Información / Dirección General de la Familia y Comunidad / Oficina de Atención a la Ciudadanía y Gestión Documental	Oracle	Web	3
5	Certificado Digital para la firma	Permite firmar documentos a través del Software de Firma	Despacho Viceministerial de Poblaciones Vulnerables	Java	Cliente	4
6	Sistema de supervisión, acreditación y fiscalización de centros de atención para personas adultas mayores	Permitirá realizar oportuna y eficiente la supervisión acreditación y el seguimiento a los centros de atención para personas adultas mayores a fin de garantizar su adecuado funcionamiento.	Dirección de Personas Adultas Mayores	Oracle	Web	4
7	Sistema de registro de centros integrales de atención del adulto mayor	Supervisa y acredita a los centros de adultos mayores. Empadrona a los adultos mayores y luego de ello se brinda servicios.	Dirección de Personas Adultas Mayores	Oracle	Web	4

N°	Nombre del Sistema	Descripción	Unidad de organización	Base de Datos	Tipo	Prioridad
8	Sistema informático de medidas de protección temporal para personas adultas mayores en situación de riesgo	Busca atender en forma oportuna y eficiente los casos que tome conocimiento la DIPAM sobre personas adultas mayores en situación de riesgo o desprotección, para su identificación, evaluación multidisciplinaria.	Dirección de Personas Adultas Mayores	Oracle	Web	4
9	Sistema de beneficencias públicas	Este sistema permite el registro y supervisión, de las Beneficencias Publicas	Dirección de Sociedades de Beneficencia	Oracle	Web	4
10	Sistema Integrado de Gestión Administrativa del MEF	Sistema de gestión administrativa del MEF para la gestión y registro del sistema nacional de abastecimiento	Oficina General de Administración / Oficina General de Planeamiento, Presupuesto y Modernización	Oracle	Cliente - Servidor	4
11	Sistema de mesa de partes virtual	El Sistema de interoperabilidad ha sido creado con el fin simplificar y agilizar el despacho y recepción de los documentos entre entidades del estado.	Oficina de Atención a la Ciudadanía y Gestión Documental	Oracle	Web	4
12	Sistema informático para el registro nacional de adopciones	Sistema que permite el registro y evaluación de familias que desean seguir el proceso de adopción.	Dirección de Adopciones	Oracle	Web	1
13	Sistema de banco de familias acogedoras	El Sistema de Bancos de Familia Acogedoras que permite el registro, evaluación y acreditación de las familias que deseen formar parte del banco de familia acogedoras.	Dirección de Protección Especial	Oracle	Web	1
14	Sistema de registro de personas desplazadas	Sistema que permite el registro, evaluación y acreditación de personas que han sufrido temas de desplazamiento por terrorismo y otro tipo de desastres.	Dirección de Desplazados y Cultura de Paz	Sql Server	Web	1
15	Sistema de voluntariado	Este sistema permite la inscripción, capacitación, evaluación de los requisitos y registro de los voluntarios y organizaciones y poder articularlos para realizar actividades de voluntariado.	Dirección de Voluntariado	Oracle	Web	2
16	Sistema de defensorías de la niña, niño y adolescentes	Sistema que permite la inscripción, supervisión y acreditación de las Defensorías Municipales de las Niñas, Niños y Adolescentes.	Dirección de Sistemas Locales y Defensorías	Oracle	Web	2

N°	Nombre del Sistema	Descripción	Unidad de organización	Base de Datos	Tipo	Prioridad
17	Sistema de centros de atención residencial	Sistema que permite la inscripción, supervisión y acreditación de los Centros de Atención Residencial.	Dirección General de Niñas, Niños y Adolescentes	Oracle	Web	2
18	Módulo de consulta externas	Permite a los usuarios externos hacer seguimiento a los documentos que han sido generados en el Sistema de Gestión Documental.	Oficina de Tramite Documentario y Atención al Ciudadano	Oracle	Web	2
19	Sistema de Hogares de Refugio Temporal	Permite el registro de los hogares de refugio temporal hasta su acreditación	Dirección de Asistencia Técnica y Promoción de Servicios	Oracle	Web	2
20	Sistema de transversalización del enfoque de genero	Registrar, evaluar, subsanar las actividades que las entidades de transversalización del enfoque de género implementadas en las entidades públicas.	Dirección General de Transversalización del Enfoque de Genero	Oracle	Web	3
21	Módulo de consulta congresales	Permite hacer seguimiento a los documentos congresales que han sido generados en el Sistema de Gestión Documental.	Secretaria General	Oracle	Web	3
22	Sistema de verificación de documentos	Permite hacer consulta de documentos que han sido generado en el Sistema de Gestión Documental, para verificar la emisión del documento digital.	Oficina de Tramite Documentario y Atención al Ciudadano	Oracle	Web	3
23	Módulo de consulta hoja tramite SGD	Permite hacer consultas a los documentos que han sido generados en el Sistema de Gestión Documental por diferentes filtros de búsquedas. Además, exporta en formato Excel los datos consultados.	Oficina de Tramite Documentario y Atención al Ciudadano	Oracle	Web	3
24	Sistema de monitoreo y evaluación de políticas de NNA	Sistema que permite el registro y seguimiento de indicadores para el cumplimiento del PNAIA.	Dirección General de Niñas, Niños y Adolescentes	Oracle	Web	3
25	módulo de tablero de desempeño	Permite la visualización de tableros de desempeño de la PP117 de la información obtenida a las niñas, niños y adolescentes - NNA	Oficina de Monitoreo y Evaluación de Políticas	Oracle	Web	4
26	Sistema de envíos y mensajería	Sistema que permite el envío de documentos por correspondencia.	Oficina de Tramite Documentario y Atención al Ciudadano	Oracle	Escritorio	4
27	Sistema nacional de indicadores de genero	Sistema que permite el registro, seguimiento de los indicadores de género en cumplimiento al PLANIG.	Dirección General de Igual de Genero y No Discriminación	Oracle	Web	4

