RESOLUCIÓN DE ALCALDÍA N° 563-2024-MPLC/A.

Quillabamba, 25 de octubre del 2024.

VISTOS:

El Informe N° 0213-2024-MAAQ/OTIC-MPLC, de fecha 25 de septiembre de 2024, emitido por el Jefe de la Oficina de Tecnologías de la Informacion y Comunicaciones, Informe N° 1651-2024-ZLLD-MPLC, de fecha 26 de septiembre de 2024, emitido por la Directora de la Oficina General de Administración, Informe N° 360-2024-OPM-OGPP-MPLC/LC, de fecha 14 de octubre de 2024, emitido por el Jefe de la Oficina de Planeamiento y Modernización, Informe N° 0633-2024-JVM/OGPP-MPLC, de fecha 14 de octubre del 2024, emitido por el Director de la Oficina General de Planeamiento y Presupuesto, Informe Legal N° 1148-2024-OAGJ-MPLC, de fecha 22 de octubre de 2024, emitido por el Director de la Oficina General de Asesoría Jurídica, con Proveído N° 005885, de fecha 24 de octubre de 2024, y;

CONSIDERANDO:

Que, el artículo 194 de la Constitución Política del Perú, establece que los Gobiernos Locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia, siendo que conforme al artículo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, "Los Gobiernos Locales gozan de autonomía política, económica y administrativa en asuntos de su competencia, cuya autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico";

Que, el numeral 6) del Articulo 20°de la Ley N° 27972 Ley Orgánica de Municipalidades, establece como atribución del Alcalde, el de dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas; asimismo el Artículo 43, preceptúa que las resoluciones de alcaldía aprueban y resuelven los asuntos de carácter administrativo;

Que, los numeral e 2) y 2.1 del Título III de las normas de Control Interno, aprobadas por Resolución de Contraloría, aprobada por resolución de Contraloría N°320-2006/CG, establece que la evaluación de riegos es parte del proceso de administración de riesgos que debe ser ejecutado en todas las entidades y que incluye el planeamiento de la administración de riegos, que es el proceso de desarrollar y documentar una estrategia clara, organizada e interactiva para identificar y valorar riesgos que puedan impactar en una entidad impidiendo el logro de los objetivos, para lo cual se deben desarrollar planes, métodos de respuesta y monitoreo de cambios, así como un programa para la obtención de los recursos necesarios para definir acciones en respuesta a riesgos;

Que, a su vez en el inciso 7 del numeral 3.10 "Controles para las Tecnologías de la Información y Comunicación", de las citadas normas de Control Interno, se indica que para el adecuado ambiente de control en los sistemas informativos, se requiere que estos sean preparados y programados con anticipación para mantener la continuidad del servicio y que para ello se debe elaborar, mantener y actualizar periódicamente un Plan de Contingencia debidamente autorizado y aprobado por el titular o funcionario designado, donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia, así como se tiene otras normas conexas que promueven la implementación de mecanismos para mejorar la seguridad de la información;

Que, el Decreto de Urgencia N°006-2020 Decreto de urgencia que se crea el Sistema Nacional de Transformación Digital, en su artículo 5° , indica que el Sistema Nacional de Transformación Digital tiene por finalidad lo siguiente: 1.-*Formentar e impulsar la transformación digital de las entidades públicas, las empresas privadas y la sociedad en su conjunto, fortalecer el uso efectivo de las tecnologías digitales, las redes y los servicios digitales por parte de los ciudadanos y personas en general. 2.- Impulsar la innovación digital, el fortalecimiento de una sociedad digital inclusiva y el ejercicio de una ciudadanía digital con deberes y derechos digitales de los ciudadanos. 3.- Promoverla economía digital, la competitividad, productividad e inclusión financiera en una sociedad digital. 4.- Fortalecer el acceso y la inclusión a las tecnologías digitales en el país y la confianza digital fomentando la seguridad, transparencia, protección de datos personales y gestión ética de tecnologías en el entorno digital para la sostenibilidad, prosperidad y bienestar social y económico del país;*

Que, el Decreto de Urgencia N°007-2020 Decreto de urgencia que aprueba el Marco de Confianza Digital y Dispone Medidas para su fortalecimiento, en el artículo 1° Objeto indica que, "*El presente Decreto de urgencia tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional*";

Asimismo, mediante Decreto Supremo N°118-2018-PCM, que declara de interés nacional las estrategias, acciones actividades e iniciativas para el desarrollo del gobierno digital la innovación y la economía digital;

Que, el 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;

Que, mediante Informe N° 0213-2024-MAAQ/OTIC-MPLC, de fecha 25 de septiembre de 2024, el Jefe de la Oficina de Tecnologías de la Informacion y Comunicaciones Ing. Marco Antonio Auccapuma Quispe, solicita a la Directora de Administración Abg. Zoraida Llerena Delgado, la evaluación y aprobación del "**Plan de Contingencia Informático de La Municipalidad Provincial de La Convención 2024-2026**", mediante acto resolutivo, con la finalidad de garantizar el buen funcionamiento de los equipos de OTIC, sistema de información y software, dispositivos que son parte de la infraestructura tecnológica, la unidad de estadística e información de la Municipalidad Provincial de La Convención, buscando la prevención y mitigación de los riegos y cualquier otro inconveniente;

RESOLUCIÓN DE ALCALDÍA N°563-2024-MPLC.

Que, mediante Informe N° 1651-2024-ZLLD-MPLC, de fecha 26 de septiembre de 2024, la Directora de la Oficina General de Administración Abg. Zoraida Llerena Delgado, remite al Director de la Oficina General de Planeamiento y Presupuesto Econ. John Vargas Muñiz, la propuesta del "**Plan de Contingencia Informático de La Municipalidad Provincial de La Convención 2024-2026**", alcanzado por la Oficina de Tecnologías de la información y Comunicaciones, para su previa revisión y emisión del informe técnico correspondiente para que sea aprobado mediante acto resolutivo, teniendo en cuenta que uno de más importantes activos de toda institución es la información que esta genera en sus diferentes acciones y ámbitos;

Que, con Informe N° 360-2024-OPM-OGPP-MPLC/LC, de fecha 14 de octubre de 2024, el Jefe de la Oficina de Planeamiento y Modernización Econ. Edison Ayala Vera, se dirige al Econ. John Vargas Muñiz Director de la Oficina General de Planeamiento y Presupuesto, para señalar que, evaluado el "**Plan de Contingencia Informático de La Municipalidad Provincial de La Convención 2024-2026**", solicita se derive a la Oficina General de Asesoría Jurídica, para su opinión legal correspondiente para su aprobación mediante acto resolutivo;

Que, mediante Informe N° 0633-2024-JVM/OGPP-MPLC, de fecha 14 de octubre del 2024, emitido por el Director de la Oficina General de Planeamiento y Presupuesto Econ. John Vargas Muñiz se dirige al Director de la Oficina General de Asesoría Jurídica Abog. Paul Jean Barrios Cruz, para solicitar opinión legal correspondiente para la aprobación del "**Plan de Contingencia Informático de La Municipalidad Provincial de La Convención 2024-2026**", mediante acto resolutivo;

