RESOLUCIÓN DE GERENCIA MUNICIPAL N° 064-2025-MDLP/GM

La Perla, 21 de marzo de 2025

VISTOS:

Memorándum N°D000283-2024-MDLP/GSC de fecha 26 de diciembre de 2024, Memorándum N°D002459-2024-MDLP/OGPP de fecha 26 de diciembre de 2024, Memorándum N°D00286-2024-MDLP/GSC de fecha 27 de diciembre de 2024, Memorándum N°D000235-2024-MDLP/SGGRD de fecha 27 de diciembre de 2024, Informe N°D00019-2025-MDLP/OTI de fecha 21 de enero de 2025, Memorándum N°D00099-2025-MDLP/OGA de fecha 22 de enero de 2025, Memorándum N°D000245-2025-MDLP/OGPP de fecha 03 de febrero de 2025, Informe N°D000181-2025-MDLP/OGAJ de fecha 18 de marzo de 2025 y;

CONSIDERANDO:

Que, la Constitución Política del Estado en su artículo 194°, modificado por la Ley N°30305, Ley de Reforma Constitucional, reconoce a las Municipalidades Distritales su calidad de Órganos de Gobierno Local con autonomía política, económica y administrativa en los asuntos de su competencia, en concordancia con lo señalado en el Art. 2° del Título Preliminar de la Ley N°27972 - Ley Orgánica de Municipalidades y, que dicha autonomía radica en la facultad de ejercer actos de gobierno, administrativo y de administración con sujeción al ordenamiento jurídico;

Que, mediante Ley N°29664 que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).

Que, mediante el Decreto Supremo N°060-2024-PCM, el mismo que aprueba la modificatoria del Reglamento de la Ley N°29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), aprobado por Decreto Supremo N°048-2011-PCM.

Que, en el numeral 6.1 de la Resolución Ministerial N°230-2021-PCM, indica que corresponde al Titular de la entidad: ***"d. Aprobar la conformación del Grupo de Comando, a propuesta de la unidad Orgánica responsable de la Gestión de la Continuidad Operativa. f. Aprobar el Plan de Continuidad Operativa y activarlo, cuando corresponda, y a propuesta del Grupo de Comando."***

Que, mediante Resolución de Alcaldía N°137-2024-MDLP/AL, se aprobó la conformación del "GRUPO DE COMANDO PARA LA GESTION DE LA CONTINUIDAD OPERATIVA". Encargado de formular, aprobar e implementar del Plan de Continuidad Operativa de la Municipalidad Distrital de La Perla, siguiendo los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de Gobierno.

Que, mediante Memorándum N°D000283-2024-MDLP/GSC de fecha 26 de diciembre de 2024, la Gerencia de Seguridad Ciudadana se dirige a la Oficina General de Planeamiento y Presupuesto a fin de solicitar la evaluación del informe técnico respecto a la aprobación del Plan de Continuidad Operativa de la Municipalidad Distrital de La Perla 2024-2026.

Que, mediante Memorándum N°D002459-2024-MDLP/OGPP de fecha 26 de diciembre de 2024, la Oficina General de Planeamiento y Presupuesto se dirige a la Gerencia de Seguridad Ciudadana a fin de devolver el Plan de Continuidad Operativa de la Municipalidad Distrital de la Perla 2025-2026 con la finalidad de que se adecue ya que se encuentra al termino del año fiscal puesto que sus ejecuciones se desarrollaran en virtud al Cronograma de Implementación de la Gestión de la continuidad operativa, el mismo que comenzara a desarrollarse el segundo trimestre del año 2025 y durara hasta el segundo trimestre del 2026.

Que, mediante Memorándum N°D000286-2024-MDLP/GSC de fecha 27 de diciembre de 2024, la Gerencia de Seguridad Ciudadana se dirige a la Sub Gerencia de Gestión del Riesgo de Desastres a fin de remitir el Memorándum N°D002459-2024-MDLP/OGPP de la Oficina General de Planeamiento y Presupuesto para su atención correspondiente.

Que, mediante Memorándum D°00235-2024-MDLP/SGGRD de fecha 27 de diciembre de 2024, la Sub Gerencia de Gestión del Riesgo de Desastres se dirige a la Oficina de Tecnología de la Información fin de actualizar el Plan de Contingencia Informático y continuidad de los servicios de Tecnología de Información y Comunicaciones de la Municipalidad Distrital de La Perla 2022-2024.

Que, mediante Informe N°D00019-2025-MDLP/OTI de fecha 21 de enero de 2025, la Oficina de Tecnología de la Información se dirige a la Oficina General de Administración a fin de remitir la actualización del Plan de Contingencia Informativo y Continuidad de Servicios de Tecnología de Información y Comunicaciones 2025-2026.

Que, mediante Memorándum N°D00099-2025-MDLP/OGA de fecha 22 de enero de 2025, la Oficina General de Administración se dirige a la Oficina General de Planeamiento y Presupuesto a fin de solicitar opinión técnica respecto a la aprobación Plan de Contingencia Informativo y Continuidad de Servicios de Tecnología de Información y Comunicaciones 2025-2026.

Que, mediante Memorándum N°D000245-2025-MDLP/OGPP de fecha 03 de febrero de 2025 la Oficina General de Planeamiento y Presupuesto se dirige a la Oficina General de Asesoría Jurídica a fin de solicitar opinión legal; asimismo, emitir opinión **FAVORABLE** al "Plan de Contingencia Informativo y Continuidad de los Servicios de Tecnología de Información y Comunicaciones de la Municipalidad Distrital de La Perla", el cual deberá ser aprobado mediante acto Resolutivo correspondiente previo informe legal.

Que, mediante Informe N°D00181-2025-MDLP/OGAJ de fecha 18 de marzo de 2025, la Oficina General de Asesoría Jurídica se dirige a la Gerencia Municipal a fin de remitir opinión legal sobre el Plan de Contingencia Informático y Continuidad de Servicios de Tecnología de Información y Comunicaciones.

(...) ANALISIS:

3.1. Que, el Artículo 194° de la Constitución Política del Perú establece que, las municipalidades provinciales y distritales son órganos de Gobierno Local, que tienen autonomía política, económica y administrativa en los asuntos de su competencia. En concordancia con éste se pronuncia el artículo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, que agrega que dicha autonomía radica en ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico, por lo que están sujetos a las leyes y disposiciones que, de manera general y de conformidad a la Constitución Política del Perú, regulan las actividades y funcionamiento del Sector Público, así como a las normas técnicas referidas a los sistemas administrativos del Estado que, por su naturaleza son de observancia y cumplimiento obligatorios.

