MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
PROVINCIA DE LIMA

RESOLUCIÓN DE ALCALDÍA Nº 624-2025 /MDSM

San Miguel, 24 de diciembre de 2025

EL ALCALDE DISTRITAL DE SAN MIGUEL;

VISTOS, el Memorando N°0844-2025-MDSM/GM emitido por la Gerencia Municipal, el Informe N°331-2025-OAJ/MDSM emitido por la Oficina de Asesoría Jurídica, el Informe N°062-2025-OTIC/MDSM emitido por la Oficina de Tecnologías de la Información y Comunicaciones, Informe N°129-2025-USC-OTIC/MDSM emitido por la Unidad de Soporte y Comunicaciones y;

CONSIDERANDO:

Que, el artículo 194º de la Constitución Política del Perú, modificado por el artículo único de la Ley Nº30305 – Ley de Reforma Constitucional, concordante con el artículo II del Título Preliminar de la Ley 27972 – Ley Orgánica de Municipalidades, dispone que los gobiernos locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia, la misma que radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico;

Que, la Ley N°27658 - Ley Marco de Modernización de la Gestión del Estado, declara al Estado 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;

Que, mediante Ley N°28551 se establece la obligación de elaborar y presentar planes de contingencia, con sujeción a los objetivos, principios y estrategias del Plan Nacional de Prevención y Atención de Desastres;

Que, el artículo 2° de la norma en comentario, define que los planes de contingencia son instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, víctimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos;

Que, asimismo, el artículo 3° de la acotada ley, señala que todas las personas naturales y jurídicas de derecho privado o público que conducen y/o administran empresas, instalaciones, edificaciones y recintos tienen la obligación de elaborar y presentar, para su aprobación ante la autoridad competente, planes de contingencia para cada una de las operaciones que desarrolle;

Que, mediante Decreto Legislativo N°1412 se aprobó la Ley de Gobierno Digital cuyo objeto es establecer la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, la Presidencia de Consejo de Ministros con 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. 2° Edición", la cual especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización;

Que, el artículo 2° del Decreto Supremo N°050-2018-PCM define que la Seguridad Digital en el ámbito nacional, es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas, frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas;

Que, mediante Resolución Ministerial N°320-2021-PCM se aprueban los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno", los cuales tienen como objetivo, establecer los procedimientos para la implementación de la Gestión de la Continuidad Operativa y la formulación de los Planes de Continuidad Operativa en las entidades públicas de los tres niveles de gobierno, con el fin de continuar funcionando ante un desastre o cualquier evento que interrumpa prolongadamente sus operaciones;

Que, el numeral 5 inciso 5.1, literal e) y f) de los acotados lineamientos, definen lo siguiente:

e) *Plan de Continuidad Operativa: Instrumento a través del cual se implementa la continuidad operativa, tiene como objetivo garantizar que la entidad ejecute las actividades críticas identificadas previamente. Contiene la identificación de riesgos y recursos, acciones para la continuidad operativa y el cronograma de ejercicios.*

f) *Plan de Recuperación de los servicios informáticos: Plan que forma parte del Plan de Continuidad Operativa, el cual busca, inicialmente, restaurar los servicios de tecnología de información necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. Para su desarrollo toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 20071:2014.*

Que, el Reglamento de Organización y Funciones de la Municipalidad Distrital de San Miguel aprobado mediante Ordenanza 476/MDSM, en su artículo 78° numeral 4, establece como una competencia adscrita a la Unidad de Soporte y Comunicaciones: «*Formular, elaborar y ejecutar el plan de contingencia informático y de comunicaciones, a fin de garantizar la normal operatividad de la red, los servicios de internet, correo electrónico y transmisión de datos*»;

Que, en razón a ello, la Unidad de Soporte y Comunicaciones con Informe N°129-2025-USC-OTIC/MDSM, señala que un Plan de Contingencia Informático (PCI) es un documento estratégico y operativo que detalla los procedimientos, recursos y responsabilidades que una organización debe activar inmediatamente después de que un incidente o desastre afecte seriamente su infraestructura tecnológica (hardware, software, datos o redes); por ello, en el marco de sus competencias, remite a la Oficina de Tecnologías de la Información y Comunicaciones, el Plan de Contingencia para su respectiva aprobación mediante acto administrativo;

Que, la Oficina de Tecnologías de la Información y Comunicaciones mediante Informe N°062-2025-OTIC/MDSM, señala que la Unidad de Soporte y Comunicaciones sostiene la obligatoriedad de contar en nuestra Entidad con un Plan de Contingencia Informático, detallando los potenciales riesgos en los que se podría incurrir en caso de la no existencia de este; en ese sentido, eleva a la Gerencia Municipal el referido plan, para la continuación del trámite correspondiente;

Que, la Oficina de Asesoría Jurídica con Informe N°331-2025-OAJ/MDSM, considera que el "Plan de Contingencia de Tecnologías de la Información", se ajusta a derecho, por encontrarse conforme a lo dispuesto en la Resolución Ministerial N°320-2021-PCM, debiendo aprobarse mediante Resolución de Alcaldía;

Que, la Gerencia Municipal con Memorando N°0844-2025-MDSM/GM, deriva los documentos glosados en los párrafos precedentes y el Proyecto de Resolución de Alcaldía, para la prosecución del trámite correspondiente conforme a lo desarrollado por las áreas competentes y la normatividad vigente y;

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
PROVINCIA DE LIMA

Estando a lo expuesto y en uso de las atribuciones conferidas al Alcalde en el numeral 6 del artículo 20° de la Ley N°27972, Ley Orgánica de Municipales;

SE RESUELVE:

Artículo 1°. - APROBAR el Plan de Contingencia de Tecnologías de la Información de la Municipalidad Distrital de San Miguel conforme a los considerandos antes expuestos, el mismo que en anexo forma parte del presente acto resolutivo.

Artículo 2°. - PUBLICAR la presente resolución y anexo, en el portal institucional de la Municipalidad Distrital de San Miguel (www.munisanmiguel.gob.pe).

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
SECRETARÍA GENERAL
Abog. KARIN GARCÍA JUÁREZ
SECRETARIA GENERAL

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
PROVINCIA DE LIMA
EDUARDO BLESS CABREJAS
ALCALDE

Municipalidad Distrital de San Miguel

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

2025

ROL	NOMBRE	CARGO	FIRMA / V°B°
Elaborado por:	Percy Alexis Acosta Figueroa	Especialista en Tecnologías de la Información y Comunicaciones	
Revisado por:	Renato Antonio Álvarez Llosa	Subgerente de la Unidad de Soporte y comunicaciones	
	Ricardo Gustavo Alvarado Bustos	Gerente de Tecnologías de la Información y Comunicaciones	
Aprobado por:	Renato Antonio Álvarez Llosa	Subgerente de la Unidad de Soporte y comunicaciones	

Municipalidad Distrital de san Miguel	PLAN DE CONTINGENCIA DE TI		
	Código: PC-01-2025-MDSM	Versión: 1.0 Fecha de Aprobación	Páginas: 74
DEPENDENCIA	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES		
UNIDAD ORGANICA	UNIDAD DE SOPORTE Y COMUNICACIONES		

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SAN MIGUEL

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
V°B°
RENATO ALVAREZ LLOSA
SUBGERENTE
UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel
V°B°
RICARDO G. ALCARAZ BUSTOS
GERENTE
OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES

ELABORADO POR:	Unidad de Soporte y Comunicaciones
San Miguel - 2025	

CONTROL DE CAMBIOS *				
N°	**Ítems**	**Descripción del cambio**	**Versión**	**Fecha de vigencia**
1		Versión inicial del documento	1.0	

Comentarios a las Versiones

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

(*) Contemplar solo las dos últimas versiones.