Que, mediante Informe Legal N° 1148-2024-OGAJ-MPLC, de fecha 22 de octubre de 2024, emitido por el Director de la Oficina General de Asesoría Jurídica Abog. Paul Jean Barrios Cruz, **opina** que, es **PROCEDENTE APROBAR**, el "**PLAN DE CONTINGENCIA INFORMÁTICO DE LA MUNICIPALIDAD PROVINCIAL DE LA CONVENCIÓN 2024-2026",** el mismo que cuenta con **Cuarenta y Siete (47) folios**, cuya finalidad es garantizar la continuidad de los servicios de tecnología de información y comunicaciones de la municipalidad Provincial la Convención (MPLC), a fin de que se establezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento; presentado por el Jefe de la Oficina de Tecnologías de Información y Comunicaciones Ing. Marco Aurelio Auccapuma Quispe mediante Informe N° 0213-2024-MAAQ/OTIC-MPLC;

Que, mediante Proveído N° 005885, con fecha de recepción 22 de octubre de 2024, Gerencia Municipal, dispone la emisión del Acto Resolutivo correspondiente;

Por las consideraciones expuestas y en uso de las atribuciones conferidas por el Artículo 20°, Inciso. 6) y Artículo 43°, de la Ley N° 27972 Ley Orgánica de Municipalidades, sus modificatorias y demás normas vigentes;

RESUELVE:

ARTICULO PRIMERO. –APROBAR, el "**PLAN DE CONTINGENCIA INFORMÁTICO DE LA MUNICIPALIDAD PROVINCIAL DE LA CONVENCIÓN 2024-2026"**; el mismo que cuenta con **Cuarenta y Siete (47) folios**, cuya finalidad es garantizar la continuidad de los servicios de tecnología de información y comunicaciones de la municipalidad Provincial la Convención (MPLC), a fin de que se establezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento; en merito al Informe N° 0213-2024-MAAQ/OTIC-MPLC.

ARTICULO SEGUNDO. - ENCARGAR, a Gerencia Municipal, Oficina de Tecnologías de la Información y Comunicaciones Oficina de Planeamiento y Modernización, Oficina General de Planeamiento y Presupuesto, Oficina General de Administración, y demás áreas competentes de la Municipalidad adopten las acciones necesarias para el cumplimiento e implementación de la presente Resolución de Alcaldía en estricta observancia a las normas legales.

ARTICULO TERCERO. - NOTIFICAR, la presente Resolución de Alcaldía a Gerencia Municipal, Oficina de Tecnologías de la Información y Comunicaciones, Oficina de Planeamiento y Modernización, Oficina General de Planeamiento y Presupuesto, Oficina General de Administración, y demás órganos estructurales de la Municipalidad para su conocimiento y fines.

ARTÍCULO CUARTO. - ENCARGAR, a la Oficina de Tecnologías de la Información y Comunicaciones, la publicación de la presente Resolución de Alcaldía en el Portal Web de la Municipalidad (https://www.gob.pe/munilaconvencion).y en el Portal de Transparencia de la Entidad.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

CC.
ALCALDIA.
GM.
OGPP
OPLTOyM
OGA
OTIC.
ARCHIVO.

MUNICIPALIDAD PROVINCIAL DE LA CONVENCIÓN
Dr. ALEX CURI LEON
ALCALDE PROVINCIAL
DNI: 23984679

PLAN DE CONTINGENCIA INFORMÁTICO DE LA MUNICIPALIDAD PROVINCIAL DE LA CONVENCIÓN 2024-2026

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

2024

PLAN DE CONTINGENCIA INFORMATICO

ÍTEM	MIEMBRO	CARGO
1	LÍDER DE GOBIERNO DIGITAL	GERENTE MUNICIPAL
2	COMITÉ DE GOBIERNO DIGITAL	JEFE DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
3		JEFE DE LA OFICINA DE GESTIÓN DE RECURSOS HUMANOS
4		JEFE DE LA OFICINA DE ATENCIÓN AL CIUDADANO Y GESTIÓN DOCUMENTARIA
5		DIRECTOR DE LA OFICINA GENERAL DE ASESORÍA JURÍDICA
6		DIRECTOR DE LA OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO
7		RESPONSABLE DE SISTEMAS Y PORTAL INSTITUCIONAL

INTRODUCCIÓN

El presente documento contiene el Plan de Contingencia de la Municipalidad Provincial de La Convención, elaborado por la Oficina de Tecnología de la Información y Comunicaciones. Establece los objetivo, alcance y metodología desarrollada. Incluye, además, las definiciones utilizadas, políticas de seguridad, análisis situacional, análisis de sensibilidad de la información manejada, identificación de los riesgos y controles, y la clasificación de activos de OTI.

De igual modo, la metodología aplicada a la identificación de riesgos, calificación de la probabilidad de ocurrencia de un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias. Permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución eficiente.

Uno de los más importantes activos de toda institución es la información que está genera en sus diferentes acciones y ámbitos. Conscientes de esta premisa, podemos indicar que se debe adoptar medidas de seguridad para la información y así mismo estar preparados para poder afrontar contingencias y desastres de tipo diverso.

Ahora bien, la Oficina de Tecnología de la Información y Comunicaciones, en adelante OTIC, tiene, entre otros, el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a ello presenta el Plan de Contingencia Informático de la Municipalidad Provincial de La Convención.

Finalmente, El Plan de Contingencias Informático está basado en la realidad que manifiesta la Municipalidad Provincial de La Convención (MPLC), y puede servir como punto de partida hacia la adecuación y establecimiento de políticas tanto en la Municipalidad como en las diferentes oficinas. Un Plan de Contingencias debe ser diseñado y elaborado de acuerdo con las necesidades y realidad de cada institución, tener sus propios requerimientos, tener que adoptar un sitio especial para el procesamiento de la información o hasta tener que construirlo o implementarlo, requerirá además de pruebas de procedimientos nuevos y que sean compatibles con los procesos existentes, incluso muchas veces se requerirá contar con la participación de personal de otros departamentos o áreas para trabajar en conjunto cuando se desarrollen o implementen soluciones.

1. PLAN DE CONTINGENCIA

Para la Municipalidad Provincial de La Convención es indispensable recurrir a los recursos informáticos y tecnológicos como un medio para procesar y proveer información a todas las áreas, y es fundamental que dicha información sea lo más exacta, confiable y oportuna. También es importante mencionar que estos recursos informáticos y tecnológicos son los encargados de procesar la información de los sistemas gubernamentales como el SIAF, SIGA, SEACE, SD PLANILLAS, SIADEG, SISTEMA INTEGRAL DE RECAUDACION PARA LA UNIDAD DE RENTAS E IMPUESTOS Y CORREO INSTITUCIONAL, imprescindibles para las gestiones administrativas de la Municipalidad Provincial de La Convención.

Es importante resaltar que para lograr nuestros objetivos institucionales es necesario definir tiempos de disponibilidad máximos, tanto en sus recursos informáticos como en las comunicaciones; de este modo podrá mantener una contingencia eficiente en todas las áreas operativas.