3.2. Que, en atención al Informe Legal requerido por el despacho de la OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO, es necesario precisar el rol que ejerce la Oficina General de Asesoría Jurídica, en su función de asesorar sobre los alcances de la interpretación y correcta aplicación de las disposiciones constitucionales, legales y administrativas, es decir, el presente informe se circunscribe al carácter estrictamente legal, conforme así lo establece el artículo 57° del Reglamento de Organización y Funciones (ROF) de la Municipalidad Distrital de La Perla, no constituyéndose por tanto en un órgano de gestión sino de asesoramiento, que tiene por finalidad coadyuvar a dilucidar sobre una materia concreta a través de un informe en Derecho.

3.3. Que, el artículo 1° de la Ley N°29664, Ley del Sistema Nacional de Gestión del Riesgo de Desastres – SINAGERD, indica lo siguiente:

"Créase el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) como sistema interinstitucional, sinérgico, descentralizado, transversal y participativo, con la finalidad de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, y preparación y atención ante situaciones de desastre mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres".

3.4. De acuerdo al numeral 14.1 del artículo 14° de la ley antes señalada, establece que:

"...gobiernos locales, como integrantes del SINAGERD, formulan, aprueban normas y planes, evalúan, dirigen, organizan, supervisan, fiscalizan y ejecutan los procesos de la Gestión del Riesgo de Desastres, en el ámbito de su competencia, en el marco de la Política Nacional de Gestión del Riesgo de Desastres y los lineamientos del ente rector, en concordancia con lo establecido por la presente Ley y su reglamento".

3.5. Asimismo, con fecha 6 de junio de 2024, se aprobó el Decreto Supremo N° 060-2024-PCM, el mismo que aprueba la modificatoria del Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), aprobado por Decreto Supremo N°048-2011-PCM, donde el numeral 39.2 del artículo 39° del Decreto Supremo N°060-2024-PCM, indica que las gobiernos regionales y locales, de acuerdo a sus competencias, formulan, aprueban e implementa los siguientes planes específicos:

- *Plan de Prevención y Reducción del Riesgo*
- *Plan de Gestión Reactiva.*
- *Plan de Continuidad Operativa*

3.6. Asimismo, en el numeral 6.1.1 de la Resolución Ministerial N°320-2021-PCM, indica que corresponde al Titular de la entidad, lo siguiente:

"(...)
d. Aprobar la conformación del Grupo de Comandando, a propuesta de la unidad Orgánica responsable de la Gestión de la Continuidad Operativa.
f. Aprobar el Plan de Continuidad Operativa y activarlo, cuando corresponda, y a propuesta del Grupo de Comando."

3.7. Por consiguiente, mediante la Resolución de Alcaldía N° 137–2024–MDLP/AL, se aprobó la conformación del "GRUPO DE COMANDO PARA LA GESTIÓN DE LA CONTINUIDAD OPERATIVA". Encargado de formular, aprobar e implementar el Plan de Continuidad Operativa de la Municipalidad Distrital de La Perla, siguiendo los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de Gobierno.

3.8. Al respecto, mediante Memorándum N° D000245-2025-MDLP/OGPP de fecha 03 de febrero de 2025 la Oficina General de Planeamiento y Presupuesto expresa lo siguiente:

"Según las normas aprobadas de uso obligatorio en Técnicas de Seguridad en el Sistema de Gestión de Seguridad de la Información, la Municipalidad Distrital de La Perla, cuenta con un Plan de Contingencia Informático y Continuidad de los Servicios de Tecnología de Información y Comunicaciones desactualizado, por lo cual, la Oficina de Tecnología de la Información , propone el Proyecto del nuevo Plan 2025-2026, en virtud a la Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la recuperación y consolidación de la economía peruana"

la Normativa 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, el mismo que debe estar articulado al Plan de Continuidad Operativa de La Municipalidad Distrital de La Perla 2024 – 2026 de la Subgerencia de Gestión de Riesgo y Desastres".

3.9. Por consiguiente, es de necesidad aprobar el PLAN DE CONTINGENCIA INFORMÁTICO Y CONTINUIDAD DE SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES.

3.10. Al respecto de lo mencionado, de acuerdo con la Resolución de Alcaldía N° 77-2024-MDLP/AL se delegan las facultades a la Gerencia Municipal para aprobar los planes de la municipalidad.

(...) IV. <u>CONCLUSIÓN</u>:

*4.1 Estando a lo expuesto, y conforme a la normativa legal vigente, esta Oficina General de Asesoría Jurídica opina por la **PROCEDENCIA** del **PLAN DE CONTINGENCIA INFORMÁTICO Y CONTINUIDAD DE SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES.***

Por los fundamentos glosados y de conformidad con lo establecido por el Texto Único Ordenado de la Ley del Procedimiento Administrativo General N°27444, modificado por el Artículo 2° del Decreto Legislativo N°1272, aprobado mediante Decreto Supremo N°004-2019-JUS; Ley Orgánica de Municipalidades N°27972; y, en uso de las facultades conferidas por el ROF y la Resolución de Alcaldía N°085-2024-ALC/MDLP de fecha 18 de marzo de 2024.

<u>SE RESUELVE:</u>

ARTICULO PRIMERO: APROBAR el **PLAN DE CONTINGENCIA INFORMATIVO Y CONTINUIDAD DE SERVICIOS DE TECNOLOGIA DE INFORMACION Y COMUNICACIONES.**

ARTÍCULO SEGUNDO: DISPONER, a la Oficina de Tecnología de la Información, el cabal cumplimiento de la presente resolución.

ARTICULO TERCERO: DISPONER, la publicación de la presente Resolución en el Portal web de la Municipalidad Distrital de La Perla.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE

MUNICIPALIDAD DISTRITAL DE LA PERLA
GERENCIA MUNICIPAL
Abog. JOSE ARTURO PAATRESIERRA
GERENTE

MUNICIPALIDAD DE LA PERLA

PLAN DE CONTINGENCIA INFORMÁTICO Y CONTINUIDAD DE SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE LA PERLA

2025 - 2026

Tabla de contenido

INTRODUCCIÓN

El presente documento define el Plan de Contingencia Informática y Continuidad de servicios de Tecnologia de la Información y Comunicaciones 2025 – 2026 como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible contingencia que pueda presentarse en la Municipalidad Distrital de la Perla. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnología de la Información y Comunicaciones en el menor tiempo e impacto posible.

En tal sentido, y como buena práctica tecnológica, se ha elaborado el Plan de Contingencia Informático y recuperación de servicios de Tecnología de Información y Comunicaciones de la Municipalidad Distrital de la Perla, dado que la Institución pueda ser vulnerable a diferentes hechos que pueden interrumpir los servicios informáticos y afectar el normal funcionamiento de las actividades en la Institución, lo que no solo afecta a usuarios internos; sino también a usuarios externos. Asimismo, el Plan se encuentra alineado al Objetivo estratégico Institucional OEI.11 "Fortalecer la Eficiencia en la Gestión Institucional de la Municipalidad Distrital de la Perla", del Plan Estratégico Institucional (PEI) 2025 – 2030. Así, el presente plan establece los objetivos, el alcance y metodología del plan, con la finalidad de lograr minimizar el impacto negativo de la interrupción de los servicios informáticos, contribuyendo a que la Institución esté preparada ante cualquier eventualidad de contingencia a nivel de tecnología de información, toda vez que se está considerando acciones del antes, durante y después de los incidentes.