N°	Nombre del Sistema	Descripción	Unidad de organización	Base de Datos	Tipo	Prioridad
28	Sistema georreferenciado MIMP	Permite la visualización de los servicios que brinda el MIMP, a través de un mapa geográfico.	Oficina de Monitoreo y Evaluación de Políticas	Oracle	Web	4
29	Sistema de gestión de capacidades	Sistema que permite la programación y ejecución de actividades con la finalidad de sensibilizar a los diferentes niveles de gobierno en temáticas del MIMP	Oficina de Monitoreo y Evaluación de Políticas	Oracle	Web	4
30	Sistema de intervenciones del MIMP	Permite el registro de las estructuras nominales EDNE	Oficina de Monitoreo y Evaluación de Políticas	Oracle	Web	4
31	Sistema de resoluciones	Permite el registro de resoluciones y comisiones; así mismo, permite la búsqueda avanzada de resoluciones por contenido.	Secretaria General	Oracle	Web	4
32	Sistema Repositorio RENE	Sistema permite la carga de las estructuras de datos nominales del sector	Oficina de Monitoreo y Evaluación de Políticas	Oracle	Web	4

ANEXO N°05

FORMATOS DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES POR EVENTO DE RIESGO

MIMP	EVENTO TERREMOTO/SISMO	FPC – 01

1. PLAN DE PREVENCIÓN

A. DESCRIPCIÓN DEL EVENTO

Un terremoto o sismo puede causar daños estructurales a las instalaciones del Centro de Datos, interrumpir la conectividad de la red de telecomunicaciones y/o incluso provocar daños en los equipos informáticos y sistemas de almacenamiento, el movimiento sísmico puede también afectar al suministro eléctrico y los sistemas de respaldo.

Infraestructura

- Oficinas y/o Centro de Datos

Recursos Humanos

- Personal de la entidad.

B. OBJETIVO

Establecer las acciones que se ejecutarán ante un terremoto/sismo a fin de minimizar el tiempo de interrupción de las operaciones del MIMP, sin exponer la seguridad de las personas.

C. ENTORNO

Este evento puede afectar las instalaciones de la Sede Central y el Centro de Datos, al ubicarse en la misma ciudad y distritos colindantes, donde se encuentran las Aplicaciones y/o recursos críticos.

D. PERSONAL ENCARGADO

Equipo de Prevención de TIC de la OGTI – MIMP.

E. ACCIONES DEL EQUIPO DE PREVENCIÓN DE TIC

- Evaluar en coordinación con el Grupo de Comando de Continuidad Operativa el ambiente para el Centro de Datos, en el sitio alterno.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información base de datos, código fuentes y ejecutables.
- Revisión periódica de las instalaciones y equipos para garantizar que estén protegidos ante posibles sismos.
- Monitoreo constante de los sistemas de energía y generadores de respaldo.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.

- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- Implementación de un site de contingencia en donde se implementarán los servicios y recursos críticos.
- Realizar las gestiones con las unidades de organización pertinentes para el refuerzo estructural del Centro de Datos
- Implementar soluciones capaces absorber la frecuencia y reducir el nivel de vibración producto de un terremoto/sismo que llegará a los recursos críticos de TI.

2. PLAN DE EJECUCIÓN

A. EVENTOS QUE ACTIVAN LA CONTINGENCIA

- Desplazamiento físico de equipos informáticos y servidores debido al movimiento sísmico.
- Pérdida de conectividad y/o daños a las infraestructuras tecnológicas y de telecomunicaciones, corte del suministro eléctrico e indisponibilidad de los sistemas de climatización y de energía en el Centro de Datos.

B. PROCESOS RELACIONADOS ANTES DEL EVENTO

- Todos los procesos y recursos críticos de TI que dependan de la infraestructura tecnológica y de telecomunicaciones deben contar con los procedimientos necesarios para el restablecimiento de los mismos.
- Asegurar la programación y ejecución del mantenimiento preventivo y/o correctivo de infraestructura tecnológica del Centro de Datos y/o servidores de aplicaciones y/o servicios sobre tecnologías de contendedores y Dockers.
- Coordinar y supervisar la ejecución de pruebas de restauración de hardware y software.
- Realizar y mantener actualizado el inventario hardware y software utilizado en el Centro de Datos del MIMP, equipos de cómputo, equipos de telecomunicaciones, teléfonos IP y anexos del personal del MIMP.
- Realizar el monitoreo de los servicios y de la infraestructura tecnológica.

C. PERSONAL QUE AUTORIZA LA CONTINGENCIA INFORMÁTICA

El/La Supervisor/a de Continuidad de TIC.

D. PERSONAL ENCARGADO

Equipo de Emergencia de TIC.

E. DESCRIPCIÓN DE LAS ACTIVIDADES DESPUÉS DE ACTIVAR LA CONTINGENCIA

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de determinar el impacto del evento en la continuidad de las operaciones del MIMP.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Ejecutar los procedimientos que resulten pertinentes para minimizar el impacto del evento y dar continuidad a las operaciones de los recursos críticos del MIMP.

- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento del MIMP, para las acciones que deban ser efectuadas por ellos.
- Notificar y mantener informado al supervisor/a de continuidad de TIC, las acciones de emergencia ejecutadas.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la Director/a General de la OGTI deberá coordinar con la Secretaria General.