INDICE

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES

I. INTRODUCCIÓN

La Municipalidad Distrital de San Miguel, para asegurar el cumplimiento de su misionalidad, se apoya en los procesos de tecnologías de la información con el fin que los servicios brindados tanto a sus contribuyentes y administrados, se presten con la eficiencia que se requiere; así mismo, para que los productos que generan, con la oportunidad y calidad planificadas.

En tal sentido, uno de los aspectos de mayor importancia, es la salvaguarda de la información que se procesa y administra, por ello, se deben evitar riesgos de pérdida de información o riesgos de suspensión de servicios por fallas de cualquier índole. Es así como, el Plan de Contingencia de TI, se convierte en un mecanismo sustantivo para mantener en operación el conjunto de procesos, procedimientos, asegurar los recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro de TI; un Plan de contingencia de TI, es un instrumento de gestión para una buena gestión de las Tecnologías de la Información y Comunicaciones que tiene como fin, garantizar la continuidad de los servicios de TI.

El presente documento, establece roles y responsabilidades para la operación del Plan de contingencia de TI, muestra la identificación de los riesgos y los responsables de su administración, relaciona el inventario de activos de TI, sobre los cuales se deben realizar las actividades prioritarias en caso de presentarse un evento que pongan en riesgo la continuidad de la operación y de la prestación de los servicios de TI.

El Plan de Contingencia de TI, aplica las actividades necesarias para mantener en operatividad los sistemas de información de la MUNICIPALIDAD DISTRITAL DE SAN MIGUEL, para lo cual, establece los aspectos técnicos, humanos y logísticos, que permitan afrontar cualquier contingencia.

De igual forma, el Plan de Contingencia de TI, define un plan de las pruebas a realizar con el objetivo de reducir la probabilidad de riesgos frente a un siniestro a un nivel aceptable, tanto para el hardware como del software y la apropiada recuperación de la información.

II. OBJETIVOS

Establecer disposiciones que permitan garantizar el restablecimiento de la operación normal de la plataforma tecnológica de la entidad municipal, en caso de la ocurrencia de un evento o la materialización de un riesgo de TI, que pueda alterar el normal funcionamiento de los sistemas de información críticos de la Municipalidad Distrital DE SAN MIGUEL.

III. ALCANCE

El Plan de Contingencia de TI de la Municipalidad Distrital DE SAN MIGUEL, 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 Unidad de Soporte y Comunicaciones, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad municipal.

IV. BASE LEGAL

- Ley 28551, Ley que establece la obligación de elaborar y presentar Planes de Contingencia.
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley 28716, Ley de Control Interno de las Entidades del Estado.
- Decreto Legislativo N° 1412-2018 Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento de la Ley de Gobierno Digital.
- Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
- Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Resolución Ministerial N° 087-2019-PCM, que dispone sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso Obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 028-2015-PCM, Aprueban Lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.
- Resolución Directoral N° 047-2018-INACAL/DN, que aprueba la Norma Técnica Peruana NTP-ISO/IEC 27005:2018 Tecnología de la Información. Técnicas de Seguridad. Gestión de riesgos de seguridad de la información.

- Resolución de Secretaria de Gobierno Digital N° 001-2018-PCM/SEGDI, que aprobó el uso de servicios en la nube para las entidades de la Administración Pública del Estado Peruano.
- Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 EDI. señala en el Anexo A. 17.1 Continuidad de Seguridad de la Información. "Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización".
- Norma Técnica Peruana "NTP-ISO/IEC 27005:2009 EDI. el cual está diseñado para asistir a la implementación satisfactoria de la seguridad de la información en base a un enfoque de Gestión del Riesgo.

V. DEFINICIONES

Para efectos del presente Plan de Contingencia de TI, se entenderá por;

a. **Plan de Contingencia de TI:** 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 visto afectado negativamente por causa de algún incidente interno o externo a la entidad municipal.
b. **Incidente:** Circunstancia o suceso que ocurre de manera inesperada y que puede afectar al desarrollo normal 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 MUNICIPALIDAD DISTRITAL DE SAN MIGUEL.
c. **Incidente de seguridad de la información:** Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operatividad de la entidad municipal.
d. **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, etc.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).
e. **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.
f. **Probabilidad:** Posibilidad de que un evento determinado ocurra en un periodo de tiempo dado.
g. **Activo de información:** Cualquier información que tiene valor para la entidad municipal y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.
h. **Amenaza:** Cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la entidad municipal.

i. **Confidencialidad:** Evita que personas no autorizadas accedan a la información institucional.
j. **Disponibilidad:** Permite la disposición de la información cuando sea requerido por el personal autorizado.
k. **Integridad:** Mantiene la información en su totalidad y sin alteraciones, a menos que sea modificado por el personal autorizado

VI. ROLES Y RESPONSABILIDADES

Para el manejo de la activación del Plan de Contingencia de TI, en alguno de sus escenarios, es importante destacar que la Unidad de Soporte y Comunicación, de conformidad a lo establecido en su artículo 76° numeral 4 del Reglamento de Organización y Funciones – ROF, aprobado mediante Ordenanza N° 433-MDSM de la MUNICIPALIDAD DISTRITAL DE SAN MIGUEL, señala: ***"Formular, elaborar y ejecutar el plan de contingencia informático y comunicaciones, .a fin de garantizar la normal operatividad de la red, los servicios de internet, correo electrónico y transmisión de datos"*** ; en tal sentido dicha Unidad será quien deberá establecer los protocolos de comunicación primarios con la Seguridad y Vigilancia de los sistemas de comunicación y gestión en coordinación con la unidad de Logística y control patrimonial, con el fin de establecer los canales de comunicación al interior de la entidad municipal, en caso de presentarse alguna contingencia como la caída del fluido eléctrico, inundación, sismo, o en el evento de la programación o ejecución de actividades de mantenimiento que afecten el fluido eléctrico de la entidad municipal, en días laborales y no laborales y/o cuando se encuentren o no servidores en las instalaciones de las sedes de la entidad municipal.

De igual manera, se deberá priorizar la comunicación con la Oficina de Tecnologías de la Información y Comunicaciones – OTIC, para la coordinación logística del lugar y para que la Unidad de Soporte y Comunicaciones, proceda con el apagado seguro de los elementos del Data Center.

El compromiso de los funcionarios públicos de la entidad municipal, especialmente de la Alta Dirección y los de la Oficina de Tecnologías de la Información y Comunicación, es fundamental debido a que son ellos quienes tienen la responsabilidad de responder de forma adecuada ante un incidente tecnológico inesperado en la operación de la entidad municipal y el desarrollo del trabajo, desde el momento que se declare la interrupción hasta la vuelta a la normalidad, (prevención, mitigación, preparación, alertas, respuestas, rehabilitación y reconstrucción) de forma que se reduzca al mínimo el impacto sobre la prestación del servicio.