1 CAPITULO 1: GENERALIDADES Y CONCEPTOS PREVIOS

1.1 FINALIDAD

Garantizar la continuidad de los servicios de tecnología de información y comunicaciones de la Municipalidad Distrital de la Perla, a fin de que se restablezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

Así mismo definir las acciones a ejecutar en caso de fallas de los elementos que componen un sistema de información.

1.2 BASE LEGAL

a) Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Normativa 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.
b) Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres – SINAGERD.
c) Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
d) Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y usos de la tecnología y medios electrónicos en el procedimiento administrativo.
e) Ley N° 28551 – Ley que establece la obligación de elaborar y presentar planes de contingencia.

1.3 OBJETIVOS

1.3.1 Objetivo General

Establecer los principios básicos y el marco necesario para garantizar la operatividad de los servicios y/o procesos de tecnología de información y comunicaciones de la Municipalidad Distrital de la Perla, a fin que se restablezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

1.3.2 Objetivo Específico

a) Identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnología de la información y comunicaciones de la Entidad.
b) Identificar las amenazas y riesgos con impacto en la infraestructura tecnológica.
c) Definir estrategias adecuadas para asegurar y proteger la información contra los daños y prejuicios producidos por cortes de servicios, fenómenos naturales o humanos.
d) Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse en las actividades de la Municipalidad Distrital de la Perla.

1.4 ALCANCE

Las disposiciones del presente Plan de Contingencias son de cumplimiento obligatorio de todos los órganos y unidades orgánicas de la Municipalidad Distrital de la Perla, así como los administrados, según corresponda.

También, considerar que el proveedor de servicio de Telecomunicaciones (servicio de internet) está sujeto a contrato para garantizar que la prestación de dicho servicio no afectará la continuidad operativa de los servicios informáticos de la entidad municipal.

1.5 METAS

Este plan permite minimizar las consecuencias en caso de incidentes con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

Así mismo, 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.

1.5.1 INCIDENTE

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

1.5.2 MÉTODO DE ANÁLISIS DE RIESGO

Los métodos de análisis de riesgo 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.

El presente documento debe contribuir proactivamente a la identificación de los riesgos y amenazas informáticas a través de los siguientes componentes:

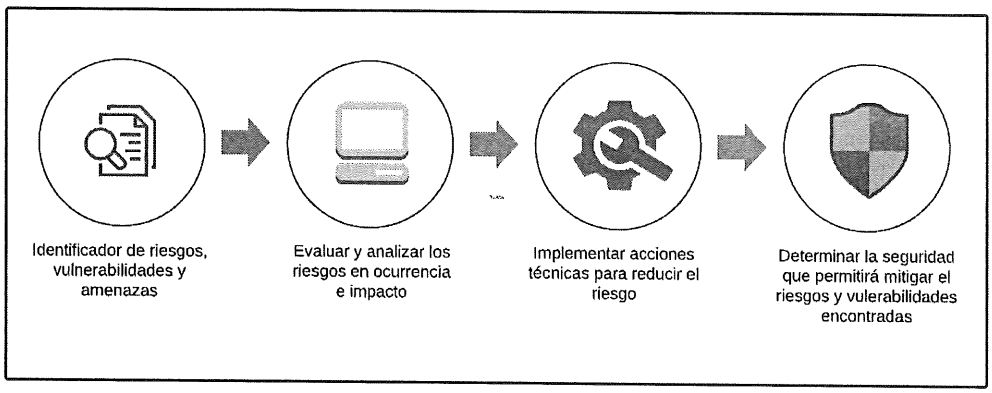

Figura 1: Componentes para identificar los riesgos Fuente: Elaboración personal

1.5.3 PLAN DE EJECUCIÓN

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como 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 a atender la contingencia.

1.5.4 PLAN DE RECUPERACIÓN

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

1.6 DEFINICIONES

Amenaza: Causa potencial de un incidente de seguridad de información no deseado, que puede resultar en un daño para la organización o sistema.

Probabilidad: Posibilidad que un evento determinado ocurra en un periodo de tiempo dado.

Riesgo: Posibilidad de que suceda algún evento adverso que tendrá sobre un impacto sobre el cumplimiento de los objetivos institucionales o de los procesos para la presentación de servicios al ciudadano. Se expresa en términos de probabilidad y consecuencias.

Sistema de información: Es un conjunto de elementos organizados a fin de administrar datos e información necesarios para lograr un objetivo. Dichos sistemas están formados por personas, equipos y procedimientos.

Vulnerabilidad: Debilidad de un acto o grupos de activos o controles, que pueden ser explotados por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.

Plan de Contingencia:

El plan de contingencia es un documento técnico basado en la ingeniería y define los alcances aplicados en materia tecnológica referidos a riesgos y amenazas y las metodologías desarrolladas y aplicadas para gestionar el control de riesgos informáticos.

La identificación del riesgo no solo tiene origen de dominio computacional o informático, existiendo, factores ambientales externos como internos que inducen el incremento o sostiene el factor de vulnerabilidad previo al disparo del riesgo.

Características Principales de un Plan de Contingencia.

Amplio: Porque considera a todos los componentes de los procesos de una institución u organización.

Participativo: Porque se pretenden que intervengan todos los agentes, instituciones o agrupaciones que estén implicados de una u otra forma en el servicio.

Eminentemente práctico: Ya que fija objetivos concretos y establece los medios y los plazos.

El Plan de Contingencia 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.

2 CAPITULO 2: METODOLOGÍA DE TRABAJO

Si bien los planes de contingencia de tecnología de información se realizan a fin de prevenir fallas o accidentes en las operaciones de una entidad, para la elaboración de los mismos es importante tener en cuenta los estados de la infraestructura informática y de los servicios informáticos de la institución, por lo que los planes de cada institución son muy propios. En ese sentido, el desarrollo del Plan se lleva a cabo en las siguientes seis (6) fases:

Fase 1: Planificación

Fase 2: Determinación de Vulnerabilidades

Fase 3: Estrategias del Plan de Contingencia

Fase 4: Desarrollos de los Procedimientos del Plan de Contingencia

Fase 5: Implementación del Plan de Contingencia

Fase 6: Monitoreo

A continuación, se detallan cada uno de las fases:

2.1 FASE 1: PLANIFICACIÓN

2.1.1 ORGANIZACIÓN

La Oficina de Tecnología de Información (OTI), depende directamente de la Oficina General de Administración (OGA), y es responsable de administrar y brindar soluciones informáticas y soporte técnico en materia de tecnología de la Información (TIC) a los órganos de la Municipalidad Distrital de la Perla, para la mejor ejecución de sus funciones, así como, desarrollar el soporte tecnológico y soluciones informáticas para la operatividad de la red nacional de información científica e interconexión. Tiene dentro de sus funciones, elaborar y proponer lineamientos, directivas de tecnologías informáticas y de comunicaciones para la Municipalidad Distrital de la Perla, para el funcionamiento del Plan de Contingencias de Tecnologías de Información se ha establecido, el siguiente organigrama describiendo los roles y los equipos que conforman el plan de contingencias de TI y está conformado por el personal de la Oficina de Tecnología de Información (OTI).