F. DURACIÓN

La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

Las acciones tomadas por el equipo de emergencia de TIC deben ser realizadas en un plazo promedio de 12 horas, dependiendo de la gravedad de los daños.

3. PLAN DE RECUPERACIÓN

A. PERSONAL ENCARGADO

El personal encargado es el/la Supervisor/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es restaurar el desarrollo normal de los servicios y operaciones de TI del MIMP.

B. DESCRIPCIÓN DE ACTIVIDADES

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de restaurar las operaciones en su totalidad.
- Verificar la disponibilidad de recursos para la recuperación como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Ejecutar los procedimientos que resulten pertinentes para la restauración de los procesos y recursos críticos del MIMP.
- Brindar asistencia técnica en las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.
- Informar al Grupo de Comando de Continuidad Operativa sobre la culminación de la restauración de los procesos y recursos críticos del MIMP.

C. MECANISMOS DE COMPROBACIÓN

Se presentará un informe al Grupo de Comando de Continuidad Operativa, de los resultados de las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.

D. DESACTIVACIÓN DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD EJECUTORA 001: ADMINISTRACIÓN NIVEL CENTRAL DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

El/La Supervisor/a de Continuidad de TIC desactivará el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables una vez que se haya tomado las acciones descritas en el presente Plan, mediante una comunicación al Grupo de Comando de Continuidad Operativa.

E. PROCESO DE ACTUALIZACIÓN

El proceso de actualización será en base al informe presentado, luego del cual se determinará las acciones a tomar.

MIMP	EVENTO INCENDIO EN EL CENTRO DE DATOS	FPC – 02

1. PLAN DE PREVENCIÓN

A. DESCRIPCIÓN DEL EVENTO

Un incendio en el Centro de Datos podría destruir los recursos críticos, interrumpir el acceso a servicios y poner en riesgo la integridad de los datos almacenados, también puede afectar al suministro eléctrico y los sistemas de respaldo.

Infraestructura

- Oficinas y/o Centro de Datos

Recursos Humanos

- Personal de la entidad.

B. OBJETIVO

Establecer las acciones que se ejecutarán, a fin de mitigar el impacto de un incendio en el Centro de Datos y asegurar la rápida restauración de los servicios afectados.

C. ENTORNO

Este evento podría ocurrir en cualquier parte del Centro de Datos, especialmente en áreas con equipos eléctricos o de almacenamiento de datos, donde se encuentran las Aplicaciones y/o recursos críticos.

D. PERSONAL ENCARGADO

Equipo de Prevención de TIC de la OGTI – MIMP.

E. CONDICIONES DE PREVENCIÓN DE RIESGO

- Asegurar la programación y ejecución del sistema de detección y extinción de incendios (sensores de humo, aspersores, alarmas).
- Asegurar la programación y ejecución del sistema de protección eléctrica (UPS).
- Asegurar la programación y ejecución del mantenimiento preventivo y/o correctivo de infraestructura tecnológica del Centro de Datos.
- Asegurar la programación y ejecución del mantenimiento preventivo y/o correctivo de los tableros eléctricos del Centro de Datos.
- Realizar el seguimiento de la programación y ejecución del mantenimiento preventivo y/o correctivo del grupo electrógeno.
- Capacitación del personal de la OGTI y de seguridad (OAS) en procedimientos de evacuación y uso de equipos de emergencia.

F. ACCIONES DEL EQUIPO DE PREVENCIÓN DE TIC

- Evaluar en coordinación con el Grupo de Comando de Continuidad Operativa el ambiente para el Centro de Datos, en el sitio alterno.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información base de datos, código fuentes y ejecutables.

- Revisión periódica de las instalaciones y equipos para garantizar que estén en óptimas condiciones.
- Monitoreo constante de los sistemas de energía y generadores de respaldo.
- Mantener actualizado el inventario hardware utilizado en el Centro de Datos de la entidad.

2. PLAN DE EJECUCIÓN

A. EVENTOS QUE ACTIVAN LA CONTINGENCIA

Pérdida de conectividad y/o daños a las infraestructuras tecnológicas y de telecomunicaciones, corte del suministro eléctrico e indisponibilidad de los sistemas de climatización y de energía en el Centro de Datos debido al incendio.

B. PROCESOS RELACIONADOS ANTES DEL EVENTO

- Todos los procesos y recursos críticos de TI que dependan de la infraestructura tecnológica y de telecomunicaciones deben contar con los procedimientos necesarios para el restablecimiento de los mismos.
- Asegurar la programación y ejecución del mantenimiento preventivo y/o correctivo de infraestructura tecnológica del Centro de Datos.
- Coordinar y supervisar la ejecución de pruebas de restauración de hardware y software.
- Realizar y mantener actualizado el inventario hardware y software utilizado en el Centro de Datos del MIMP, equipos de cómputo, equipos de telecomunicaciones, teléfonos IP y anexos del personal del MIMP.
- Realizar el monitoreo de los servicios y de la infraestructura tecnológica.
- Realización de simulacros internos en horarios que no afecten las actividades.

C. PERSONAL QUE AUTORIZA LA CONTINGENCIA INFORMÁTICA

El/La Supervisor/a de Continuidad de TIC.

D. PERSONAL ENCARGADO

Equipo de Emergencia de TIC.