A continuación, se definen tres niveles de gestión (estratégico, táctico y operativo) y sus responsabilidades durante una situación de contingencia de TI, organización que permitirá segregar funciones y roles para que las tareas y áreas de responsabilidad no presenten conflicto alguno; en cada nivel se debe establecer un

plan de sucesión para que en caso de no estar disponible el servidor público principal, pueda su reemplazo proceder con la misma autoridad y responsabilidad:

Nivel Estratégico: Este nivel corresponde básicamente a la planeación del logro de los objetivos del Plan de Contingencia de TI, se basa en decidir y asignar las políticas, directrices y los recursos para lograr su efectividad en caso de presentarse una interrupción tecnológica no planeada en la entidad municipal.

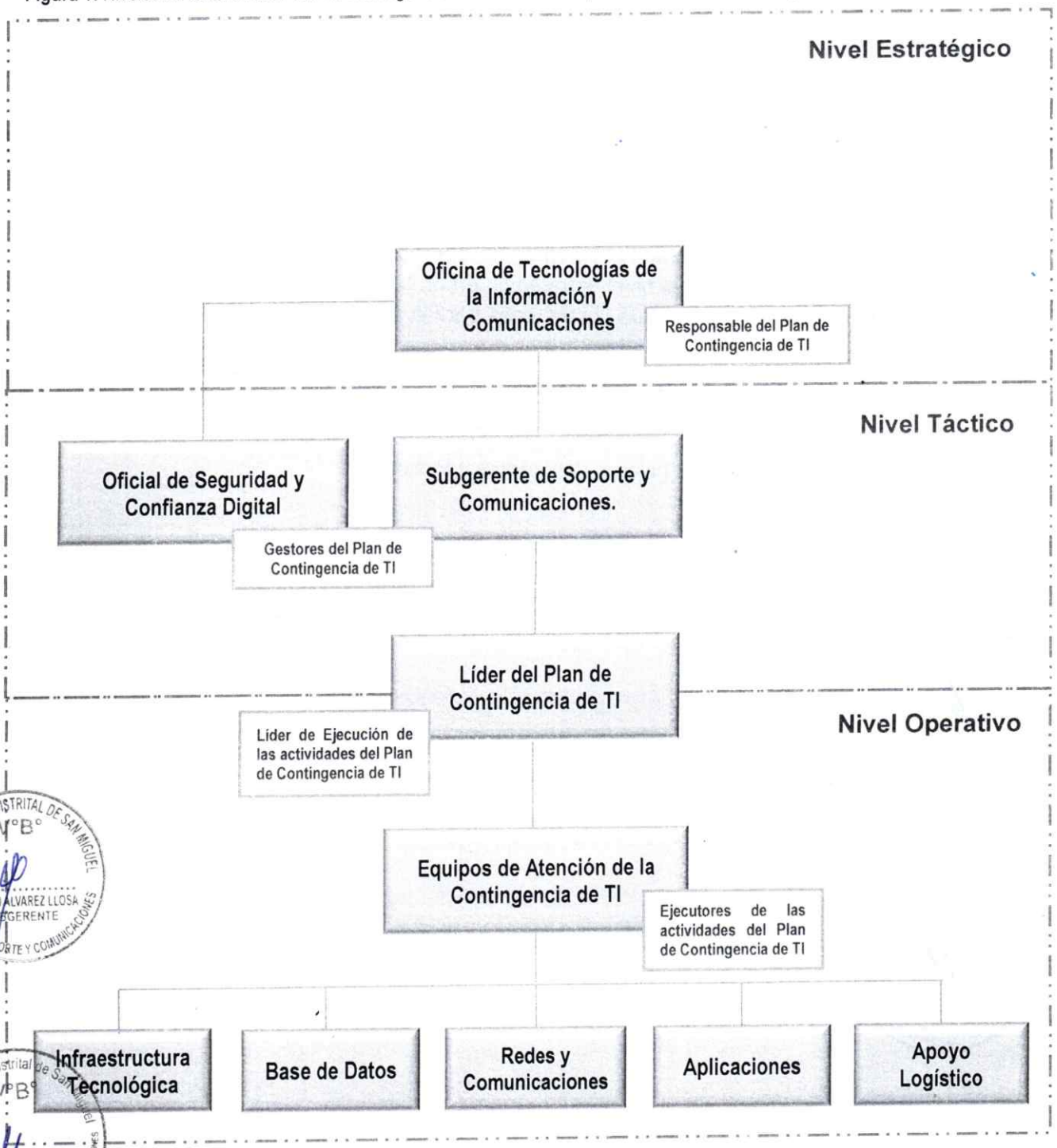
Nivel Táctico: Llevará a cabo la coordinación de las actividades que se deriven del Plan de Contingencia de TI, así como la evaluación de las situaciones de interrupción y dará lineamientos para la operación de mismos, a su vez es el encargado de escalar al nivel estratégico en un lenguaje claro las necesidades de la operación de TI y brindará los insumos para la evaluación.

Nivel Operativo: Este nivel realiza las tareas puntuales en el momento de presentarse un incidente o evento inesperado que activa el Plan de Contingencia de TI de la entidad municipal; se ejecutará a partir de los lineamientos proporcionados por los niveles estratégico y táctico.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
V°B°
RENATO ALVAREZ LLOSA
SUBGERENTE
UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel
V°B°
RICARDO G. ALEGRIADO BUSTOS
GERENTE
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

Figura 1: Niveles de Gestión del Plan de Contingencia de TI de la Municipalidad Distrital de San Miguel.



Fuente: Elaboración propia.

VII. INVENTARIO DE SERVICIOS E INFRAESTRUCTURA DE TI

Conforme a lo descrito en el Plan de Gobierno Digital 2022 – 2024 de la entidad municipal, a continuación, se presenta la Infraestructura, los servicios de TI y Sistemas de Información que tienen identificados en la Unidad de Soporte y Comunicaciones para su gestión y mantenimiento respectivo.

1. Sistemas de Información

Actualmente, los procesos se apoyan en sistemas de informáticos diseñados a la medida, así como también sistemas y aplicativos informáticos cedidos por el Ministerio de Economía y Finanzas y la PCM, de conformidad con la legislación vigente, de los cuales la entidad municipal en algunas aplicaciones y/o sistemas informáticos realizó las adecuaciones necesarias considerando ajustarlo a su dinámica funcional.

A continuación, se presenta la descripción de cada uno de los sistemas de información con que cuenta la entidad municipal.

Tabla 1 - Lista de Sistemas Informáticos de la MDSM

N°	NOMBRE	DESCRIPCION
2	Sistema Integrado de Administración Financiera – SIAF	El Sistema Integrado de Administración Financiera SIAF, es una herramienta para un registro único y obligatorio de la información financiera de todas las entidades públicas.
3	Sistema Informático Municipal Tributario – SAMNET	Registra y administra la información de los tributos y no tributos, tales como el impuesto predial, arbitrios, multas tributarias y no tributarias.
4	Sistema Informático Municipal ADMICOM	Sistema Informático Municipal Integrado - primera versión web, es el sistema de control de gastos de la Municipalidad distrital de San Miguel. Este controla la mayor parte de las oficinas de la MDSM, sistema para realizar requerimientos y el monitoreo de los mismos.
6	Sistema de tramite documentario (SISDOC)	Sistema de tramite documentario, versión aplicativo de escritorio Este se encarga de la recepción y circulación de documentos internos entre oficinas para su proceso formal de atención. Asimismo, almacena los registros de licencias y certificados de funcionamiento.