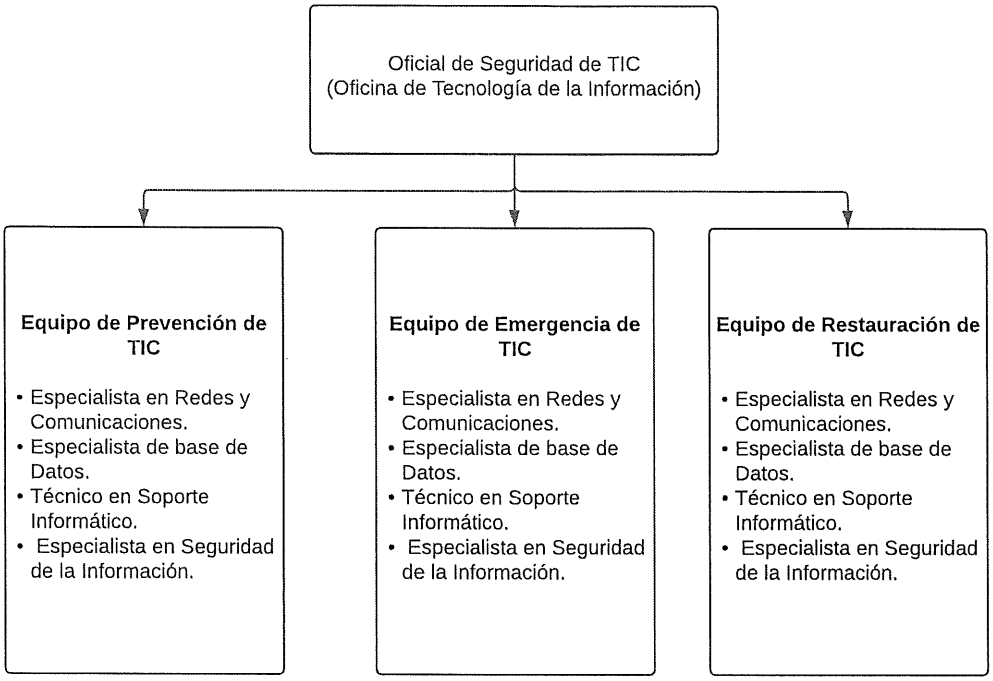

Figura N°2- Organización Operativa del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones (TIC)

2.1.2 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 y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

a. **Oficial de Seguridad de TI**
Está conformado por un representante de la Oficina de Tecnología de la Información 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 y Recuperación de Servicios 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 Comando de Continuidad Operativa acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.

- Monitoreo, 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 y Recuperación de Servicios 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 desastres. 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/la 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 (backup).

Especialista en Redes y Comunicaciones

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Ejecutar y verificar las tareas de copias de respaldo (backup).
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los 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.
- Realizar las pruebas previas de recuperación.

Especialista en Administración de Base de Datos

- 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 Municipalidad Distrital de la Perla, procurando salvaguardar su pérdida o deterioro. A continuación, se citan las acciones que se realizarán durante la contingencia, según los miembros del equipo:

Especialista en Redes y Comunicaciones

- Notificar el desastre o incidencia al Oficial de Seguridad de TI.
- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados Centro de Datos de la Municipalidad de la Perla
- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos de la Municipalidad Distrital de la Perla, durante la emergencia.
- Comunicar al Oficial de Seguridad de TI las acciones de emergencia ejecutadas.

Especialista en Administración en Base de Datos

- Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.
- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de las bases de datos de los sistemas de información.

Técnico de Soporte Informático y redes

- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
- Comunicar al Coordinador al Oficial de Seguridad de TI las acciones de emergencia ejecutadas.
- 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 Municipalidad Distrital de la Perla.

Especialista en Seguridad de la Información

- Apoyar 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 Municipalidad Distrital de la Perla.

Oficial de Seguridad de TI

- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar el estado de las bases de datos de los sistemas de información. Coordinar y monitorear la restauración de aplicativos y ejecución de pruebas para verificación de funcionalidad.

Especialista en Redes y Comunicación

- 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 componentes del Centro de Datos de la Municipalidad Distrital de la Perla.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI y los componentes del Centro de Datos de la Municipalidad Distrital de la Perla.
- Notificar al Oficial de Seguridad de TIC, las acciones de recuperación ejecutadas.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicaciones y los componentes del Centro de Datos.

Especialista en Administración de Base de Datos

- Verificar el funcionamiento de las bases de datos institucionales.
- 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 datos e información de la Municipalidad Distrital de la Perla luego de efectuado el proceso de recuperación.

Técnico de Soporte Informático y Redes

- Verificar el funcionamiento de los equipos personales en las sedes de la Municipalidad Distrital de la Perla afectadas, distribuyendo el trabajo entre los técnicos de soporte.
- 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 Municipalidad Distrital de la Perla, 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.

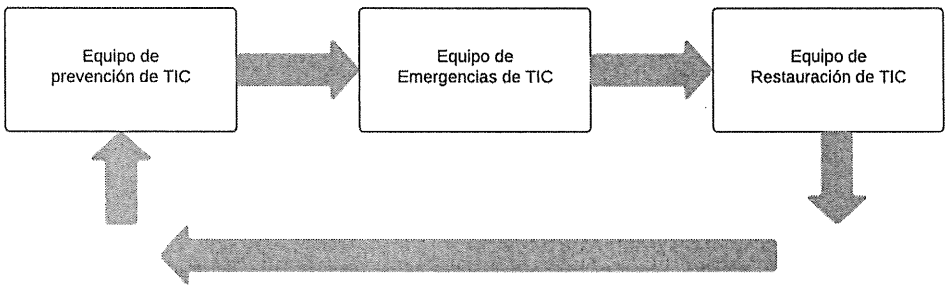

Figura N°3: Flujo del orden de operación de los equipos de TI

2.2 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.