E. DESCRIPCIÓN DE LAS ACTIVIDADES DESPUÉS DE ACTIVAR LA CONTINGENCIA

Fase de ALERTA:

- Recibida la alerta del Sistema de detección de incendios a través de la bocina exterior ubicada en la puerta del centro de datos, se realiza la verificación del estado en el que se encuentra la sala de servidores.
- Si se visualiza que la alarma interior de la sala de gabinetes está destellando una luz blanca NO SE DEBE INGRESAR, ya que es indicador de que el segundo sensor ha notificado al panel de control la descarga del agente para la extinción de un posible incendio.
- Si no se visualiza que la alarma interior de la sala de gabinetes está activa, el Equipo deberá ingresar de manera inmediata a fin de evaluar si se trata de una FALSA ALARMA, y activar el Sistema de Deshabilitación para cancelar la descarga del agente.

- Si se confirma el amago de un incendio, se deberá activar la Estación Manual para la descarga del agente y la extinción del incendio, acto seguido deberá evacuar en 10 segundos el interior del centro de datos.

Fase de EMERGENCIA PARCIAL:

- Si no se controla el amago de incendio, se procederá al uso de extintores portátiles, que deberán estar ubicados en el interior del centro de datos.
- Si no es posible controlar el amago, se procede a evacuar el centro de datos e informar al personal del MIMP para la evacuación de todo el edificio.

Fase de EMERGENCIA GENERAL:

- Ante la imposibilidad de controlar el incendio, se informa del estado al Grupo de Comando de la Continuidad operativa Sede Central del MIMP y se establece comunicación con las autoridades.

F. DURACIÓN

La duración total del evento dependerá del grado del incendio, la extinción total del fuego residual y los daños a la infraestructura.
Las acciones tomadas por el equipo de emergencia de TIC deben ser realizadas en un plazo promedio de 12 horas, dependiendo de la gravedad de los daños.

3. PLAN DE RECUPERACIÓN

A. PERSONAL ENCARGADO

El personal encargado es el/la Supervisor/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del MIMP.

B. DESCRIPCIÓN DE ACTIVIDADES

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de restaurar las operaciones en su totalidad.
- Verificar la disponibilidad de recursos para la recuperación como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Ejecutar los procedimientos que resulten pertinentes para la restauración de los procesos y recursos críticos del MIMP.
- Brindar asistencia técnica en las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.
- Informar al Grupo de Comando de Continuidad Operativa sobre la culminación de la restauración de los procesos y recursos críticos del MIMP.

C. MECANISMOS DE COMPROBACIÓN

Se presentará un informe al Grupo de Comando de Continuidad Operativa, de los resultados de las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.

D. DESACTIVACIÓN DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD EJECUTORA 001: ADMINISTRACIÓN NIVEL CENTRAL DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

El/La Supervisor/a de Continuidad de TIC desactivará el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables una vez que se haya tomado las acciones descritas en el presente Plan, mediante una comunicación al Grupo de Comando de Continuidad Operativa.

E. PROCESO DE ACTUALIZACIÓN

El proceso de actualización será en base al informe presentado, luego del cual se determinará las acciones a tomar.

MIMP	EVENTO INUNDACIÓN EN EL CENTRO DE DATOS	FPC – 03

1. PLAN DE PREVENCIÓN

A. DESCRIPCIÓN DEL EVENTO

Las inundaciones pueden dañar equipos de almacenamiento, servidores y sistemas de telecomunicaciones, comprometiendo la integridad física de la infraestructura tecnológica, también puede afectar al suministro eléctrico.

Infraestructura

- Oficinas y/o Centro de Datos

Recursos Humanos

- Personal de la entidad.

B. OBJETIVO

Establecer las acciones que se ejecutarán, a fin de prevenir daños por inundación y restaurar rápidamente aplicaciones y/o recursos críticos del MIMP.

C. ENTORNO

Este evento puede afectar las instalaciones de los Centros de Datos ubicados en zonas propensas a inundaciones o áreas con sistemas hidráulicos defectuosos, donde se encuentran las aplicaciones y/o recursos críticos del MIMP.

D. PERSONAL ENCARGADO

Equipo de Prevención de TIC de la OGTI – MIMP.

E. CONDICIONES DE PREVENCIÓN DE RIESGO

- Instalación de sistemas de drenaje adecuados.
- Uso de equipos de protección en áreas propensas a inundaciones (por ejemplo, barreras contra inundaciones).
- Mantenimiento de sistemas hidráulicos y revisión de los niveles de agua cercanos al centro.

F. ACCIONES DEL EQUIPO DE PREVENCIÓN DE TIC

- Evaluar en coordinación con el Grupo de Comando de Continuidad Operativa el ambiente para el Centro de Datos, en el sitio alterno.
- Verificación periódica de la infraestructura de drenaje.
- Inspección de las condiciones de humedad y posibles filtraciones en áreas críticas.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.

2. PLAN DE EJECUCIÓN

A. EVENTOS QUE ACTIVAN LA CONTINGENCIA

Pérdida de conectividad y/o daños a las infraestructuras tecnológicas y de telecomunicaciones, corte del suministro eléctrico e indisponibilidad de los sistemas de climatización y de energía en el Centro de Datos debido a la inundación.

B. PROCESOS RELACIONADOS ANTES DEL EVENTO

- Todos los procesos y recursos críticos de TI que dependan de la infraestructura tecnológica y de telecomunicaciones deben contar con los procedimientos necesarios para el restablecimiento de los mismos.
- Asegurar la programación y ejecución del mantenimiento preventivo y/o correctivo de infraestructura tecnológica del Centro de Datos.
- Coordinar y supervisar la ejecución de pruebas de restauración de hardware y software.
- Realizar y mantener actualizado el inventario hardware y software utilizado en el Centro de Datos del MIMP, equipos de cómputo, equipos de telecomunicaciones, teléfonos IP y anexos del personal del MIMP.
- Realizar el monitoreo de los servicios y de la infraestructura tecnológica.
- Realización de simulacros internos en horarios que no afecten las actividades.