Fuente: Inventario de la OTIC.

2. Servicios Digitales

Se entiende por servicio digital a todo servicio que se pone a disposición del usuario a través del Internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por Internet.

En base a lo anterior los servicios digitales que brinda actualmente la entidad municipal, cumplen con las características: es automático, no presencial, interoperable, escalable, usable y accesible. LA MUNICIPALIDAD DISTRITAL DE SAN MIGUEL cuenta con los siguientes servicios digitales.

Tabla 2 - Lista de Servicios Digitales de la MDSM

N°	SERVICIO DIGITAL	DESCRIPCIÓN	CANAL	URL
1	Mesa de Partes Virtual	Es una plataforma digital, responsable de brindar atención a los ciudadanos de diferentes canales de atención, así como de registrar y canalizar el trámite de los documentos que ingresan a la entidad municipal.	Web	http://www.tramite.munisanmiguel.gob.pe/
2	Pagos en Línea	Es un sistema de pago electrónico a través de internet, que permite al contribuyente pagar y a la entidad municipal cobrar los tributos municipales.	Web	https://servicios.munisanmiguel.gob.pe/frmLogin.aspx?ReturnUrl=%2f
4	Libro de Reclamaciones Virtual	Es una herramienta virtual útil de participación ciudadana, mediante el cual permite a los ciudadanos y ciudadanas formular sus reclamos ante la insatisfacción o disconformidad con la atención brindada por la entidad municipal.	Web	https://reclamos.servicios.gob.pe/?institution_id=145

Fuente: Inventario de la OTIC.

3. Servicios Tecnológicos

Los servicios tecnológicos que brinda la Oficina Tecnologías de la Información y Comunicaciones, están diseñados para mantener un correcto funcionamiento de la plataforma tecnológica de la entidad municipal. Así mismo, permiten brindar una respuesta oportuna a las diferentes eventualidades que en materia de tecnologías de la información pudieran presentarse y afectar el funcionamiento oportuno de la red de datos, equipos tecnológicos, red comunicaciones, entre otros servicios asociados, etc.

Tabla 3 – Descripción de los Catálogos de Servicios Tecnológicos de la MDSM

SERVICIO TI	DESCRIPCION	ALCANCE Y FUNCIONALIDAD	IMPORTANCIA PARA LA MDSM
Impresión y Digitalización	Dentro de la garantía de las maquinas comprende el mantenimiento preventivo, correctivo y garantía a las impresoras.	Este servicio va dirigido a todos los usuarios de la entidad.	Por la cobertura dentro de la entidad y complejidad que maneja en las áreas se cataloga como ALTO.
Telefonía IP	comprende el mantenimiento preventivo, correctivo.	Este servicio va dirigido a todos los usuarios de la entidad municipal.	Funcionalidad de las comunicaciones en voz y datos en las instalaciones de la entidad municipal.

Equipos de Computo	Comprende el mantenimiento preventivo y correctivo de los equipos de cómputo de la entidad municipal.	Este servicio de soporte va dirigido a todos los equipos de cómputo de la entidad municipal.	Funcionalidad del sistema operativo y demás aplicaciones instaladas en los equipos de cómputo de la entidad municipal.
Ofimática	Conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en la entidad municipal para optimizar, automatizar, y mejorar los procedimientos o tareas.	Este servicio de soporte va dirigido a todos los equipos de cómputo de la entidad municipal.	Funcionalidad herramientas informáticas y demás aplicaciones instaladas en los equipos de cómputo de la entidad municipal.
Correo Electrónico	Se refiere a los servicios asociados a la cuenta de correo electrónico, tales como creación y configuración de cuentas de correo.	Este servicio de soporte comprende a la creación y configuración de usuarios que estén previamente autorizados por su jefe inmediato y aprobado por la Oficina de TIC.	El Servicio de Correo Electrónico se brinda para los usuarios y funcionarios de la entidad municipal.
Servidores	Hace referencia a la administración, configuración y disponibilidad de los servidores de la entidad municipal.	Este servicio de soporte va dirigido los servidores que están en el Data center, el cual está ubicado en el piso 6 en la Oficina de TIC de la entidad municipal.	Dirigido · para la continuidad y administración de las aplicaciones que están instaladas en estos servidores de la entidad municipal.
Base de Datos	Servicio para la creación, respaldo, restauración de la Base de Datos que interactúan con las aplicaciones informáticas de la entidad municipal.	Este servicio de soporte va dirigido a las Bases de Datos de Oracle y PostgreSQL, la cual existen en los servidores que se encuentran en el Data Center de la entidad municipal.	Servicio de las Bases de Datos es la que da la continuidad y el funcionamiento de la Aplicaciones informáticas de la entidad municipal.
Data Center	Este servicio incluye servicios de apoyo logístico, instalación de componentes, monitoreo, Backups, mantenimientos, etc..	El Data Center es donde están los Servidores de BD, las aplicaciones que maneja la entidad municipal, también reside la central de telefónica, el Smith Core de comunicaciones, el aire acondicionado, el sistema contra incendios, entre otros.	El Data Center deberá estar en óptimas condiciones en cuanto al sistema eléctrico y aire acondicionado, ya que si estos dos factores no están funcionando se verán afectados los servidores y la comunicación de telefonía.
Seguridad Informática	Actividades orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información y la plataforma tecnológica de la Entidad y sus servicios asociados.	La seguridad Informática de la entidad se basa en el Subsistema de Gestión de Seguridad de la Información, la administración del equipo de seguridad perimetral firewall y Políticas del Directorio activo. Se complementa con protección de equipos con software antivirus y en el caso requerido la encriptación de información.	Por medio de este servicio se controla y garantiza el servicio de Internet, y el óptimo funcionamiento de las aplicaciones WEB que tiene la entidad. Se protegen los equipos de cómputo contra la presencia de software malicioso que pretenda realizar daño o robo de información.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. [illegible] BUSTOS GERENTE OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES

Portales	Servicios asociados con los sitios WEB desarrollados y mantenidos por la entidad municipal con el propósito de divulgar información y ofrecer servicios de interés general para los colaboradores de la entidad o para la ciudadanía.	Está constituido por la página Web e intranet donde se ofrecen los diferentes servicios para usuarios internos y externos de la entidad municipal.	Por medio de este servicio se realizan publicaciones de las diferentes actividades que se realizan en la entidad municipal.
Internet	Administración de la disponibilidad de los servicios de Internet.	El servicio es utilizado por la Sede Principal y por las Sedes remotas de la entidad municipal.	Este servicio es importante para la funcionalidad de las aplicaciones Web, correo electrónico y demás actividades que realiza la entidad municipal con el administrado y otras entidades.
Gestión de Usuarios	Servicio para la creación, modificación, eliminación de usuarios y licencias.	El servicio hace referencia a las solicitudes que realizan los funcionarios para la asignación de usuarios o accesos a los recursos tecnológicos entidad municipal.	Es importante para que los usuarios puedan ingresar a los recursos tecnológicos para realizar sus actividades de acuerdo a sus funciones establecidas por la entidad municipal.
Copias de Respaldo	La Oficina de TIC realiza copia a bases de datos de los sistemas de información y de archivos ubicados en Data Center.	El servicio busca respaldar la información que se considera crítica y mantener su disponibilidad en el momento requerido. Se respalda la información contenida en el sitio de almacenamiento llamado Data Center.	Mantener respaldo de la información considerada como crítica en la entidad municipal y que se encuentra almacenada en las bases de datos de los sistemas de informáticos y de los archivos alojadas en la carpeta institucional.