2.2.1 PROCESOS Y RECURSOS CRÍTICOS

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

Proceso	Aplicaciones y/o recursos	Tiempo de Recuperación	
		Grave	Moderado
Gestión de Infraestructura Tecnológica	Equipos de comunicaciones	4 h	1 h
	Infraestructura del Centro de Datos	1 h	30 min
	Radioenlaces para la Interconexión entre sedes	4 h	1 h
	Sistema de almacenamiento	1 h	15 min
Desarrollo y Mantenimiento de soluciones Tecnológicas	Sistema de información administración	4 h	30 min
	Correos Corporativos	4 h	1 h

Tabla N° 1 – Procesos y recursos críticos de TI

2.2.2 TIPOS DE AMENAZAS A LOS SERVICIOS DE TI

Permite identificar aquellas amenazas que pudieran vulnerar los servicios de TI de la Municipalidad Distrital de la Perla, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos.

N°	Amenaza	Tipo
01	Incendio en el Centro de Datos	Siniestro Natural
02	Terremoto/ Sismo	
03	Caída de Internet	Tecnológico
04	Incidente de seguridad informática	
05	Falla de Hardware y Software	
06	Falla Suministro eléctrico	Físico y Ambiental
07	Robos	

Tabla N° 2 – Tipo de Amenazas a los servicios de TI

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, se calcula el nivel de probabilidad de ocurrencia, para lo cual se utilizó los valores definidos en la metodología de Gestión de riesgos que se encuentran en la siguiente tabla:

Valor	Clasificación	Definición
1	Muy Bajo	Puede que no se haya presentado u ocurrido en situaciones excepcionales (Nunca Ocurrido)
2	Bajo	Puede ocurrir en pocas situaciones (ocurrió una vez en la historia de la institución)
3	Medio	Puede ocurrir a largo plazo (Ocurre una vez al año)
4	Alto	Se produce por tendencia o constantemente (Ocurre una vez al mes)
5	Muy Alto	Se produce a corto plazo y sin interrupciones (Ocurre una o más veces a la semana)

Tabla N° 3 – Determinación de la Probabilidad

A continuación, se detalla el resultado obtenido, en base a la metodología de gestión de riesgos, mediante la cual se ha determinado el valor de probabilidad por cada amenaza:

N°	Amenaza (Evento)	Nivel de Probabilidad de ocurrencia (valor)	Nivel de Probabilidad Estimada
1	Incendio en el Centro de Datos	1	Muy bajo
2	Terremoto	1	Muy bajo
3	Caída de Internet	3	Medio
4	Incidente de Seguridad Informática	2	Bajo
5	Falla de Hardware y Software	3	Medio
6	Falla Suministro eléctrico	3	Alto
7	Robos	2	Muy bajo

Tabla N° 4 – Tipos de Amenazas a los servicios de TI

2.2.3 IDENTIFICACIÓN DE CONTROLES EXISTENTES

La identificación de controles existentes, permiten conocer que tan protegidos están los recursos de TI de la Municipalidad Distrital de la Perla, frente a cada amenaza. Los controles existentes son los siguientes:

- Cámaras de vigilancia para la seguridad física de los bienes informáticos.
- Respaldo de información y custodia externa de los medios de respaldo.
- Solución de antivirus instalada en los servidores de red y computadoras.
- Seguridad perimetral Hillstone.
- Sistema contra incendios en el centro de datos.
- Antivirus y antispyware instalados en servidores de red y computadoras.

2.2.4 EVALUACIÓN DE NIVEL DE RIESGOS

Para determinar el Nivel de riesgo de un Recurso de TI crítico de la Municipalidad Distrital de la Perla, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el numeral 2.2.3, así como el valor de probabilidad de ocurrencia Identificado en la Tabla N°3 Determinación de la Probabilidad estimada de los servicios de TI.

Para calcular el resultado del impacto, se considera el valor del nivel del impacto, definido en la aplicación de la metodología de Gestión de riesgos, de acuerdo a la siguiente Tabla:

NIVEL	DESCRIPCIÓN	IMPACTO
4	GRAVE	Si el evento llegara a presentarse, tendría un trágico impacto, comprometiendo la confidencialidad o integridad de información crítica de la entidad o la continuidad de las operaciones por paralización de los servicios críticos.
3	MODERADO	Si el evento llegara a presentarse, tendría un moderado impacto en la confidencialidad, integridad y disponibilidad de la información. Su efecto sería limitado en tiempo y alcance, afectando únicamente un proceso de soporte o una actividad específica que podría subsanarse en corto plazo.
2	MENOR	Si el evento llegara a presentarse, tendría un menor impacto (El impacto es leve y puede prescindir del mismo en un tiempo limitado).
1	INSIGNIFICANTE	Si el evento llegara a presentarse, no representa un impacto importante en la entidad.

Tabla N° 5 – Determinación del impacto.

El valor obtenido ha sido en base a la metodología de Gestión de Riesgos (Tabla N° 5) que ha determinado el impacto por cada amenaza, siendo el resultado el siguiente:

ITEM	RECURSOS CRÍTICOS / AMENAZAS (EVENTOS)	Falla en la red	Incidencia de Seguridad	Falla de los suministros	Falla de Hardware y/o	Usencia o no disponibilidad
1	Equipos de comunicación	4	4	3	3	2
2	Aire acondicionado del Centro de Datos	2	1	3	3	2
3	Sistema de almacenamiento (Storage)	1	1	2	4	1
4	Sistema de información y portales web	3	4	2	4	1
5	Base de datos utilizados por los sistemas y aplicativos	3	4	2	4	1
6	Estaciones de trabajo del personal crítico (Computadoras personales y portátiles)	3	4	2	3	2
7	Servidores de red	3	4	2	4	1

Tabla N° 6 – Resultado del Impacto de los Servidores de TI

2.2.5 ESCENARIOS DE RIESGO

Se han establecido los siguientes escenarios que corresponden a amenazas con probabilidad de nivel medio o superior:

a) Destrucción e indisponibilidad del centro de Datos por terremoto o incendio.
b) Falla en el funcionamiento de los sistemas de información, Hosting, Correos Corporativos y portales Web por delito informático (ataque cibernético, virus, etc.)
c) Indisponibilidad de los servidores de red por falla de Hardware y Software.
d) Interrupción de comunicaciones por fallas en el suministro eléctrico.
e) Falla en los equipos de telecomunicaciones.

A continuación, se detallan los escenarios de riesgo y su impacto, para activar el Plan de Contingencia de Tecnologías de la Información conforme a la aplicación de la clasificación de gestión de riesgos que se describe.