Por todo lo anteriormente manifestado, al no contar con equipos informáticos en óptimas condiciones, por un lapso mayor origina distorsiones al funcionamiento normal de nuestros servicios y mayores costos de operación. De continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar las operaciones por falta de datos e información para la operatividad, control y toma de decisiones de la institución.

Es necesario, por tanto, prever cómo actuar y qué recursos necesitamos ante una situación de contingencia, con el objeto de que su impacto en la reposición de las actividades sea lo más eficiente posible. Cabe señalar que la Municipalidad Provincial de La Convención, ingresa en una situación de contingencia cuando el equipo informático falla, afectando los servicios institucionales y termina cuando se restablecen dichos servicios.

2. FINALIDAD

Garantizar la continuidad de los servicios de tecnología de información y comunicaciones de la Municipalidad Provincial La Convención (MPLC), a fin de que se restablezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

3. OBJETIVOS

3.1 Objetivo General:

Definir normas y procedimientos necesarios para afrontar dificultades que se presenten en los equipos de cómputo, sistemas de información y comunicación en la Municipalidad Provincial La Convención de modo que se asegure la continuidad, seguridad y confiabilidad de los mismos.

3.2 **Objetivos Específicos:**

- Identificar, evaluar y proteger los servicios que brinda la Municipalidad Provincial La Convención, de riesgos potenciales que perjudiquen la continuidad de las operaciones y procesos informáticos desarrollado por los trabajadores.
- Establecer actividades de planeamiento, preparación, capacitación y ejecución de tareas, con la finalidad de proteger y garantizar la óptima funcionalidad de los servicios informáticas, contra cualquier corte de servicio, o fenómeno natural.
- Implementación de políticas y directivas de procesos que permitan la restauración de los servicios brindados por la Municipalidad Provincial La Convención, en el menor tiempo posible.
- Determinar acciones que permitan evaluar el avance, logros y resultados obtenidos con la ejecución del plan de contingencia y permitan a su vez realizar los cambios necesarios.
- Establecer actividades que contribuyan al cumplimiento de objetivos institucionales y garanticen al ciudadano la continuidad de los servicios informáticos brindados por la Municipalidad Provincial La Convención.
- Contar con personal debidamente capacitado y organizado que afrontar adecuadamente las contingencias que se puedan presentar y perjudiquen la continuidad de los servicios y procesos informáticos.

4. ALCANCE

El Plan de Contingencia Informático de Tecnología de la Información y Comunicaciones, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la Entidad.

5. BASE LEGAL

5.1. **Ley N°27658** – Ley Marco de Modernización de la Gestión del Estado.

Art 1: Declárase al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano.

5.2. Ley N°27269 – Ley de Firmas y Certificados Digitales.

Art 1: La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte

con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

5.3. Ley N°31572, Ley del Teletrabajo. Ley N°29733, Ley de Protección de Datos Personales.

5.4. Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

5.5. Decreto Legislativo N°604, Ley de Organizaciones y Funciones del INE.

5.6. Decreto Supremo N°033-2018-PCM, se crea la Plataforma Digital Única del Estado Peruano.

5.7. Decreto de Urgencia N°006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

5.8. Decreto de Urgencia N°007-2020-PCM, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

5.9. Decreto Supremo N°118-2018-PCM, que declara de interés nacional las estrategias, acciones, actividades e iniciativas para el desarrollo del gobierno digital, la innovación y la economía digital en el Perú con enfoque territorial.

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°157-2021-PCM, Reglamento del Decreto de Urgencia N°006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital. Decreto Supremo que aprueba el Reglamento del Decreto de Emergencia N°006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, Decreto Supremo N°157- 2021-PCM.

5.12. Decreto Supremo N°103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.

5.13. Decreto Supremo N°003-2013-JUS, que aprueba el Reglamento de la Ley N°29733, Ley de Protección de Datos Personales.

5.14. Decreto Supremo N°002-2023-TR, Decreto Supremo que aprueba el Reglamento de la Ley N°31572, Ley del Teletrabajo.

5.15. Decreto Supremo N°026-2016-PCM, que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado.

5.16. Decreto Supremo N°052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales.

5.17. Resolución Ministerial N°004-2016-PCM, Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

5.18. Resolución Ministerial N°119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.

5.19. Resolución Ministerial N°087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.

5.20. Resolución de Secretaría de Gobierno y Transformación Digital N°003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Seguridad de la Información en las Entidades Públicas.

5.21. Resolución Directoral N°022-2022-INACAL/DN, que aprueba, entre otras, 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. 3ra. Edición. Reemplaza a la NTP-ISO/IEC 7001:2014.

6. MARCO TEORICO

6.1. PLAN DE CONTINGENCIA INFORMÁTICO

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

- Antes, como un plan de prevención para 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.

6.2. INCIDENTE

Circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en la MPLC.

6.3. MÉTODO DE ANÁLISIS DE RIESGOS

Los 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.

6.4. PLAN DE PREVENCIÓN

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan. El plan de prevención es la parte principal del Plan de Contingencia porque, permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

6.5. PLAN DE EJECUCIÓN

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentre disponible. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

6.6. PLAN DE RECUPERACIÓN

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

6.7. PLAN DE PRUEBAS

Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

7. METODOLOGÍA

El desarrollo del presente Plan seguirá la siguiente metodología basada en siete (7) fases:

- Fase 1: Planificación.
- Fase 2: Determinación de vulnerabilidades y escenarios de contingencia.
- Fase 3: Estrategias.
- Fase 4: Elaboración del Plan de Contingencia Informático.
- Fase 5: Definición y Ejecución del Plan de Pruebas.
- Fase 6: Implementación del Plan de Contingencia.
- Fase 7: Monitoreo.

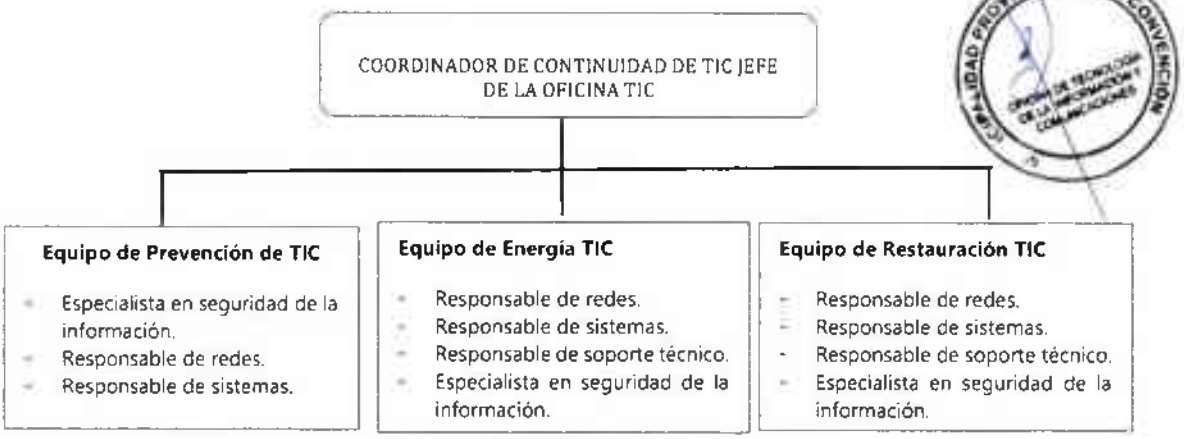
7.1. FASE 1: PLANIFICACIÓN

7.1.1. ORGANIZACIÓN

La Oficina de Tecnologías de la Información y Comunicaciones (OTIC) depende directamente de Gerencia Municipal (GM), y tiene dentro de sus funciones administrar la integridad, confiabilidad, y seguridad en el acceso a las bases de datos de la Entidad, así como establecer mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control de accesos a la base de datos; además de diseñar, desarrollar, implementar y mantener los sistemas informáticos e infraestructura tecnológica necesaria para el cumplimiento de los objetivos de la MPLC, así como asegurar la disponibilidad y brindar soporte a los mismos.