Fuente: Elaboración propia.

4. Infraestructura

Para soportar los servicios tecnológicos que se entregan a los procesos que realiza la entidad municipal, se tiene establecida una infraestructura tecnológica que está conformada por servicios de conectividad, sistemas de información y elementos físicos; así mismo la entidad municipal, cuenta con un Data Center propio ubicado en la sede PALACIO MUNICIPAL, que tiene conectividad con las demás sedes de la entidad municipal.

La infraestructura tecnológica de la Municipalidad Distrital DE SAN MIGUEL, se encuentra distribuida en las siguientes dependencias que lo conforman.

Tabla 4 - Sedes de la Municipalidad Distrital DE SAN MIGUEL

N°	SEDES / DEPENDENCIA	DIRECCION
01	Palacio Municipal (Sede Principal)	Av. Federico Gallese 370 – San Miguel
02	CASA DE LA CULTURA	Av. Federico Gallese 420- San Miguel
03	CASA DE LA JUVENTUD	Programas sociales: Jr. Castilla 800 - San Miguel
04	SERVICIOS A LA CIUDAD	Servicios a la ciudad: Calle Espinar 131- San Miguel
05	CENTRO INTEGRAL DEL ADULTO MAYOR - CIAM	Jr. Grau #414 – San Miguel
06	OMAPED	Av. F. Gallese #420 – San Miguel
07	MAESTRANZA	Venezuela 30- San Miguel
08	SERENAZGO J.C. TELLO	Complejo habitacional J.C. TELLO- San Miguel
09	CCO – LA MARINA	Av. La Marina 2400- San Miguel
10	PLAZA SAN MIGUEL	Centro Comercial Plaza San Miguel - Sótano 1.
11	SEDE MAGALLANES	Jr. Mariscal Agustín Gamarra 120 - San Miguel

Fuente: Elaboración propia.

Respecto a la conectividad, la Municipalidad Distrital DE SAN MIGUEL se encuentra interconectada con todas las sedes de la entidad municipal mediante una conexión propia de fibra óptica, dicha red se encuentra segmentada por cada sede de la entidad municipal como parte de las buenas prácticas del sistema de gestión de seguridad informática.

Tabla 5 - Interconexión Sedes de la Municipalidad Distrital DE SAN MIGUEL

N°	SEDES / DEPENDENCIA	INTERCONECTA (Fibra/Cobre/Radio Enlace/Otro)	Ancho de Banda Asignada	Consumo de Ancho de Banda en Horario de Oficina
1	Palacio Municipal (Sede Principal)	Av. Federico Gallese 370 – San Miguel.	42MB	75%
2	CASA DE LA CULTURA	Av. Federico Gallese 420- San Miguel	8MB	85%
3	CASA DE LA JUVENTUD	Programas sociales: Jr. Castilla 800 - San Miguel	5MB	85%
4	SERVICIOS A LA CIUDAD	Servicios a la ciudad: Calle Espinar 131- San Miguel	4MB	85%
7	MAESTRANZA	Venezuela 30- San Miguel	4MB	85%
8	SERENAZGO J.C. TELLO	Complejo habitacional J.C. TELLO- San Miguel	5MB	85%
9	CCO – LA MARINA	Av. La Marina 2400- San Miguel	5MB	85%
10	PLAZA SAN MIGUEL	Centro Comercial Plaza San Miguel - Sótano 1.	12MB	85%
11	SEDE MAGALLANES	Jr. Mariscal Agustin Gamarra 120 - San Miguel	5MB	85%

Fuente: Inventario de la OTIC.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

5. Acuerdos de Niveles de Servicios Tecnológicos

La Unidad de Soporte y Comunicaciones, ha considerado los Acuerdos de Niveles de Servicio para la prestación de estos servicios, los cuales son definidos teniendo en cuenta el nivel de complejidad y la afectación que cause sobre la infraestructura tecnológica de la entidad municipal.

Tabla 6 – Acuerdos de Niveles de Servicios del Catálogo de Servicios Tecnológicos de la MDSM

SERVICIO TI	CANALES DE ACCESO	HORARIOS DE DISPONIBILIDAD	HORARIO DE SOPORTE	HORARIO DE USO	REQUISITOS PARA ACCEDER AL SERVICIO
Sistema Integrado de Administración Financiera – SIAF	Los usuarios acceden al sistema a través de la intranet.	Permanente con acceso por medio de la red de la entidad	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Permanente con acceso por medio de la red de la entidad	- Acceso a la red interna. - Computador con sistema operativo Windows XP, 7, 8 o 10.
Sistema Informático tributario Municipal SAMNET	Aplicación cliente/servidor que debe ser instalada en los equipos de cómputo de los usuarios	Permanente con acceso por medio de la red de la entidad	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Permanente con acceso por medio de la red de la entidad	- Acceso a la red interna. - Computador con sistema operativo Windows XP, 7, 8 o 10.
Sistema Informático Municipal de control de gasto - ADMICON	Los usuarios acceden al sistema a través de la intranet.	Permanente con acceso por medio de la red de la entidad	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Permanente con acceso por medio de la red de la entidad	- Acceso a la red interna. - Computador con sistema operativo Windows XP, 7, 8 o 10. - Navegador Mozilla Firefox o Google Chrome
Sistema Informático Municipal de tramite documentario - SISDOC	Aplicación cliente/servidor que debe ser instalada en los equipos de cómputo de los usuarios	Permanente con acceso por medio de la red de la entidad	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Permanente con acceso por medio de la red de la entidad	- Acceso a la red interna. - Computador con sistema operativo Windows XP, 7, 8 o 10 - Navegador Mozilla Firefox o Google Chrome
Mesa de Partes Virtual	Link publicado en la Intranet de la Entidad, utilizando preferiblemente el navegador	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Días hábiles de 8:00 a.m. a 5:00 p.m.	- Navegador Mozilla - Firefox o Google - Chrome - Acceso a internet
Pagos en Línea	Link publicado en la Intranet de la Entidad, utilizando preferiblemente el navegador	7 días 24 horas los 365 días del año.	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Días hábiles de 8:00 a.m. a 5:00 p.m.	- Navegador Mozilla - Firefox o Google - Chrome - Acceso a internet
Libro de Reclamaciones Virtual	Link publicado en la Intranet de la Entidad, utilizando preferiblemente el navegador	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Días hábiles de 8:00 a.m. a 5:00 p.m.	- Navegador Mozilla - Firefox o Google - Chrome - Acceso a internet
Impresión y Digitalización	- Teléfono - Correo Electrónico - WhatsApp - Documento	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Acceso a la red