ESCENARIO DE RIESGO	DESCRIPCIÓN	IMPACTO
a) Destrucción e indisponibilidad del centro de Datos por terremoto en incendio	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 componente del mismo.	Extremo
b) Falla en el funcionamiento de los sistemas de información, Hosting, Correos Corporativos y Portales Web por delito informático (ataque cibernético, virus, etc.)	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
c) 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
d) Interrupción de comunicaciones por fallas en el suministro eléctrico.	Este escenario consiste en el corte o interrupción de las comunicaciones entre la sede central y el centro de datos, así como los servicios publicados en internet, como resultado de falla del sistema eléctrico.	ALTO
e) Falla en los equipos de comunicaciones	Se refiere al fallo físico o lógico de los equipos de comunicaciones (Switches, Firewall, Controladores, etc.) lo cual produce que la información o servicios brindados por ellos no estén disponibles	Extremo

Tabla N° 7 – Escenarios de riesgos

2.3 FASE3: ESTRATEGIAS DEL PLAN DE CONTINGENCIAS

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

2.3.1 ESTRATEGIAS DE PREVENCIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

a) ALMACENAMIENTO Y RESPALDO

Los puntos de restauración son aquellos hitos en los cuales se efectúa BACKUP incrementales de todas las actividades y procesos relacionados a la comuna edil; si bien, los incidentes de impacto tecnológico pueden suceder en cualquier momento, la naturaleza de ese impacto deja una secuela cuya restauración es lenta y se basa en los documentos físicos de la organización. El BACKUP debe coadyuvar a reducir a O (cero) esas gestiones semi manuales, que requieren de mayor de tiempo y de recursos asignados adicionales para el proceso de restauración.

I. Realización de copias de respaldo de la información almacenada y procesada en el Centro de Datos.
II. Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
III. Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.

PERIOCIDAD: SEMANAL

RESPONSABLE: Especialista de Soporte Informático y el especialista de seguridad digital.

b) RENOVACIÓN TECNOLÓGICA

La estrategia de riesgo desarrollada y recomendada es **evitar**, ya que existe un plan de renovación o repotenciación del equipamiento de cómputo. Por lo tanto, se recomienda renovar los equipos al finalizar su ciclo de vida útil, lo cual suele ocurrir cada 3 a 4 años. Este reemplazo es necesario para cerrar la brecha tecnológica tangible, tomando en cuenta el ciclo de vida del producto computacional, así como el código y el año de inventario del equipo más antiguo.

Se desarrolla la programación en el plan operativo institucional que incluye acciones de renovación tecnológica.

PERIOCIDAD: 3 – 4 años.

RESPONSABLE: Especialista Técnico de Soporte Informático, Especialista en redes y comunicaciones.

2.3.2 ESTRATEGÍA FRENTE A EMERGENCIAS EN TECNOLOGIAS 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 Municipalidad Distrital de la Perla 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 una contingencia:

Acciones durante la emergencia

1. Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración.
2. Informar al coordinador de continuidad sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
3. Determinar si el área afectada es segura para el personal (en caso de catástrofe).
4. Estudiar y evaluar la magnitud de los daños a los equipos, y elaborar un informe detallado sobre los daños producidos.
5. 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.

2.3.3 ESTRATEGÍA 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 Municipalidad Distrital de la Perla para estabilizar la infraestructura tecnológica luego del evento suscitado.

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

PRIORIDAD DE ATENCIÓN	DESCRIPCIÓN
1	**Atención prioritaria:** Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios y manejen alto volumen de información. Ejemplo, Sistema Integrado de Administración Financiero (SIAF), Sistema integrado de gestión administrativa (SIGA), Sistema de Gestión Documentario(SGD) Portal Web institucional, servidores de bases de datos, correos corporativos, entre otros.
2	**Atención normal:** Sistema de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requieran 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 manejen bajo volumen de información. Asimismo, equipos de apoyo.

Tabla N° 8 – Prioridad de atención durante la restauración de TI

Los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática, se describen en el Anexo N° 1.

2.4 FASE4: ELABORACIÓN DEL PLAN DE CONTINGENCIAS

Una vez identificados los eventos de contingencia y los escenarios de riesgo, se procede con el desarrollo de los procedimientos del Plan de Contingencia, agrupados por las categorías indicadas previamente, lo cual comprenderá los eventos de mayor impacto, identificado en la matriz e riesgos de contingencia y serán abordados tal como se indica en la siguiente tabla, asimismo en el Anexo N° 2 se detalla cada formato del procedimiento del plan de contingencia.

2.5 FASE 5: IMPLEMENTACION DEL PLAN DE CONTINGENCIAS

La implementación del presente plan iniciará en un plazo no mayor de treinta (30) días calendarios después de su aprobación. Para tal efecto, el/la Oficial de Seguridad de la Información en coordinación con el Jefe de Tecnologías de la Información y el Técnico especialista en Soporte informático, realizaran las siguientes funciones:

a) Supervisar las actividades de copias de respaldo y restauración.
b) Establecer procedimientos de seguridad en los sitios de recuperación.
c) Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información (TI)
d) Participar en las pruebas y simulacros de desastres.

2.6 FASE6: MONITOREO

Dado que las condiciones pueden variar con el tiempo, al igual que los bienes informáticos, incluidos los equipos del Centro de Datos, es importante realizar una verificación periódica del Plan de Contingencia.

Las acciones de verificación se deben realizar de manera trimestral y bajo un ambiente controlado, donde se comprueben que con las acciones definidas los bienes y servicios informáticos respondan de acuerdo a lo esperado, considerando que los procesos pueden variar y afectar la disponibilidad de los sistemas.

Como parte del mantenimiento del plan de contingencia, se debe contemplar el entrenamiento al personal de la OTI, a través de capacitaciones virtuales o presenciales de acuerdo a lo planificado por el coordinador de continuidad, y será de manera anual, a fin de que puedan dar una respuesta adecuada a las eventualidades que puedan afectar los servicios informáticos.

ANEXO N° 1

LISTADO DE EQUIPOS, APLICACIONES Y SISTEMAS DE INFORMACIÓN DE CENTRO DE DATOS Y GABINETE CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN

N°	TIPO DE EQUIPO	ROL	IP	DESCRIPCION	PRIORIDAD
1	SERVIDOR	VIRTUAL	192.168.1.222	VMWARE (VIRTUALIZADO)	1
2	SERVIDOR	CONTROLADOR DE DOMINIOS	192.168.1.240	WINDOWS SERVER 2012 R2	1
3	SERVIDOR	SERVIDOR DE ARCHIVOS	192.168.1.246	Donde se encuentra la información de las carpetas compartidas en red	1
4	SERVIDOR	APLICACIONES	192.168.1.244	Servidor de sistema de rentas	1
5	SERVIDOR	APLICACIONES	192.168.1.251	Servidor de Siaf y Siga (VIRTUALIZADO)	1
6	SERVIDOR	WEB	NUBE	Servidor de correo corporativo	1
7	SERVIDOR	WEB	NUBE	Servidor de Portal Web Institucional	1
8	SERVIDOR	SEGURIDAD	NUBE	SERVIDOR DE ANTIVIRUS	3
9	SERVIDOR	APLICACIONES	192.168.1.241	Servidor de sistema de Catastro	2
10	UPS	ENERGIA		Equipo de suministro eléctrico para servidores y equipos de comunicación	3

ANEXO N° 2

FORMATOS DEL PROCEDIMIENTOS DE CONTINGENCIA (FPC) INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TI

MUNICIPALIDAD DISTRITAL DE LA PERLA	EVENTO: Incidente de Seguridad Informática (ataque)	FPC - 01