Para el funcionamiento del Plan de Contingencia Informático de Tecnologías de la Información y Comunicaciones, se ha establecido la siguiente organización operativa, conformado exclusivamente por personal de la OTIC:

Figura N° 1 – Organización Operativa del Plan de Contingencia Informático de Tecnologías de la Información y Comunicaciones (TIC)



El Jefe de la Oficina de Tecnologías de la Información y Comunicaciones debe nombrar un miembro titular y un alterno, por cada integrante de los tres (3) equipos mencionados previamente, detallados en la Figura N° 1. Para tal efecto, se debe contar con la relación del personal de la OTIC que forman estos equipos, quienes serán requeridos en el momento de la contingencia.

Asimismo, los responsables de cada Equipo previamente señalados, deben tener operativo su dispositivo móvil, para las comunicaciones pertinentes.

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o en remoto, conforme a los escenarios de prueba que pudieran desprenderse ante los diversos eventos de mayor impacto

considerados para el presente Plan de Contingencia Informático; así como, conforme a las disposiciones vigentes.

7.1.2. ROLES, FUNCIONES Y RESPONSABILIDADES DENTRO DEL PLAN

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia Informático de Tecnologías de la Información y Comunicaciones.

a. Coordinador de Continuidad de TIC

Está representado por el Director de la OTIC y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- Tomar la decisión de activar el Plan de Contingencia Informático de Tecnologías de la Información y Comunicaciones.
- Guiar y supervisar a los equipos operativos de contingencia informática, en el desarrollo de sus actividades.
- Evaluar la extensión de la contingencia y sus consecuencias potenciales sobre la infraestructura tecnológica.
- Notificar y mantener informados, a los miembros del Grupo de Continuidad Operativa, acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información (TI) en el Centro de Datos.
- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.
- Declarar el evento de término de la ejecución de las operaciones del Plan de Contingencia Informático de Tecnologías de la Información y Comunicaciones, cuando las operaciones del Centro de Datos hayan sido restablecidas.

b. Equipo de Prevención de TIC

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre. Su finalidad es evitar la materialización 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 responsable del Equipo de Prevención de TIC es el Especialista en Seguridad de la Información.

A continuación, se detallan las funciones por cada integrante del equipo de prevención:

Especialista en Seguridad de la Información

- Establecer y supervisar los procedimientos de seguridad de los servicios de TIC.
- Coordinar la realización de las pruebas de restauración de hardware y software.
- Participar en las pruebas y simulacros de desastres.
- Verificar la realización del mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Verificar las tareas de copias de respaldo (copias de seguridad).

Responsable de Redes

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del Centro de Datos, considerando el tiempo de vida útil y garantía de los mismos.
- Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del Centro de Datos.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
- Verificar que se mantiene actualizado los diagramas de servidores, los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones, el inventario de software de gestión y otros.
- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.

Responsable de Sistemas

- Soporte y mantenimiento de los sistemas y aplicativos instalados en la Entidad.
- Realizar periódicamente las pruebas de restauración de las fuentes de los sistemas de información en producción de la entidad.
- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la Entidad.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas.
- Realizar las pruebas de restauración de bases de datos en coordinación con el Especialista en Seguridad de la Información.

c. Equipo de Emergencia de TIC

Este equipo es el encargado de ejecutar las acciones requeridas durante la materialización del siniestro o desastre. Su finalidad es mitigar el impacto que puedan tener sobre los equipos tecnológicos y la información de la MPLC, procurando salvaguardar su pérdida o deterioro.
A continuación, se citan las acciones que se realizarán durante la contingencia, según los miembros del equipo:

Responsable de Redes

- Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.
- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados en el Centro de Datos de la MPLC.
- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos de la MPLC, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

Responsable de Sistemas

- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- Revisar las bitácoras de los aplicativos informáticos afectados durante la emergencia.
- Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.

Responsable de Soporte Técnico

- Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, impresoras, entre otros).
- Notificar los casos críticos en cuanto a equipos de usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios de la MPLC.

Especialista en Seguridad de la Información

- Asistir en las labores de verificación y validación de operación de los servicios de TIC.

d. Equipo de Restauración de TIC

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos de la MPLC.

Responsable de Redes

- Es el responsable del equipo de Restauración de TIC

- Debe iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos de la MPLC.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI y los equipos componentes del Centro de Datos de la MPLC.
- Notificar al Coordinador de Continuidad de TIC, las acciones de recuperación ejecutadas.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicaciones y los equipos componentes del Centro de Datos.

Responsable de Sistemas

- Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones de la MPLC.
- En caso se requiera, debe desplegar y/o reinstalar los aplicativos informáticos y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Verificar el funcionamiento de las bases de datos de la Entidad.
- Realizar la creación de bases de datos en servidores alternos, en caso sea necesario.
- Restaurar las copias de respaldo correspondientes, respetando la prioridad establecida para cada escenario.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y los datos de la MPLC, luego de efectuado el proceso de recuperación.

Responsable de Soporte Técnico

- Verificar el funcionamiento de los equipos personales en la MPLC.
- Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos personales e información del personal de la MPLC, luego de efectuado el proceso de recuperación.

Especialista en Seguridad de la Información

- Supervisar la restauración de los servicios de TI.
- Validar la información documentada de los procedimientos de restauración utilizados.