Conectividad WIFI	Los usuarios (Gerencia Municipal, Sala de Regidores, Alcaldía), acceden al servicio a solicitud formal del funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Tener un usuario válido para acceder a la Red WIFI.
Telefonía IP	Los usuarios acceden al servicio a solicitud formal del funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	---
Equipos de Computo	Los usuarios acceden al servicio a solicitud formal del funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Tener Usuario valido para poder acceder a los Equipos de Cómputo.
Ofimática	Los usuarios acceden al servicio a solicitud formal del funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Tener Usuario valido para poder acceder a los Equipos de Cómputo.
Correo Electrónico	Los usuarios acceden al correo institucional mediante la intranet.	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	- Tener Usuario valido para poder acceder al correo institucional. - Tener acceso a internet
Servidores	Estar autorizado y tener acceso al Data Center	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Tener Aplicaciones en los Servidores que están en el Data Center del piso 6 de la sede Principal.
Base de Datos	Estar autorizado y tener acceso al Data Center	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Tener Aplicaciones que interactúen con las Bases de Datos que están en los Servidores del Data Center de la entidad municipal.
Almacenamiento	Solicitar acceso a la red y servidor de archivos por el funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	Días hábiles de 8:00 a.m. a 5:00 p.m.	- Acceso a la red - Acceso al servidor de archivos
Data Center	Estar autorizado y tener acceso al Data Center	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Estar autorizado para el ingreso a las instalaciones del data center
Seguridad Informática	Estar autorizado de acuerdo a lo establecido en la Directiva para la Seguridad de la Información	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Estar autorizado de acuerdo a lo establecido en la Directiva para la Seguridad de la Información
Portales	Solicitar acceso por el funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Estar autorizado para acceder al portal de la entidad municipal.
Internet	Solicitar acceso por el funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Estar autorizado para acceder a internet de la entidad municipal.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO E. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Gestión de Usuarios	Solicitar acceso por el funcionario responsable	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Estar autorizad mediante una credencial de acceso a los recursos tecnológicos de la entidad municipal.
Copias de Respaldo	La Oficina de TIC, designa un responsable para gestionar las copias de seguridad de los servidores del Data Center.	7 días 24 horas los 365 días del año	Lunes a viernes de 8:00 a.m. a 5:00 p.m.	7 días 24 horas los 365 días del año	Personal calificado de la Oficina de TIC.

Fuente: Elaboración propia.

6. Análisis de Impacto de la Continuidad de los Servicios Tecnológicos

Para la continuidad de los servicios tecnológicos, 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 consideran todos los elementos susceptibles de provocar eventos que conlleven a la activación la contingencia.

Tabla 7 – Análisis de Impacto de Continuidad de los Servicios del Catálogo de Servicios Tecnológicos de la MDSM

N°	SERVICIO TI	DESCRIPCIÓN	CRITICO PARA OPERACIONES INTERNAS	CRITICO PARA OPERACIONES EXTERNAS
1	Internet Corporativo	El servicio de acceso a Internet con flujo de carga (publicación) y descarga (navegación) en la entidad municipal.	Alta	Alta
2	Transmisión de Datos	El servicio de conectividad remota de la Sede Principal con las demás sedes de la entidad municipal.	Alta	Alta
3	Acceso a Dominio	Servicio de autenticación en el dominio de la MDSM, con el uso de credenciales de acceso autorizado.	Alta	Baja
4	Telefonía IP	Servicio de comunicación telefónica por Red IP mediante el uso de Teléfono físico.	Baja	Alta
5	Correo Electrónico	Servicio de mensajería de correo electrónico bajo el dominio **@munisanmiguel.gob.pe**	Media	Media
6	Acceso a Red	El servicio de acceso a Red, permite la conexión de una computadora a la red de datos institucional.	Alta	media
8	Base de Datos	Servicio de repositorio de información indexada en Base de Datos para aplicaciones y servidores del Data Center.	Alta	Alta
10	Estaciones de Trabajo	Equipamiento de cómputo como recurso para el procesamiento de información.	Media	Baja
11	Sistemas de Información Internos	Aplicaciones disponibles para acceso por personal administrativo de la entidad municipal	Alta	Media
12	Sistemas de Información Externos (publicados)	Aplicaciones disponibles para acceso para público en general.	Media	Alta
13	Data Center	Servicio de hosting como infraestructura de soporte para los servicios de TI de la entidad municipal.	Alta	Alta
14	Personal crítico responsable de los procesos TI	Servicios profesionales críticos encargados de procesos de TI de la Oficina de TIC.	Media	Media

Fuente: Elaboración propia.

7. Priorización de Restauración de Servicios de TI

La priorización de la restauración de los servicios de tecnologías de información se realizará según la siguiente manera.

Tabla 7 – Clasificación de Priorización de Restauración de Servicio de TI

N°	DESCRIPCIÓN	PRIORIDAD DE RECUPERACIÓN
1	**ATENCIÓN PRIORITARIA** Sistemas de información y equipos que requieran alta disponibilidad de atención a clientes externos.	1
2	**ATENCIÓN ESTÁNDAR** Sistemas de información y equipos no relacionados con la atención a los clientes externos.	2
3	**ATENCIÓN BAJA** Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información.	3

Fuente: Elaboración propia.

Luego del análisis, considerando la criticidad, se determina de la siguiente manera la priorización de restauración de los servicios de tecnologías de la información:

Tabla 8 – Priorización de Restauración de Servicio de TI

N°	SERVICIO TI	PRIORIDAD
1	Internet Corporativo	1
2	Transmisión de Datos	2
3	Acceso a Dominio	1
4	Telefonía IP	1
5	Correo Electrónico	2
6	Acceso a Red	1
7	Almacenamiento en Servidores	1
8	Base de Datos	1
9	Estaciones de Trabajo	2
10	Sistemas de Información Internos	1
11	Sistemas de Información Externos (Publicados)	1
12	Data Center	1
13	Personal crítico responsable de los procesos TI	2

Fuente: Elaboración propia.

VIII. ANÁLISIS Y EVALUACIÓN DE RIESGOS

Los incidentes que pasan a ser tratados dentro del Plan de Contingencia de TI, serán evaluados de acuerdo con el impacto que puede generar la materialización de alguno de los riesgos identificados en el proceso de Gestión de Tecnologías de la Información, se realiza la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de TI de la entidad municipal, considerando todos los elementos susceptibles de provocar eventos que con lleven la activación de la contingencia.

1. Procesos y Recursos Críticos

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

Tabla 9 – Procesos y Recursos Críticos de TI

N°	PROCESO CRITICO	RECURSOS CRITICOS DE TI	TIEMPO DE RECUPERACION - RTO
1	Gestión de Redes e Infraestructura de TI	Equipos de comunicaciones.	12 horas
		Equipos de protección eléctrica del Data Center (UPS) entre otros.	48 horas
		Sistema de aire acondicionado del Data Center.	24 horas
		Sistema Contra incendio del Data Center	72 horas
		Infraestructura del Data Center.	24 horas
		Cableado de Red de Datos.	24 horas
		Enlaces de cobre y fibra óptica para interconexión entre la sede principal.	12 horas
		Sistema de Almacenamiento (storage)	24 horas
		Medios de Respaldo (Backup)	24 horas
		Servidores de Red criticos: Directorio Activo, File Server, Base de Datos, etc.	72 horas
		Servidores de Red en general: Correo, Desarrollo, Backup, etc.	72 horas
		Central Telefónica IP	24 horas
2	Desarrollo y Mantenimiento de Soluciones Tecnológica	Sistemas y Aplicativos Informáticos	24 horas
		Base de Datos y repositorios utilizados por los sistemas y aplicativos informáticos.	24 horas

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. [illegible] BUSTOS GERENTE OFICINA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

3	Soporte Técnico, de Soluciones y Recursos Tecnológicos	Estaciones de Trabajo del personal crítico (computadoras personales y portátiles)	48 horas
4	Operación y Mantenimiento de TIC.	Personal Crítico responsable de los procesos de TIC.	4 horas

Fuente: Elaboración propia.
Nota: RTO - Tiempo de Recuperación Objetivo, es determinado por Especialistas Expertos de TI.