C. PERSONAL QUE AUTORIZA LA CONTINGENCIA INFORMÁTICA

El/La Supervisor/a de Continuidad de TIC.

D. PERSONAL ENCARGADO

Equipo de Emergencia de TIC.

E. DESCRIPCIÓN DE LAS ACTIVIDADES DESPUÉS DE ACTIVAR LA CONTINGENCIA

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de determinar el impacto del evento en la continuidad de las operaciones del MIMP.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Ejecutar los procedimientos que resulten pertinentes para minimizar el impacto del evento y dar continuidad a las operaciones de los recursos críticos del MIMP.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento del MIMP, para las acciones que deban ser efectuadas por ellos.
- Notificar y mantener informado al supervisor/a de continuidad de TIC, las acciones de emergencia ejecutadas.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la Director/a General de la OGTI deberá coordinar con la Secretaria General.

F. DURACIÓN

La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

Las acciones tomadas por el equipo de emergencia de TIC deben ser realizadas en un plazo promedio de 12 horas, dependiendo de la gravedad de los daños.

3. PLAN DE RECUPERACIÓN

A. PERSONAL ENCARGADO

El personal encargado es el/la Supervisor/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del MIMP.

B. DESCRIPCIÓN DE ACTIVIDADES

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de restaurar las operaciones en su totalidad.
- Verificar la disponibilidad de recursos para la recuperación como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Ejecutar los procedimientos que resulten pertinentes para la restauración de los procesos y recursos críticos del MIMP.
- Brindar asistencia técnica en las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.
- Informar al Grupo de Comando de Continuidad Operativa sobre la culminación de la restauración de los procesos y recursos críticos del MIMP.

C. MECANISMOS DE COMPROBACIÓN

Se presentará un informe al Grupo de Comando de Continuidad Operativa, de los resultados de las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.

D. DESACTIVACIÓN DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD EJECUTORA 001: NIVEL CENTRAL DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

El/La Supervisor/a de Continuidad de TIC desactivará el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables una vez que se haya tomado las acciones descritas en el presente Plan, mediante una comunicación al Grupo de Comando de Continuidad Operativa.

E. PROCESO DE ACTUALIZACIÓN

El proceso de actualización será en base al informe presentado, luego del cual se determinará las acciones a tomar.

MIMP	EVENTO CIBERDELITO INFORMACION	FPC – 04

1. PLAN DE PREVENCIÓN

A. DESCRIPCIÓN DEL EVENTO

Un ciberataque puede comprometer la seguridad de los sistemas, filtración de datos, daño a la infraestructura o interrupción de servicios críticos.

El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc.

Este evento incluye los siguientes elementos mínimos identificados por MIMP, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores
- Estaciones de Trabajo

Software

- Software Base
- Sistemas de información, aplicativos y portales del MIMP

B. OBJETIVO

Proteger las aplicaciones y/o recursos críticos contra los ciberataques y restaurar la operatividad de los servicios afectados.

C. ENTORNO

Este evento puede darse en cualquiera de los servidores y estaciones ubicadas en el Centro de Datos y en la sede principal del MIMP.

D. PERSONAL ENCARGADO

El Equipo de Prevención de TIC es el responsable del correcto funcionamiento de los servidores, estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

E. CONDICIONES DE PREVENCIÓN DE RIESGO

- Instalación de parches de seguridad en los equipos.
- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.

- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones y servidores, para su reemplazo provisional hasta su desinfección y habilitación.
- Acceso a Internet a las estaciones de trabajo de acuerdo a perfiles de navegación que restrinjan el uso de acuerdo a sus funciones.
- Eliminación o restricción de lectoras y/o quemadores de CD en estaciones de trabajo de acuerdo a las funciones.
- Des habilitación de los puertos de comunicación USB en las estaciones de trabajo, para prevenir la conexión de unidades de almacenamiento externo.
- Ejecución de ataques de Hacking Ético por terceros especializados a fin de identificar brechas de seguridad y vulnerabilidades dentro de las aplicaciones y/o recursos críticos del MIMP.
- Implementación de firewalls, antivirus y sistemas de detección de intrusos.
- Auditorías de seguridad frecuentes.
- Capacitación continua del personal en mejores prácticas de seguridad.

F. ACCIONES DEL EQUIPO DE PREVENCIÓN DE TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en el Centro de Datos.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos.
- Documentar y validar los manuales de restauración de los sistemas de información en producción.
- Monitorear constantemente el tráfico de red y las actividades sospechosas.
- Optimización continua de las políticas de seguridad de accesos.

2. PLAN DE EJECUCIÓN

A. EVENTOS QUE ACTIVAN LA CONTINGENCIA

- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).
- Detección de malware, ransomware, acceso no autorizado o pérdida de datos debido a un ciberataque.

B. PROCESOS RELACIONADOS ANTES DEL EVENTO

- Todos los procesos y recursos críticos de TI que dependan de la infraestructura tecnológica y de telecomunicaciones deben contar con los procedimientos necesarios para el restablecimiento de los mismos.
- Coordinar y supervisar la ejecución de pruebas de restauración de hardware y software.