Cabe precisar que los equipos podrían ejecutar sus actividades paralelamente, de acuerdo al siguiente orden de operación:

Figura N° 2 – Flujo del orden de operación de los equipos de TI

7.2. FASE 2: DETERMINACIÓN DE VULNERABILIDADES Y ESCENARIOS DE CONTINGENCIA

En esta fase se procederá a la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de tecnologías de la información y comunicaciones, para los cuales se considerarán todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

7.2.1. PROCESOS Y RECURSOS CRÍTICOS

A continuación, se detalla los procesos, aplicaciones y recursos críticos, con su respectiva expectativa del tiempo de recuperación:

Tabla N° 1 – Procesos y recursos críticos de TI

Proceso crítico	Aplicaciones y/o recursos críticos	Tiempo de Recuperación (RTO)
Gestión de redes e infraestructura de TI	Equipos de comunicaciones	12 h
	Equipos de protección eléctrica del centro de datos (UPS)	24 h
	Sistema de aire acondicionado del Centro de Datos	24 h
	Infraestructura del Centro de Datos	24 h
	Cableado de red de datos	24 h
	Enlaces de cobre para interconexión de palacio municipal y el centro de datos	4 h
	Sistema de almacenamiento (NAS)	24 h
	Servidores de red críticos: Directorio Activo, SGD, SIAF, SIGA, SIADEG, Base de Datos	48h
	Servidores de red en general: Tomcat, Payara	48h
Gestión de sistemas de información y bases de datos	Sistemas de información y portales de la Entidad	48 h
	Sistemas de información administrativos	48 h
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	24 h
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	48 h
Operación y mantenimiento de TICS	Personal crítico responsable de los procesos de TIC.	4 h

* El RTO: Tiempo de Recuperación Objetivo, es determinado por Juicio de Expertos

7.2.2. IDENTIFICACIÓN DE AMENAZAS

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

Tabla N° 2 – Procesos y recursos críticos de TI

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo	Siniestros Naturales
02	Inundación y aniego en el Centro de Datos	
03	Incendio en el Centro de Datos	
04	Falla en telecomunicaciones	Tecnológicos
05	Delito informático	
06	Falla de hardware y software	
07	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de TI	Humanos
09	Pandemia y/o epidemia	Ambiental

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, 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:

Tabla N° 3 – Probabilidad estimada de las amenazas a los servicios de TI

N°	Amenaza (Evento)	Ocurrencia	Percepción	Nivel Probabilidad Estimado
01	Terremoto	2	2	Menor
02	Inundación y aniego en el Centro de Datos	2	2	Menor
03	Incendio en el Centro de Datos	1	3	Menor
04	Falla en telecomunicaciones	3	4	Moderado
05	Delitos informáticos	2	4	Moderado
06	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	3	3	Moderado
07	Falla del hardware y software	3	3	Moderado
08	Ausencia o no disponibilidad del personal crítico de TI	2	3	Menor
09	Pandemia y/o Epidemia	1	2	Menor

7.2.3. IDENTIFICACIÓN DE CONTROLES EXISTENTES

La identificación de controles existentes, permiten conocer que tan protegidos están los recursos de TI de la MPLC frente a cada amenaza.

- Acuerdos de niveles de servicio con el proveedor de enlace de comunicación donde se encuentra ubicado el Centro de Datos.
- Cámaras de vigilancia en el interior del Centro de Datos.
- Mantenimiento de UPS en el Centro de Datos debe incluir el cambio de baterías.
- Mantenimiento para equipos de aire acondicionado del Centro de Datos.
- Redundancia en los enlaces de comunicaciones (fibra óptica) y de internet.
- Sistema contra incendios en el Centro de Datos.
- Respaldo de información y custodia externa de medios de respaldo.
- Solución antivirus instalada en los servidores de red y computadoras.
- Solución de protección de portales y aplicaciones web publicadas en internet a través de solución en la nube.
- Póliza de seguro contra todo riesgo.

7.2.4. EVALUACIÓN DEL NIVEL DE RIESGO

Para determinar el Nivel de Riesgo de un recurso de TI crítico de la MPLC, se consideraron los controles existentes que mitigan la afectación de la amenaza

descritos en el punto 6.2.2 y de acuerdo a la aplicación de la metodología de riesgos descrita en el Anexo 1, se obtuvo el siguiente resultado:

Tabla N° 4 – Resultado de la evaluación de riesgos de los servicios de TI

	Recursos Críticos / Amenazas (Eventos)	Terremoto	Instalación y ataque en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Delitos informáticos	Falla del suministro eléctrico en el Centro de Datos y/o Sistema de comunicación	Falla de hardware y software	Ausencia del personal crítico del proceso (Unidad de TI)	Pandemia y/o Epidemia
1	Equipos de comunicaciones.									
2	Equipos de protección eléctrica del centro de datos (UPS).									
3	Aire acondicionado de precisión del Centro de Datos.									
4	Infraestructura del Centro de Datos.									
5	Cableado de red de datos.									
6	Enlaces de cobre y fibra óptica para interconexión entre la sede central y el Centro de Datos.									
7	Sistema de almacenamiento (NAS).									
8	Servidores de red									
9	Sistemas de información y portales web									
10	Base de datos utilizados por los sistemas y aplicativos.									
11	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)									
12	Personal crítico responsable de los procesos de TIC.									

7.2.5. ESCENARIOS DE RIESGO

- Destrucción e indisponibilidad del centro de datos por terremoto.
- Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
- Indisponibilidad de los servidores de red por falla de hardware y software.
- Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de palacio municipal.

A continuación, se presenta el consolidado de los escenarios de riesgo y su impacto, para activar el Plan de Contingencia Informático.

Tabla N° 5 – Escenarios de Riesgos

Escenario de Riesgo	Descripción	Impacto
Destrucción e Indisponibilidad del centro	Este escenario consiste en que el Centro de Datos deje de funcionar o se destruya, como resultado de un terremoto o incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el Centro de Datos, como también los componentes del mismo.	Extremo
Falla en el funcionamiento de los sistemas de información y portales web	Se refiere a la falla lógica o caída de los sistemas de información, aplicativos y portales web, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
Indisponibilidad de los servidores de red por falla de hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, lo cual produce que la información o servicios brindados por ellos, no estén disponibles.	Extremo
Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de palacio municipal.	Este escenario consiste en el corte o interrupción de las comunicaciones del Centro de Datos, así como los servicios publicados en Internet, como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como el corte de energía eléctrica, lo cual ocasionará caídas de los servicios informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	

7.3. FASE 3: ESTRATEGIAS DEL PLAN DE CONTINGENCIA

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre.

7.3.1. ESTRATEGIAS DE PREVENCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

a) Almacenamiento y respaldo de la información (COPIAS DE SEGURIDAD)

- Gestión de copias de respaldo (Copias de seguridad) de la información almacenada y procesada en el Centro de Datos, de acuerdo a la Directiva N° 001-2022-MPLC, en donde se define los respaldos de información.
- Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.
- Se utiliza lugares alternativos externos para el almacenamiento de las copias de respaldo.

b) Sitios Alternos para el Centro de Datos

El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; los sitios alternativos podrán ser:

- Biblioteca Municipal
- Central de Seguridad Ciudadana

Para tal efecto, se debe identificar un ambiente adecuado como lugar alterno para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.

c) Evaluación y gestión de proveedores

- Listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto actualizados.
- Mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.
- 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.
  - Equipo compatible existente: Equipo existente en sitios alternativos.

Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación. Asimismo, almacenar un equipo sin ser usado es costoso, pero permite que la recuperación inicie en el menor tiempo posible.

d) Entrenamiento y personal de reemplazo

- Todo el personal de la OTIC, debe entrenarse en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.
- Se debe elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OTIC, tales como, sistemas de información, redes y comunicaciones, soporte, así como seguridad de la información.