2. Identificación de Amenazas

En esta etapa se identificará aquellas amenazas que pudieran vulnerar los servicios TI de la entidad municipal, considerando la ubicación geográfica, el contexto actual de la sede principal (Palacio Municipal) y Data Center, así como la percepción del especialista de TI.

Tabla 10 – Amenaza a los Servicios de TI

N°	AMENEZA O EVENTO	TIPO
1	Terremoto/Sismo	Siniestros Naturales
2	Inundación y Aniego en el Centro de Datos.	
3	Incendio en el Data Center.	
4	Falla en Telecomunicaciones.	Tecnológicos
5	Incidente en Seguridad Informática.	
6	Falla de Hardware y Software.	
7	Falla del Suministro Eléctrico en el Data Center y Gabinetes de Comunicación.	Físico y Ambiental
8	Ausencia o no Disponibilidad del Personal Crítico de TI.	Humanos
9	Pandemia y/o Epidemia	Ambiental

Fuente: Elaboración propia.

3. Probabilidad de Ocurrencia

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 ***(Directiva para la Gestión de Riesgos de Seguridad de la Información en la MDSM),*** se muestra a continuación.

Tabla 11 – Escala de Determinación de la Probabilidad de Ocurrencia

PROBABILIDAD	VALOR	DESCRIPCIÓN	FRECUENCIA
Muy Baja	1	El evento puede ocurrir solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años o más.
Baja	2	El evento podría ocurrir en algún momento.	Se puede presentar al menos una vez en los últimos 5 años.
Media	3	El evento probablemente ocurrirá en la mayoría.	Se puede presentar al menos en los dos últimos años.

Alta	4	Se espera que el evento ocurra en la mayoría de las circunstancias.	Se puede presentar al menos una vez al año.

Fuente: Directiva para la Gestión de Riesgos de Seguridad de la Información en la MDSM.

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:

Tabla 12 – Probabilidad Estimada de las Amenazas a los Servicios de TI

N°	AMENEZA O EVENTO	Nivel de Probabilidad de ocurrencia (valor)	Nivel de Probabilidad Estimada
1	Terremoto/Sismo	2	Baja
2	Inundación y Aniego en el Centro de Datos.	1	Muy Baja
3	Incendio en el Data Center.	1	Muy Baja
4	Falla en Telecomunicaciones.	3	Media
5	Incidente en Seguridad Informática	4	Alta
6	Falla de Hardware y Software.	3	Media
7	Falla del Suministro Eléctrico en el Data Center y Gabinetes de Comunicación.	3	Media
8	Ausencia o no Disponibilidad del Personal Crítico de TI.	2	Baja
9	Pandemia y/o Epidemia	2	Baja

Fuente: Elaboración propia.

4. Identificación del Impacto

El impacto del riesgo mide la gravedad o magnitud del efecto adverso a causa de la ocurrencia de la amenaza. Es una calificación aplicada a la amenaza, para describir el grado de afectación. La medición puede ser cualitativa o cuantitativa.

Para nuestro caso la clasificación del impacto será en una escala 1 al 4 categorizando desde los niveles Muy Bajo hasta Alto, tal como se muestra en la siguiente tabla.

Tabla 13 – Escala de Determinación del Impacto del Riesgo

IMPACTO	VALOR	DESCRIPCIÓN	SEGURIDAD DE LA INFORMACIÓN
Insignificante	1	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la entidad municipal.	Afecta a una actividad del proceso.
Menor	2	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad municipal.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.

Moderado	3	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la entidad municipal.	Afecta un conjunto de datos personales o el proceso.
Mayor	4	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la entidad municipal.	Afecta varios conjuntos de datos personales o procesos de la entidad municipal o toda la entidad municipal. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la entidad municipal.

Fuente: Directiva para la Gestión de Riesgos de Seguridad de la Información en la MDSM.

El valor obtenido en el cuadro anterior, ha sido en base a la metodología de gestión de riesgos, que ha determinado el impacto por cada amenaza, siendo el resultado siguiente.

Tabla 14 – Resultado de la Determinación del Impacto de los Servicios de TI

ITEM	RECURSOS CRITICOS DE TI AMENEZAS (EVENTOS)	Terremoto	Inundación y aniego en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Incidente de Seguridad informática	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	4	4	4	4	4	2	3	2	1
2	Equipos de protección eléctrica del Data Center (UPS) entre otros.	4	4	4	2	1	2	4	3	1
3	Sistema de aire acondicionado del Data Center.	4	4	4	1	1	2	4	3	1
4	Sistema Contra incendio del Data Center	4	4	4	1	1	2	4	3	1
5	Infraestructura del Data Center.	4	4	4	1	1	3	4	4	3
6	Cableado de Red de Datos.	4	4	4	3	1	1	3	2	1
7	Sistema de Almacenamiento (storage)	4	4	4	3	4	2	4	3	1
8	Servidores de Red	4	4	4	3	4	2	4	4	1
9	Medios de Respaldo (Backup)	4	4	4	3	2	2	3	3	1
10	Sistemas de Información y Portales Web	4	4	4	3	4	2	4	4	1
11	Base de Datos utilizados por los sistemas y aplicativos informáticos	4	4	4	3	4	2	4	4	1
12	Estaciones de Trabajo del personal crítico (computadoras personales y portátiles)	4	4	4	3	4	2	3	3	2

Fuente: Elaboración propia.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

5. Cálculo del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un Servicio de TI de la Municipalidad Distrital DE SAN MIGUEL, se ha considerado los controles existentes que mitigan la afectación de las amenazas y/o el impacto descritas en el punto anterior. Para la identificación del Nivel de Riesgo se considera la siguiente matriz.

Tabla 15 – Matriz de Valoración del Riesgo

Impacto / Probabilidad	Mayor (4)	Moderado (3)	Menor (2)	Insignificante (1)
Alta (4)	Alto(16)	Alto (12)	Alto (8)	Medio (4)
Media (3)	Alto (12)	Alto (9)	Medio (6)	Medio (3)
Baja (2)	Alto (8)	Medio (6)	Medio (4)	Bajo (2)
Muy Baja (1)	Medio (4)	Medio (3)	Bajo (2)	Bajo (1)

Fuente: Directiva para la Gestión de Riesgos de Seguridad de la Información en la MDSM.