1. PROCEDIMIENTO DE PREVENCIÓN

a) SITUACION ACTUAL

- Si bien la instalación de software, sea propietario o de desarrollo interno, es realizado y/o supervisado por la OTI, existen casos en que el personal instala software en sus equipos sin autorización ni supervisión de la OTI, poniendo en riesgo sus equipos pues puede ser software malicioso.
- Se cuenta con un software de antivirus corporativo, el cual se renueva de forma periódica.
- El personal no es consciente a plenitud sobre el riesgo e impacto de hacer uso de software sin supervisión de la OTI, así como de abrir correos electrónicos de dudosa procedencia o hacer uso de dispositivos de almacenamiento externos sin los cuidados adecuados. Todo esto podría dañar no sólo al bien informático sino también a la información almacenada.
- Se cuenta con mecanismos de seguridad perimetral, para evitar el acceso no autorizado a la red institucional. - Es preciso describir que el malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc.

b) OBJETIVO

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

c) PERSONAL ENCARGADO

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

d) CONDICIONES DE PREVENCIÓN DE RIESGOS

- Instalación de parches de seguridad en los equipos. - 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 y 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 de acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- Deshabilitación 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.

- Capacitar y concientizar al personal de la Municipalidad Distrital de la Perla, sobre la importancia de la seguridad de la información.
- Implementar seguridad del correo corporativo entre ellos la protección en:
  - Detener el phishing y el malware
  - Transporte de datos cifrados con TLS
  - Protección contra el abuso de marca
  - Protección contra el robo de identidad
  - Protección contra Ransomware
  - Protección contra el fraude

e) ACCIONES DEL EQUIPO DE PROTECCIÓN

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información procesada y almacenadas 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. PROCEDIMIENTO DE EJECUCIÓN

a) EVENTOS QUE ACTIVAN LA CONTINGENCIA

- Mensajes de error durante la ejecución de programas.
- Caídas del Correo corporativo.
- Lentitud en el acceso a las aplicaciones.
- Fallas en el sistema operativo y aplicaciones de los equipos.

b) Personal que autoriza la contingencia informática el/la Oficial de Seguridad de la Información pueden activar la contingencia.

c) ACCIONES PARA EJECUTAR A CORTO PLAZO

- Desconectar de la red de datos el servidor o la estación infectada o vulnerable.
- Verificar si el equipo se encuentra infectado, utilizando un detector de malware / virus actualizado. En caso de aplicaciones, verificar si el código o la información de la base de datos ha sido alterada.
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

d) En caso de que se confirme un incidente de seguridad informática, la duración del evento no deberá ser mayor a 24 horas en estaciones de trabajo y 4 horas en los servidores del centro de datos.

3. PROCEDIMIENTO DE RECUPERACIÓN

a) El personal encargado del equipo de restauración, una vez restaurado el correcto funcionamiento del servidor, la estación de trabajo (PC, laptop), los sistemas de información y los portales web, coordinará con el usuario responsable e informará a su jefe inmediato para reanudar las labores de trabajo.

b) **DESCRIPCIÓN DE ACTIVIDADES**

- Instalación y configuración de software, drivers y servicios necesarios para el funcionamiento de la información recuperada.
- Instalación del motor de base de datos, con sus respectivas librerías y niveles de seguridad.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible.
- Conectar el servidor o la estación de trabajo a la red.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Ejecutar análisis de vulnerabilidad.
- Comunicar el restablecimiento del servicio.

c) **MECANISMO DE COMPROBACIÓN**

- El/la Especialista de infraestructura de Redes y/o el personal de soporte técnico, según sea el caso, presentará un informe a el/la Jefe/a de la OTI, informando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

MUNICIPALIDAD DISTRITAL DE LA PERLA	EVENTO: Falla de hardware y software	FPC - 02

1. PROCEDIMIENTO DE PREVENCIÓN

a) **SITUACIÓN ACTUAL**

- El centro de Datos se encuentra conectado a una red eléctrica estabilizada y conectado a UPS.
- Se ha detectado que en diversas oficinas existen interrupciones en el suministro eléctrico, lo que afecta a los equipos informáticos. Estos cortes de energía provocan apagones imprevistos, lo que daña progresivamente los componentes de las computadoras o genera que un equipo queda fuera de servicio o requiere una revisión técnica, lo que consume tiempo y presupuesto.
- No existe un circulo eléctrico exclusivo para los equipos informáticos.
- Dependiendo del equipo, las fallas pueden ser atendidas o resuelta por el personal interno de la OTI, pero en otros casos es necesarios sea remitido a una empresa especializada. En ambos casos es importante que se proporcione una atención rápida a las fallas que presenta los equipos.
- En los casos en que los sistemas de información estén alojados en la nube, su disponibilidad está supeditada a la disponibilidad de la infraestructura de la empresa que brinda dichos servicios, así como de las actualizaciones que dicha empresa pudiese realizar. Esto, dado que dichas actualizaciones pueden generar un funcionamiento inadecuado de los servicios.

b) **OBJETIVO**

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

c) **PERSONAL ENCARGADO**

El equipo de prevención.

d) **CONDICIONES DE PREVENCIÓN DE RIESGO**

- Revisión periódica de los riesgos (Logs) de los servidores, para prevenir mal funcionamiento de los mismos.
- Contar, como mínimo, con copias de seguridad quincenales de los datos de las aplicaciones en desarrollo y producción de la entidad.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.
- Disponer de servicios de bases de datos de contingencia, con la instalación del motor de base de datos.

e) **ACCIONES DEL EQUIPO DE PREVENCIÓN**

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- Programar y supervisar el mantenimiento preventivo y correctivo de los equipos y componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software del Centro de Datos de LA Municipalidad Distrital de la Perla.
- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datos para su correcto funcionamiento.
- Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios.
- Determinar la necesidad de adquisición de nuevos equipos considerando el tiempo de vida, y el impacto de un funcionamiento inadecuado de los mismos.

2. PROCEDIMIENTO 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) **PERSONAL QUE AUTORIZA LA CONTINGENCIA**

Jefe de la Oficina de Tecnologia de la Información

c) **PERSONAL ENCARGADO**

Equipo de emergencia.

d) **ACCIONES A EJECUTAR A CORTO PLAZO**

- Contar con la disponibilidad del personal para la reparación rápida de los equipos.
- Establecer con la empresa que brinda servicio de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios, de forma tal que se puedan ejecutar simulacros y evaluar su impacto, previniendo una interrupción de los servicios.
- Acceder a las copias de respaldo para la restauración de la información en el servidor averiado.
- Verificar que el equipo se encuentre en garantía, de lo contrario se implementará un nuevo servidor virtual.

e) **DURACIÓN**

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

3. PROCEDIMIENTO DE RECUPERACIÓN

a) **PERSONAL ENCARGADO**

El Equipo de Restauración, después de validar la corrección del problema de acceso a los servidores, y el Jefe de la Oficina de Tecnología de la Información informará a los Gerentes y Subgerentes de las áreas para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b) **DESCRIPCION DE ACTIVIDADES**

- Instalación y configuración del sistema operativo, drivers 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.
- Comunicar mediante correo electrónico a los usuarios la reanudación de los servicios.