- Elaboración de una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

e) Renovación tecnológica

- Programación de una revisión anual de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
- Registrar las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, para en base a las estadísticas de este registro, se proceda a adquirir equipos de contingencia.

f) Activación de trabajo remoto

- Verificación y validación de acceso seguro, en remoto, a los sistemas y servicios de tecnología de información y comunicaciones.
- Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse cuente con los mecanismos de seguridad informáticos necesarios.
- En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le pueda habilitar el equipo asignado, que se encuentra en la sede de la MPLC, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la Unidad de Patrimonio.
- Verificación de los accesos seguros de los proveedores a cualquier elemento de la plataforma e infraestructura de servicios de tecnología de información y comunicaciones, a cargo de la OTIC en el Centro de Datos.

7.3.2. ESTRATEGIA FRENTE A EMERGENCIAS EN TECNOLOGÍAS DE LA INFORMACIÓN

El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información de la MPLC y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre. A continuación, se citan las acciones que se realizarán durante y después de una contingencia:

Acciones durante la contingencia

- Estudiar y evaluar el alcance del desastre en cada área de responsabilidad.
- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC.

- Informar al responsable del Grupo de Continuidad Operativa sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación del sitio alterno o de respaldo.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Estudiar y evaluar la dimensión de los daños a los equipos y sus facilidades, y elaborar un informe de los daños producidos.
- Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

7.3.3. ESTRATEGIA PARA LA RESTAURACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos de la MPLC para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo cual se definen las pautas que permitan al personal de la OTIC 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° 3 – Ciclo de la estrategia de recuperación de TI

La priorización de la restauración de los servicios de tecnologías de información de la MPLC se ejecutará de acuerdo a lo indicado en la siguiente Tabla de información:

Tabla N° 6 – Prioridad de atención durante la restauración de TIC

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. Ejemplo: Sistema de Gestión Documental (SGD), Sistema Administrativo Financiero (SIAF), Sistema Integrado de Gestión Administrativa (SIGA), Servidores de bases de datos, entre otros.
2	Atención normal: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.
3	Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo, equipos de apoyo. Ejemplo: Intranet, Sistema de soporte informático, etc.

En el Anexo 2 y Anexo 3 se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática.

Acciones después de la contingencia

- Evaluar el trabajo de los equipos durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Contingencia.
- Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

7.4. FASE 4: ELABORACIÓN DEL PLAN DE CONTINGENCIA Y RECUPERACIÓN DE SERVICIOS DE TIC

Una vez identificados los eventos de contingencia y los escenarios de riesgos, se desarrollan los Planes de Contingencia agrupados por las categorías indicadas previamente.

El Plan de Contingencia y Recuperación de los Servicios de Tecnología de la Información y Comunicaciones comprenderá los eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N° 7 – Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo	Formato Plan de Contingencia
1	Terremoto/Sismo	Extremo	FPC - 01
2	Delito informático (ataque)	Extremo	FPC - 02
3	Falla de hardware y software	Extremo	FPC - 03
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Alto	FPC - 04

En el Anexo 4 se presenta el desarrollo de cada formato.

7.5. FASE 5: DEFINICIÓN Y EJECUCIÓN DEL PLAN DE PRUEBAS

El plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos sí pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por los equipos operativos de la OTIC, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

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

Las pruebas relacionadas a este plan, se deberán ejecutar semestralmente, en los meses de junio y diciembre, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado en el Anexo N° 05.

7.6. FASE 6: IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA

La implementación del presente plan se realizará en a partir del segundo mes de su aprobación.

Para tal efecto, el Oficial de Seguridad de la Información, realiza las siguientes funciones:

- Supervisar las actividades de copias de respaldo y restauración.
- Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información (TI).

- Participar en las pruebas y simulacros de desastres.

7.7. FASE 7: MONITOREO

La fase de Monitoreo permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva.

A continuación, se enumeran las actividades principales a realizar:

- Realizar mantenimiento de la documentación técnica de operación de los servicios de TI.
- Revisión continua de las aplicaciones, sistemas de información y portales web.
- Revisión continua del sistema de copias de respaldo (copias de seguridad).
- Revisión y mantenimiento de los sistemas de soporte eléctrico del Centro de Datos.

ANEXOS

- Anexo 1 Metodología aplicada a la gestión de riesgos.
- Anexo 2 Listado de aplicaciones y sistemas de información clasificados por prioridad de
- Anexo 3 Listado de equipos del Centro de Datos y Gabinetes de Comunicación clasificados
- Anexo 4 Formatos del Plan de Contingencia Informático de Tecnologías de la Información y Comunicaciones por evento de riesgo.
- Anexo 5 Formato de Control y Certificación de las Pruebas del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

ANEXO 1

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 a la MPLC 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	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% o <=10% de probabilidad, o • Puede ocurrir pero no será anticipada
3	Mediana	• >10% o <=50% de probabilidad, o • Puede ocurrir en el mediano plazo
4	Posible	• >50% o <=75% de probabilidad, o • Podría ocurrir anualmente
5	Muy Posible	• >75% o 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)
Moderada	Probabilidad de ocurrencia intermedia (Evaluación de prioridad baja)
	Probabilidad de ocurrencia muy baja (Evaluación sin prioridad)
Insignificante	No se cree que ocurra (Desestimar evaluación)

3. Calculo 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.
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	Interpretacion
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
	Riesgo aceptable con revisión de la dirección
Bajo	Riesgo aceptable sin revisión

ANEXO 2

LISTADO DE APLICACIONES Y SISTEMAS DE INFORMACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE OTIC

N°	SISTEMA APLICATIVO	BREVE DESCRIPCIÓN	AREA USUARIA	MOTOR DE BASE	TIPO	PRIORIDAD
1	SISTEMA DE GESTION DOCUMENTAL	Gestión de toda la documentación generada por todas las áreas de la MPLC, documentos ingresados por mesa de partes presencial y mesa de partes virtual.	MPLC	SQL Server	Web	1
2	SISTEMA DE SIADEG	Atención de los requerimientos de bienes y servicios.	MPLC	SQL Server	Escritorio	1
3	SISTEMA SIAF	Administrar las inversiones asignadas por el MEF.	Oficina General de Administración Oficina de Contabilidad Oficina General de Planeamiento y Presupuesto Oficina de Tesorería	FOXPRO	Escritorio	1
4	SISTEMA SIGA	Gestión de los requerimientos en la MPLC.	MPLC	SQL Server	Escritorio	1
5	SISTEMA DE RENTAS	Cobro de los arbitrios municipal.	Oficina de General de Administración Tributaria	SQL Server	Escritorio	2
6	SISTEMA DE TRÁNSITO VEHICULAR	Registro de papeleta de tránsito.	Sud Gerencia de Tránsito y Seguridad Vial	SQL Server	Escritorio	2
7	SISTEMA DE LICENCIA DE TRANSITO	generar licencia de conducir para vehículos menores.	Sud Gerencia de Tránsito y Seguridad Vial	SQL Server	Web	2
8	SISTEMA DE PLANILLAS	Gestión de la planilla de remuneración del personal de la MPLC.	Oficina de Gestión de Recursos Humanos	SQL Server	Escritorio	2
9	SISTEMA DE PATRIMONIO	Gestión de los bienes municipales.	Oficina de Control Patrimonial y Almacén	SQL Server	Escritorio	3
10	SISTEMA DE REGISTRO CIVIL	Registro de nacimiento, defunciones y matrimonios.	Oficina de General de Administración Tributaria	SQL Server	Escritorio	3
11	SISTEMA GEO REFERENCIAL	Mantener la base de catastro referencial al componente especial.	Gerencia de Desarrollo Urbano y Rural	SQL Server	Web	3
12	SISTEMA DE CONTROL DE ASISTENCIA	Control del personal que labora en la MPLC.	Oficina de Gestión de Recursos Humanos	SQL Server	Web	3