- Realizar y mantener actualizado el inventario hardware y software utilizado en el Centro de Datos del MIMP, equipos de cómputo, equipos de telecomunicaciones, teléfonos IP y anexos del personal del MIMP.
- Verificar de manera trimestral que las estaciones de trabajo de la institución cuenten con los Sistemas Operativos y antivirus actualizados.
- Realizar el monitoreo de los servicios y de la infraestructura tecnológica.
- Realización de simulacros internos en horarios que no afecten las actividades.

C. PERSONAL QUE AUTORIZA LA CONTINGENCIA INFORMÁTICA

El/La Supervisor/a de Continuidad de TIC y el/la Coordinador de la OGTI pueden activar la contingencia.

D. PERSONAL ENCARGADO

Equipo de Emergencia de TIC.

E. DESCRIPCIÓN DE LAS ACTIVIDADES DESPUÉS DE ACTIVAR LA CONTINGENCIA

- Aislar o retirar de la red de datos del MIMP, el servidor o equipo informático infectado o vulnerada que ponga en riesgo la información del Centro de Datos.
- Ejecutar pruebas de verificación sobre el equipo aislado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

F. DURACIÓN

La duración total del evento dependerá del grado de afectación a las aplicaciones y/o recursos críticos.

Las acciones tomadas por el equipo de emergencia de TIC deben ser realizadas en un plazo promedio de 12 horas, dependiendo de la afectación de los servicios.

3. PLAN DE RECUPERACIÓN

A. PERSONAL ENCARGADO

El personal encargado es el/la Supervisor/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es restaurar el desarrollo normal de los servicios y operaciones de TI del MIMP.

B. DESCRIPCIÓN DE ACTIVIDADES

Se informará a el/la Director/a General de la OGTI del MIMP el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

- Evaluar las condiciones de la infraestructura tecnológica, tanto de red como de los servidores en general del Centro de Datos, con el fin de restaurar las operaciones en su totalidad.
- Verificar la disponibilidad de recursos para la recuperación como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Ejecutar los procedimientos que resulten pertinentes para la restauración de los procesos y recursos críticos del MIMP.
- Brindar asistencia técnica en las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.
- Informar al Grupo de Comando de Continuidad Operativa sobre la culminación de la restauración de los procesos y recursos críticos del MIMP.

C. MECANISMOS DE COMPROBACIÓN

Se notificará a través del formato de incidentes de seguridad digital al Comité de Gestión de Seguridad de la Información y a la Secretaria de Gobierno y Transformación Digital.

Se presentará un informe al Grupo de Comando de Continuidad Operativa, de los resultados de las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.

D. DESACTIVACIÓN DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD EJECUTORA 001: NIVEL CENTRAL DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

El/La Supervisor/a de Continuidad de TIC desactivará el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables una vez que se haya tomado las acciones descritas en el presente Plan, mediante una comunicación al Grupo de Comando de Continuidad Operativa.

E. PROCESO DE ACTUALIZACIÓN

El proceso de actualización será en base al informe presentado, luego del cual se determinará las acciones a tomar.

MIMP	EVENTO FALLA DEL SUMINISTRO ELÉCTRICO EN EL CENTRO DE DATOS Y GABINETES DE COMUNICACIÓN	FPC – 05

1. PLAN DE PREVENCIÓN

A. DESCRIPCIÓN DEL EVENTO

Falla general del suministro de energía eléctrica en el Centro de Datos o sede principal de la entidad.

Una interrupción del suministro eléctrico puede afectar todos los sistemas del Centro de Datos y la conectividad con las Sedes Desconcentradas.

Este evento incluye los siguientes elementos mínimos identificados por MIMP, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos:

- Suministro de Energía Eléctrica

Hardware

- Servidores y sistema de almacenamiento de información (storage)
- Estaciones de Trabajo
- Equipos de Comunicaciones

Equipos Diversos

- UPS y generador eléctrico
- Aire acondicionado

B. OBJETIVO

Garantizar que los sistemas críticos continúen operando durante un corte de energía mediante sistemas de respaldo adecuados.

C. ENTORNO

Este evento puede ocurrir en la Sede Central donde se ubica el Centro de Datos, por tener cada una de ellas los gabinetes de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

D. PERSONAL ENCARGADO

Equipo de Prevención de TIC de la OGTI – MIMP.

E. CONDICIONES DE PREVENCIÓN DE RIESGO

- Contar con los UPS necesarios para asegurar el suministro eléctrico en los equipos consideradas como críticos.
- Asegurar la programación y ejecución del sistema de protección eléctrica (UPS).
- Realizar el seguimiento de la programación y ejecución del mantenimiento preventivo y/o correctivo del grupo electrógeno.

- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.

F. ACCIONES DEL EQUIPO DE PREVENCIÓN DE TIC

- Revisar periódicamente y de forma conjunta con el área de Servicios Generales las instalaciones eléctricas del Centro de Datos y Sede principal de la entidad.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, UPS, transformador y del gabinete trimestralmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos y la red de cómputo de la sede principal sea estabilizada. En caso no existan se debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en la sala de energía del centro de datos del MIMP.

2. PLAN DE EJECUCIÓN

A. EVENTOS QUE ACTIVAN LA CONTINGENCIA

Corte de suministro de energía eléctrica en los ambientes del MIMP.

B. PROCESOS RELACIONADOS ANTES DEL EVENTO

- Todos los procesos y recursos críticos de TI que dependan de la infraestructura tecnológica y de telecomunicaciones deben contar con los procedimientos necesarios para el restablecimiento de los mismos.
- Asegurar la programación y ejecución del mantenimiento preventivo y/o correctivo de los sistemas de protección eléctrica.
- Realizar y mantener actualizado el inventario hardware utilizado en el Centro de Datos del MIMP, equipos de cómputo, equipos de telecomunicaciones, estaciones de trabajo del MIMP.
- Realizar el monitoreo de los servicios y de la infraestructura tecnológica.
- Realización de simulacros internos en horarios que no afecten las actividades.