MUNICIPALIDAD DISTRITAL DE LA PERLA	EVENTO: Falla del suministro eléctrico	FPC - 03

1. PROCEDIMIENTO DE PREVENCIÓN

a) **SITUACIÓN ACTUAL**

- El inmueble no cuenta con luces de emergencia en determinados puntos.
- No se cuenta con grupo electrógeno para salvaguardar los daños ocasionados por falla de corriente eléctrica en los equipos de cómputo.
- La continuidad del fluido eléctrico del Centro de Datos está soportada en 2 UPS que dan un promedio de 30 minutos aproximadamente para el apagado progresivo de los equipos, para que ejecuten las acciones correspondientes para un apagado adecuado.
- Es importante que el personal se concientice sobre la importancia de usar adecuadamente el tiempo que brindan los UPS para el apagado de los servicios alojados en los servidores del centro de datos, a fin de realizar adecuadamente el apagado de los equipos y evitar que queden defectuosos y/o dañar información.
- No se realizan simulacros de interrupciones de fluido eléctrico en el Centro de Datos, y no existen procedimientos formales de apago y encendido del mismo.

b) **OBJETIVO**

Restaurar las funciones consideradas como críticas para el servicio.

c) **PERSONAL ENCARGADO**

- El/la especialista infraestructura de la red y Soporte Informático, es el responsable de atender y supervisar las respuestas ante el incidente.
- El Jefe de la Oficina de Tecnología de la Información es el responsable de realizar las coordinaciones para restablecer el suministro de energía eléctrica con los proveedores de energía.
- El equipo de prevención debe realizar las acciones descritas en el punto e).

d) **CONDICIONES DE PREVENCIÓN DE RIESGO**

- Para los servicios diarios, se debe de contar con grupo electrógeno, ya se cuenta con equipos UPS necesario para asegurar el suministro eléctrico en los equipos consideradas como críticos.
- El Equipo UPS deberá contar con mantenimiento preventivo. El tiempo variará de acuerdo a la función que cumplan.
- Realización de pruebas periódicas del equipo UPS para asegurar su correcto funcionamiento.
- Capacidad del 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 de 30 min.

e) ACCIONES DEL EQUIPO DE PREVENCIÓN

- Programar y supervisar el mantenimiento preventivo y correctivo a los equipos componentes del Centro de Datos.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado del Centro de Datos, UPS, grupo electrógeno, transformador y del gabinete de baterías trimestralmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos 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 Municipalidad Distrital de la Perla.
- Se deberá adquirir un grupo electrógeno que proporcione suficiente energía eléctrica para soportar una operación continua de, al menos, 4 horas. El tiempo de funcionamiento podrá variar según la función que cumpla.

2. PROCEDIMIENTO 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) **PERSONAL QUE AUTORIZA LA CONTINGENCIA**

Jefe de la Oficina de Tecnología de la Información.

c) **PERSONAL ENCARGADO**

Equipo de emergencia.

d) **ACCIONES PARA EJECUTAR A CORTO PLAZO**

- Contar con la disponibilidad del personal para la reparación rápida de los equipos.
- Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios, de forma tal que se puedan ejecutar simulacros y evaluar su impacto, previniendo una interrupción de los servicios.
- Acceder a las copias de respaldo para la restauración de la información en el servidor averiado.
- Verificar que el equipo se encuentre en garantía, de lo contrario de implementará un nuevo servidor virtual.

e) **DURACIÓN**

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

4. PROCEDIMIENTO DE RECUPERACIÓN

a) **PERSONAL ENCARGADO**

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

b) **DESCRIPCION DE 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:
  - **I.** Equipos de Comunicaciones (router, switches core, switches de acceso)
  - **II.** Equipos de almacenamiento (storage)
  - **III.** Servidores físicos por orden de prioridad.
  - **IV.** Servidores virtuales por orden de prioridad
  - **V.** La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

ANEXO N° 3

PRESUPUESTO

ITEM	DESCRIPCIÓN	VALOR ESTIMADO (no oficial)	IMPORTANCIA
1	Almacenamiento NAS 0TB SYNOLOGY DS420+ 4-bahia	S/. 5,000	El NAS es un sistema de almacenamiento conectado a la red cuya función principal es la de realizar copias de seguridad de los archivos tal y como indique su configuración particular. Por tanto, el NAS es una solución informática que permite la configuración de un almacenamiento exclusivo en la nube y así salvaguardar todos los sistemas de información integral de la entidad.
2	Ventilador para gabinete con cable de poder	S/. 500	Es importante contar con un flujo de aire saludable dentro del gabinete: de esto dependerá, en gran medida, la temperatura a la que trabajarán los distintos componentes y, por lo tanto, su performance y vida útil.
3	UPS Monofásico para servidores de 800w	S/. 12,000	Es un dispositivo que permite que una computadora siga funcionando durante unas horas durante un apagón o cuando se pierde la fuente de alimentación principal. Dado que hay apagones continuos en las madrugadas o de noche por esta zona, un UPS de durabilidad de 4 a 6 horas son primordiales para conservar los sistemas funcionando ya que el tiempo estimado de regreso de la energía eléctrica es de 2 a 3 horas. y al otro día los sistemas seguirán funcionando de manera continua sin interrupciones.
4	Aire acondicionado de precisión para DataCenter	S/ 15,000	El aire acondicionado para salas de servidores tiene una función critica: conservar la temperatura en niveles óptimos y controlar las densas cargas electrónicas en los data center, así como gestionar la humedad y aire del ambiente o sala.
5	Antivirus para Computadoras y Servidores	S/ 15,000	Los antivirus tienen la misión principal de detectar y eliminar el 'malware' (o 'software malicioso) de los equipos y dispositivos antes incluso de que hayan infectado el sistema.
6	Hillstone – Firewall y Seguridad perimetral de red.	Alquilado (Pago mensual)	Se emplea principalmente para otorgar un alto nivel de seguridad perimetral a una organización, inclusive cuentan con diferentes funciones para proteger los activos de la empresa de diversas prácticas como filtro de correo electrónico y anti spam.
7	Disco Duro SSD 2TB para servidores incluido adaptador	S/ 1,500	Muy importante cuidar la calidad y eficiencia de los servidores que almacenan los sistemas de la entidad, ayudan a más velocidad de lectura y escritura, más resistencia, menos consumo, hacen menos ruido y son más rápidos. Por estas sencillas razones son más apropiados para los servidores, tanto si van a ser servidores dedicados o servidores virtuales.