ANEXO 3

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y GABINETES DE COMUNICACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Tipo de Equipo	Rol	Descripción	Prioridad
1	Servidor	Controlador de Dominio	Servidor de dominio de red. (Directorio Activo, DNS) y Base de datos SQL Server.	1
2	Servidor	Aplicaciones	Servidor de aplicaciones de la MPLC.	1
3	Servidor	Aplicativo SGD	Base de Datos SQL Server.	1
4	Servidor	Aplicativo SIADEG	Base de Datos SQL Server.	1
5	Servidor	Aplicativo SIAF	Base de Datos FOXPRO.	1
6	Servidor	Aplicativo SIGA	Base de Datos SQL Server.	1
7	Servidor	Sistema de patrimonio	Base de Datos SQL Server.	3
8	Switch Core	Comunicaciones	Switch Core, y Cortafuegos	1
9	Switch Servidores	Comunicaciones	Switch de servidores	1
10	Cortafuegos	Seguridad	Gestión unificada de amenazas	1
11	UPS	Energía	Equipo de suministro eléctrico para servidores y equipos de comunicaciones	1
12	Aire acondicionado	Acondicionamiento	Aire acondicionado básico para el Centro de Datos	1
13	Servidor	Sistema de Planillas	Base de Datos SQL Server.	2
14	Servidor	Sistema de Patrimonio	Base de Datos SQL Server.	3
15	Servidor	Sistema de Registro Civil	Base de datos SQL Server.	3
16	Servidor virtual	Seguridad	Antivirus.	3
17	Servidor virtual	Aplicativo SIAF Copia	Base de Datos FOXPRO.	3

ANEXO 4

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO DE TIC

MPLC	Evento: Terremoto / Sismo	FPC - 01

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Los sismos son movimientos en el interior de la tierra, que generan una liberación repentina de energía, que se propaga en forma de ondas provocando el movimiento del terreno.

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

Infraestructura:

- Oficinas y/o Centro de Datos Principal

Recursos Humanos

- Personal de la entidad.

b) Objetivo

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

c) Entorno

Este evento puede afectar las instalaciones del Palacio Municipal y el Centro de Datos, al ubicarse en la misma ciudad.

d) Personal Encargado

El Grupo de Continuidad Operativa de la MPLC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones de la MPLC, el mismo que debe ser de conocimiento de todo el personal que labora en todas las oficinas.

- Realización de simulacros de evacuación con la participación de todo el personal de las distintas oficinas.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las salidas libres de obstáculos.
- Señalización de las zonas seguras y las salidas de emergencia.
- Funcionamiento de las luces de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

f) Acciones del Equipo de Prevención de TIC

- Evaluar en coordinación con el Grupo 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.
- 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

La contingencia se activará al ocurrir un sismo. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos relacionados antes del evento

- Tener la lista actualizada de los servidores.
- Mantenimiento del orden y limpieza de los ambientes del Palacio Municipal y Centro de Datos.
- Inspecciones semestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

c) Personal que autoriza la contingencia informática

El Coordinador de Continuidad de TIC.

d) Personal Encargado

Equipo de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar la señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal de la MPLC que labora en el área se encuentren bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento de la MPLC, para las acciones que deban ser efectuadas por ellos.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el Jefe de la OTIC deberá coordinar con el Gerente Municipal.

f) Duración

Los procesos de evacuación del personal de la MPLC deberán ser reducidos y demorar 5 minutos como máximo.

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

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado es el Coordinador 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 de la MPLC.

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.

En caso, el evento haya sido de considerable magnitud, se deberá:

- Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Movilizar los equipos de respaldo al sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado al Grupo de Continuidad Operativa.
- Restauración de los servicios y operaciones de TI en el sitio alterno. El Equipo de restauración de TIC restaurarán el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
    - ✓ Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
    - ✓ Verificar que las aplicaciones críticas se hayan recuperado y están funcionando correctamente.
    - ✓ Confirmar los puntos de recuperación de datos de las aplicaciones.
    - ✓ Verificar que las funcionalidades de comunicación están funcionando correctamente.
    - ✓ Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
    - ✓ Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.
- Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación

El Coordinador de Continuidad de TIC, presentará un informe al Grupo de Continuidad Operativa, explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El Coordinador de Continuidad de TIC desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo de Continuidad Operativa.

e) Proceso de Actualización

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

MPLC	Evento: Delito informático	FPC-[illegible]

1. PLAN DE PREVENCIÓN

a) Descripción del Evento

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (hacking) y/o malware.

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, rootkits, bootkits, rogues, etc.

Este evento incluye los siguientes elementos mínimos identificados por la MPLC, 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 de la MPLC

b) Objetivo

Restaurar la operatividad de los equipos y servicios después de eliminar los malware o reinstalar las aplicaciones dañadas.

c) Entorno

Este evento se puede darse en cualquiera de los servidores y estaciones de trabajo, ubicadas en el Centro de Datos y en el Palacio Municipal de la MPLC.

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.
- Restricción del acceso a Internet a las estaciones de trabajo que, por su uso no lo requieran.
- Eliminación o restricción de lectoras y/o quemadores de CD en estaciones de trabajo que no lo requieran.
- Inhabilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Ejecución de ataques de Hacking Ético por terceros especializados.

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.

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).

b) Procesos Relacionados Antes del Evento

Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estaciones de trabajo.

c) Personal que Autoriza la Contingencia

El Coordinador de Continuidad de TIC y el Oficial de Seguridad de la Información pueden activar la contingencia.

d) Personal Encargado

Equipo de Emergencia de TIC.

e) Descripción de las Actividades Después de activar Contingencia

- Desconectar o retirar de la red de datos de la MPLC, el servidor o la estación infectada o vulnerada.
- Verificar si el equipo se encuentra infectado, 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 posible 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.
- Realizar pruebas al sistema.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

f) Duración

La duración del evento no deberá ser mayor TRES HORAS en caso se confirme la presencia de un virus en estaciones de trabajo y de SEIS HORAS en servidores de red. Esperar la indicación del personal de soporte técnico para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El equipo de restauración de TIC, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el usuario responsable del mismo y/o Director del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de Actividades

Se informará al Jefe de la OTIC de la MPLC el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, controladores y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible (Restauración).
- Reinicio del servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red de la MPLC.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Solicitar la conformidad de la restauración realizada del equipo y/o sistema de información afectado.
- Comunicar el restablecimiento del servicio

En función a esto, el Oficial de Seguridad de la Información, tomará las medidas preventivas del caso enviando una alerta vía correo al personal de la MPLC.