C. PERSONAL QUE AUTORIZA LA CONTINGENCIA INFORMÁTICA

El/La Supervisor/a de Continuidad de TIC.

D. PERSONAL ENCARGADO

Equipo de Emergencia de TIC.

E. DESCRIPCIÓN DE LAS ACTIVIDADES DESPUÉS DE ACTIVAR LA CONTINGENCIA

- Informar a el/la director/a de la Oficina de Abastecimiento del problema presentado.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de energía.

- Dar aviso del corte de energía eléctrica en forma oportuna a todas las unidades de organización del MIMP y coordinar las acciones necesarias.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo, en caso exceden el tiempo de autonomía.
- En caso la interrupción de energía en el Centro de Datos sea mayor a dos (02) horas, se deberán apagar los equipos en forma ordenada mientras funcione el UPS y hasta que regrese el fluido eléctrico.

F. DURACIÓN

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica.

Las acciones tomadas por el equipo de emergencia de TIC deben ser realizadas en un plazo promedio de 12 horas, dependiendo de la duración del corte de energía eléctrica.

3. PLAN DE RECUPERACIÓN

A. PERSONAL ENCARGADO

El Equipo de Restauración de TIC, quienes se encargarán de realizar las acciones de recuperación necesarias.

B. DESCRIPCIÓN DE ACTIVIDADES

El evento será evaluado y registrado de ser necesario en el formato de incidentes de seguridad de la información.

Se debe realizar como mínimo las siguientes actividades:

- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía.
- Proceder a encender la plataforma tecnológica ordenadamente de acuerdo al siguiente detalle:
  - Restaurar el suministro eléctrico y verificar el funcionamiento de los generadores de respaldo.
  - Equipos de Comunicaciones (router, switches core, switches de acceso)
  - Equipos de almacenamiento (storage)
  - Servidores físicos por orden de prioridad
  - Servidores virtuales por orden de prioridad
- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.
- Restaurar el suministro eléctrico y verificar el funcionamiento de los generadores de respaldo.

C. MECANISMOS DE COMPROBACIÓN

Se presentará un informe al Grupo de Comando de Continuidad Operativa, de los resultados de las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.

D. DESACTIVACIÓN DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD EJECUTORA 001: NIVEL CENTRAL DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

El/La Supervisor/a de Continuidad de TIC desactivará el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables una vez que se haya tomado las acciones descritas en el presente Plan, mediante una comunicación al Grupo de Comando de Continuidad Operativa.

E. PROCESO DE ACTUALIZACIÓN

El proceso de actualización será en base al informe presentado, luego del cual se determinará las acciones a tomar.

MIMP	EVENTO SABOTAJE	FPC – 06

1. PLAN DE PREVENCIÓN

A. DESCRIPCIÓN DEL EVENTO

El sabotaje en el contexto de las Tecnologías de la Información (TI) puede manifestarse de diversas formas, incluyendo la alteración o destrucción intencional de hardware, la manipulación de sistemas operativos, la eliminación de datos críticos, o la interrupción de servicios informáticos críticos. Este evento puede involucrar el acceso no autorizado a las infraestructuras de TI por parte de empleados o terceros malintencionados, lo que afectaría la confidencialidad, integridad y disponibilidad de la información y los servicios.

Este tipo de evento puede involucrar lo siguiente:

Hardware: Equipos de servidores, dispositivos de almacenamiento, equipos de red.

Software: Sistemas operativos, aplicaciones críticas, bases de datos.
Datos: Pérdida, corrupción o robo de datos confidenciales, manipulación de registros o información sensible.

B. OBJETIVO

Minimizar el impacto del sabotaje sobre la infraestructura de TI y los servicios proporcionados por el Ministerio de la Mujer y Poblaciones Vulnerables (MIMP). Asegurar la restauración de los servicios afectados y proteger los activos tecnológicos, garantizando la seguridad de la información.

C. ENTORNO

Este evento puede ocurrir en cualquier parte de la infraestructura de TI, ya sea en el Centro de Datos o en la red de comunicaciones de las Sede Central. Afecta tanto a sistemas informáticos.

D. PERSONAL ENCARGADO

Equipo de Prevención de TIC de la OGTI – MIMP.

E. CONDICIONES DE PREVENCIÓN DE RIESGO

- Implementación de políticas de control de acceso físico y lógico a los sistemas y equipos de TI.
- Revisión periódica de sistemas de seguridad como antivirus, firewalls y sistemas de detección de intrusos (IDS).
- Capacitación continua del personal en cuanto a procedimientos de seguridad y protocolos de actuación ante incidentes.
- Uso de cifrado de datos sensibles tanto en reposo como en tránsito.
- Auditorías de seguridad periódicas de sistemas críticos y análisis de vulnerabilidades.
- Monitoreo constante de logs de acceso y actividades anómalas en los sistemas.

F. ACCIONES DEL EQUIPO DE PREVENCIÓN DE TIC

- Monitorear y revisar logs de acceso a los sistemas y de actividades inusuales que puedan sugerir intentos de sabotaje.
- Optimizar las políticas de seguridad informática y realizar análisis de vulnerabilidades.
- Implementar controles de acceso robustos y autenticación multifactorial en todas las plataformas críticas.
- Capacitar al personal en materia de seguridad de la información y buenas prácticas.