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

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.

El personal Responsable de Técnico de Soporte y/o Responsable de Redes, según sea el caso, presentará un informe al Jefe de la OTIC, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso del Coordinador de Continuidad de TIC de la MPLC, se desactivará el presente Plan.

e) Proceso de Actualización

El problema de infección o alteración presentado en la estación de trabajo y/o servidor de red, en base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

MPLC	Evento: Falla de hardware y software	FPC - 03

1. PLAN DE PREVENCIÓN

a) Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad.

El software

En ausencia del mismo, los sistemas de información que dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos
- NAS

Software

- Aplicativos usados por la MPLC y de servicio al ciudadano Información
- Información contenida en base de datos.
- Información contenida en repositorios de información

b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados de las imágenes de los servidores o máquinas virtuales en producción.

c) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones de la MPLC.

d) Personal Encargado

Equipo de Prevención de TIC.

e) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (bitácoras) de los servidores, para prevenir mal funcionamiento de los mismos.
- Contar con las copias de seguridad, diarias de datos de las aplicaciones en desarrollo/producción de la entidad.
- Contar con las copias mensuales de las imágenes de los servidores.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.
- Disponer de servidores de bases de datos de contingencia, con la instalación del motor de base de datos.
- Disponer de servidores de Aplicaciones de contingencia, con software de instalación tomcat, payara.

f) Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.

- 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.
- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datos para su correcto funcionamiento.
- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b) Procesos Relacionados antes del evento

Disponibilidad de las copias de respaldo.

Disponibilidad de instaladores de sistemas operativos y motor de base de datos.

c) Personal que autoriza la contingencia

El Coordinador de Continuidad de TIC debe activar la contingencia.

d) Descripción de las actividades después de activar la contingencia

- Realizar la revisión del servidor averiado, buscando un recurso de reemplazo verificando que dicho equipo cuente con garantía, de lo contrario se implementará un nuevo servidor virtual configurado de acuerdo a lo requerido.
- Solicitar las copias de respaldo para proceder a la restauración de la información almacenada en el servidor averiado.

e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las seis (6) horas.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El Equipo de Restauración de TIC, luego de validar la corrección del problema de acceso a los servidores, y el Coordinador de Continuidad de TIC, informará a los responsables de áreas, para la reanudación de las operaciones.

b) Descripción de actividades

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falla de los servidores.

Se debe realizar como mínimo las siguientes actividades:

- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, controladores y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- Proceder a la restauración de las copias de respaldo, de la información de los servidores afectados.
- Verificar que la data y los aplicativos se hayan restaurado correctamente.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Brindar los permisos de acceso a los usuarios finales.
- Remitir un mensaje electrónico a los usuarios de la MPLC, informando la reanudación de los servicios.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se registrará el incidente en el Sistema de Gestión de Ticket de Soporte de la OTIC, precisando las acciones realizadas.

El Responsable de Redes, presentará un informe al Jefe de la OTIC, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso del Coordinador de Continuidad de TIC, se desactivará el presente plan.

e) Proceso de Actualización

En base al informe presentado por el Responsable de Redes, quien identifica las causas de la pérdida o fallas de la base de datos institucional, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.

En caso existiese información pendiente de actualización, el Responsable de Redes deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

MPLC	Evento: Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	FPC - 04

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.

Este evento incluye los siguientes elementos mínimos identificados por la MPLC, 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 (NAS)
- Estaciones de Trabajo
- Equipos de Comunicaciones

Equipos Diversos

- UPS
- Aire acondicionado

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Entorno

Este evento puede darse en cualquiera de las instalaciones de la MPLC, considerando las oficinas externas y el palacio municipal 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

La Oficina de Abastecimiento de la OGA y el Jefe de la OTIC, son los responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica. El Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones de la MPLC, se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos consideradas como críticos.
- Equipos UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 30 minutos como mínimo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.

- Capacidad de los UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.
- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones de la MPLC (puertas, contactos magnéticos, etc.)
- Verificación del cableado eléctrico de palacio municipal y todas las oficinas externas de la MPLC, una vez por año.
- 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, aire acondicionado de precisión del Centro de Datos, UPS, transformador y del gabinete de baterías de acuerdo a la necesidad.
- 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 de la MPLC.

2. PLAN DE EJECUCIÓN

a) **Eventos que activan la Contingencia**

Corte de suministro de energía eléctrica en los ambientes de la MPLC.

b) **Procesos Relacionados antes del evento**

Cualquier actividad de servicio dentro de las instalaciones.

c) **Personal que autoriza la contingencia**

La OGA y/o el Jefe de la Oficina de Tecnología de la Información y Comunicaciones - OTIC pueden activar la contingencia.

d) **Descripción de las actividades después de activar la contingencia:**

- Informar al Jefe de la Oficina de Abastecimientos el 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 áreas de la MPLC y coordinar las acciones necesarias.
- En el caso de los equipos que, entren en funcionamiento automático con UPS, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.
- En caso la interrupción de energía en el Centro de Datos sea mayor a treinta (30) minutos, se deberán apagar los equipos en forma ordenada mientras funcione el UPS, hasta que regrese el fluido eléctrico.

e) **Duración**

El tiempo máximo de duración de la contingencia dependerá del proveedor externo 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:

- ✓ Equipos de Comunicaciones (enrutador, conmutadores principales, conmutadores de acceso)
- ✓ Servidores físicos por orden de prioridad
- ✓ Servidores virtuales por orden de prioridad
- ✓ Equipos de almacenamiento (NAS)

- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación

El Responsable de Redes presentará un informe al Jefe de la OTIC, explicando que parte del servicio, equipos u operaciones de tecnología de la información han fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Este informe deberá ser elevado al Grupo de Continuidad Operativa de la MPLC.

d) Desactivación del Plan de Contingencia

El Coordinador de Continuidad de TIC desactivará el Plan de Contingencia una vez que se recupere la funcionalidad del suministro eléctrico y la operatividad de los sistemas y servicios de tecnología de la información.

e) Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

ANEXO 5

FORMATO DE CONTROL Y CERTIFICACION DE LAS PRUEBAS

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

Prueba N°

Escenario de Prueba: (Descripción del escenario a probar / certificar)

Área Responsable: (Área responsable del escenario de prueba a probar / certificar)

INFORMACION DEL PROCESO

Metodología: (Detallar lo que se va a realizar en la prueba)

Alcance:

Condiciones de Ejecución: Equipo: (Nombre / Servidor / PC de prueba) Aplicación/Software:

Ubicación: (Lugar de prueba) Fecha de Backup:

RESULTADO DE LA PRUEBA

Resultado: Satisfactorio: ☐ Satisfactorio con Observaciones: ☐ Deficiente: ☐

Observaciones:

ACTUALIZACION EN EL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia:

ACTUALIZACION PARTICIPANTES

Participante	Cargo	Firma Digital