2. PLAN DE EJECUCIÓN

A. EVENTOS QUE ACTIVAN LA CONTINGENCIA

- Modificación no autorizada o eliminación de datos críticos.
- Alteración de la configuración de los sistemas, comprometiendo su funcionalidad.
- Interrupción de los servicios de TI como resultado de un cambio no autorizado
- Interrupción de los servicios de TI como resultado de la manipulación de hardware no autorizada a la infraestructura.

B. PROCESOS RELACIONADOS ANTES DEL EVENTO

- Realizar el análisis y evaluación de riesgos de seguridad física y lógica, a fin de efectuar el tratamiento de los mismos.
- Los procesos de acceso y manipulación de datos críticos, así como las operaciones en los servidores y redes, deben estar siempre bajo estrictos controles de seguridad.

C. PERSONAL QUE AUTORIZA LA CONTINGENCIA INFORMÁTICA

El/La Supervisor/a de Continuidad de TIC.

D. PERSONAL ENCARGADO

Equipo de Emergencia de TIC.

E. DESCRIPCIÓN DE LAS ACTIVIDADES DESPUÉS DE ACTIVAR LA CONTINGENCIA

Contención: Inmediatamente, se debe aislar los sistemas afectados para evitar la propagación del sabotaje, desconectando dispositivos comprometidos de la red, bloqueando accesos no autorizados y, si es necesario, desactivando servicios críticos temporalmente.

Evaluación inicial: Verificar la extensión del sabotaje (por ejemplo, el alcance de la pérdida de datos, alteración de sistemas, etc.).

Restauración de servicios: Si se dispone de respaldos, iniciar el proceso de restauración de la información afectada.

Investigación: Llevar a cabo una investigación forense para identificar la causa raíz del sabotaje y determinar los responsables, utilizando herramientas de análisis forense digital.

Notificación: Informar al Director/a de la OGTI, al Comité de Gobierno y Transformación Digital y, si corresponde, a las autoridades competentes, para que se tomen las acciones legales necesarias.

F. DURACIÓN

La duración de la recuperación dependerá de la magnitud del sabotaje. Si la interrupción se debe a la alteración de sistemas o datos, el tiempo estimado de recuperación puede ser de 2 a 8 horas, dependiendo de los recursos disponibles para la restauración de servicios. En casos de sabotaje de gran escala o pérdida de datos sensibles, podría tomar más tiempo, y será necesario realizar una evaluación detallada de los daños y la mitigación.

3. PLAN DE RECUPERACIÓN

A. PERSONAL ENCARGADO

El personal encargado es el/la Supervisor/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es restaurar el desarrollo normal de los servicios y operaciones de TI del MIMP.

B. DESCRIPCIÓN DE ACTIVIDADES

Verificación de los respaldos: Asegurarse de que los respaldos de los sistemas afectados estén disponibles y sean válidos. Si la información no está comprometida, proceder a la restauración de los datos.

Análisis forense: Después de la restauración de servicios, realizar un análisis exhaustivo de los sistemas afectados para identificar el origen y la naturaleza del sabotaje.

Pruebas de seguridad: Validar que todos los sistemas restaurados sean seguros y que no haya vulnerabilidades explotables por atacantes.

Comunicación: Informar al Director/a de la OGTI y a las partes interesadas sobre el estado de la recuperación y las acciones tomadas.

C. MECANISMOS DE COMPROBACIÓN

Se presentará un informe al Grupo de Comando de Continuidad Operativa y al Comité de Gobierno y Transformación Digital, de los resultados de las labores de verificación y validación de operación de los servicios de Tecnologías de la Información y Comunicaciones restaurados.

D. DESACTIVACIÓN DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD EJECUTORA 001: NIVEL CENTRAL DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

El/La Supervisor/a de Continuidad de TIC desactivará el Plan de Recuperación y Continuidad de los Servicios de Tecnologías de la Información y Comunicaciones de la Unidad Ejecutora 001: Administración Nivel Central del Ministerio de la Mujer y Poblaciones Vulnerables una vez que se haya tomado las acciones descritas en el presente Plan, mediante una comunicación al Grupo de Comando de Continuidad Operativa.

E. PROCESO DE ACTUALIZACIÓN

El proceso de actualización será en base al informe presentado, luego del cual se determinará las acciones a tomar.

ANEXO N°06

FORMATO DE CONTROL Y CERTIFICACION DE LAS PRUEBAS DEL PLAN DE RECUPERACIÓN Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

PERÚ Ministerio de la Mujer y Poblaciones Vulnerables	PLANIFICACIÓN DE PRUEBAS DE CONTINGENCIA	FORMATO 13

Prueba N°	Fecha	Propósito

N°	Objetivos de la Prueba

N°	Escenario
Participantes de la Prueba	
Detalles de la Prueba	

Resultado de la Prueba			
Resumen de la Prueba			
Fecha inicio de prueba		Hora de inicio de prueba	
Fecha termino de prueba		Hora término de prueba	
Duración de la prueba			
Participantes en la prueba			
Descripción de la prueba realizada			
Resultado de la prueba			
Mejoras identificadas.			

ANEXO N°07

FORMATO DE REGISTRO DE INCIDENCIAS DE DETERIORO DE EQUIPOS

	FORMATO DE REGISTRO DE INCIDENCIAS DE DETERIORO DE EQUIPOS	FORMATO 1

Tipo: Servidor, Switch, Almacenamiento, librería, etc.

N°	Fecha	Tipo	Nombre de Equipo	Marca	Tipo / Modelo	Sistema operativo	Versión	Uso o Función	Locación / Sitio	Criticidad	Propietario	Producción o Contingencia	Comentarios