En función a los factores mencionados, se define al nivel de riesgo como la multiplicación del Impacto y su Probabilidad de Ocurrencia.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Nivel de riesgo (Ri) = **Impacto** (Ri) x **Probabilidad** (Ri)

Con base en la determinación de la Probabilidad y la Valoración del Impacto, se establecen los Niveles de Riesgos, teniendo una clasificación propia para la entidad municipal, del cual se interpreta de la siguiente.

Municipalidad Distrital de San Miguel V°B° RICARDO ALEGRIADO BUSTOS GERENTE

Tabla 16 – Matriz de Niveles de Riesgo

DIMENSIÓN DEL RIESGO DE SEGURIDAD DE INFORMACIÓN	VALOR	ACCIÓN REQUERIDA
Riesgo Alto	Mayor a 6	Evitar el riesgo, empleando controles que busquen reducir el nivel probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Moderado	Menor a 7 y Mayor a 2	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permiten llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Bajo	Menor a 3 y Mayor a 0	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones preventivas.

Fuente: Directiva para la Gestión de Riesgos de Seguridad de la Información en la MDSM.

En concordancia y alineación con los Niveles de Riesgos, las acciones requeridas se contemplan en la siguiente tabla.

Tabla 17 – Interpretación del Cuadrante de Calor o Nivel de Riesgo

DIMENSIÓN DEL RIESGO	ACCIÓN REQUERIDA
Zona de Riesgo Bajo	**Aceptar el Riesgo:** Riesgos para los cuales se determinan que el nivel de exposición es adecuado y por lo tanto es aceptable.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Alto	**Evitar el Riesgo:** Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

Fuente: Directiva para la Gestión de Riesgos de Seguridad de la Información en la MDSM.

A continuación, se obtiene el resultado de la **Evaluación del Riesgo** de los servicios de TI:

Tabla 18 – Resultado de la Evaluación de Riesgos de los Servicios de TI

ITEM	RECURSOS CRITICOS DE TI AMENEZAS (EVENTOS)	Terremoto	Inundación y aniego en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Incidente de Seguridad informática	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI
1	Equipos de comunicaciones.	16	16	16	16	16	4	9	4
2	Equipos de protección eléctrica del Data Center (UPS) entre otros.	16	16	16	4	1	4	16	9
3	Sistema de aire acondicionado del Data Center.	16	16	16	1	1	4	16	9
4	Sistema Contra incendio del Data Center	16	16	16	1	1	4	16	9
5	Infraestructura del Data Center.	16	16	16	1	1	9	16	16
6	Cableado de Red de Datos.	16	16	16	9	1	1	9	4
7	Sistema de Almacenamiento (storage)	16	16	16	9	16	4	16	9
8	Servidores de Red	16	16	16	9	16	4	16	16
9	Medios de Respaldo (Backup)	16	16	16	9	4	4	9	9
10	Sistemas de Información y Portales Web	16	16	16	9	16	4	16	16
11	Base de Datos utilizados por los sistemas y aplicativos informáticos	16	16	16	9	16	4	16	16
12	Estaciones de Trabajo del personal crítico (computadoras personales y portátiles)	16	16	16	9	16	4	3	9

Fuente: Elaboración propia.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVA PALOSA SUB GERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

6. Identificación de Controles Existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los servicios de TI de la MUNICIPALIDAD DISTRITAL DE SAN MIGUEL, frente a cada amenaza; los controles existentes son:

Municipalidad Distrital de San Miguel V°B° RICARDO C. ARTEAGA BUSTOS GERENTE OFICINA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

a. Sistema de control de acceso al Data Center.
b. Mantenimiento para equipos de aire acondicionado del Data Center; que ésta a cargo de la Unidad de Logística y Control en coordinación con la Oficina de Administración y Finanzas.
c. Sistema de alarma contra incendios en el Data Center, que ésta a cargo de la Unidad de Logística y Control en coordinación con la Oficina de Administración y Finanzas.
d. Mantenimiento de UPS.

e. Respaldo de información en discos externos almacenadas en el Data Center.
f. Solución antivirus instalada en los servidores de red y computadoras.
g. Actualización mensual de parches de seguridad de sistemas operativos en servidores.
h. Seguridad perimetral gestionada.
i. Redundancia en los enlaces de comunicaciones de fibra óptica sede Palacio (Data Center)

7. Escenarios de Riesgos

Considerando los servicios de TI, y luego de realizar el análisis de riesgos, se han determinado los siguientes escenarios de riesgo:

a. Destrucción e indisponibilidad del Data Center por terremoto.
b. Falla en el funcionamiento de los sistemas de información 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 del Data Center, o los gabinetes de comunicación de la Sede Principal (Palacio Municipal).

A continuación, se muestra el consolidado de los ***Escenarios de Riesgos*** y su ***Impacto***, para activar el Plan de Contingencia de TI.

Tabla 19 – Escenarios de Riesgos de los Servicios de TI

ITEM	ESCENARIO DE RIESGO	DESCRIPCIÓN	IMPACTO
1	Destrucción e indisponibilidad del Data Center por terremoto.	Este escenario consiste en que el Data Center 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 Data Center, como también los componentes del mismo.	Alto
2	Indisponibilidad de servidores críticos por falla de hardware o software.	En este escenario se considera la indisponibilidad de los servicios críticos causados por una falla física o lógica de los servidores.	Alto
3	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque.	En este escenario se considera la indisponibilidad de los sistemas de información como resultado de un ciberataque.	Alto
4	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Data Center.	En este escenario se considera que el suministro de energía eléctrica del Data Center se encuentre indisponible ocasionando la indisponibilidad de los servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica y la comunicación con la Sede Principal (Palacio Municipal).	Alto

5	Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal crítico.	En este escenario se considera que no se encuentra disponible el personal necesario para la administración y gestión de la infraestructura tecnológica y servicios de tecnología, lo cual puede traer como consecuencia la indisponibilidad de los mismos.	Alto
6	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones.	En este escenario se considera que los equipos de redes y comunicaciones se encuentren indisponibles como resultado de una falla física o lógica, lo cual trae como consecuencia la caída de servicios informáticos y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.	Alto

Fuente: Elaboración propia.

IX. ASPECTOS GENERALES PARA LA ATENCION DE UNA CONTINGENCIA

El Plan de Contingencias de TI, se activa frente a una situación de interrupción de un servicio y/o infraestructura de TI o de acuerdo con lo determinado por el procedimiento de Gestión de Incidentes de Seguridad y/o lo que exprese el nivel estratégico o táctico del plan de contingencias de TI.

A continuación, se presentan las actividades generales que se deben tener en cuenta por los roles definidos.

Tabla 20 – Actividades y Responsables para el Manejo de Contingencias de TI en la MDSM

ACTIVIDAD	RESPONSABLE	ACCIÓN
1	Usuarios y/o Funcionarios de las Unidades Orgánicas	Reportar la falla por cualquier canal de comunicación (correo, teléfono, WhatsApp), siguiendo el procedimiento de Atención de Requerimientos de Soporte a los sistemas de información y equipos informáticos.
2	Personal de Soporte Técnico de Hardware Personal de Soporte de Software (Sistemas y Aplicativos)	Analiza la falla. En caso de corresponder a un incidente de seguridad digital, traslada la acción al procedimiento de Gestión de Incidentes de Seguridad Digital. Si la situación no es un incidente de seguridad, pero afecta la operación de algún servicio de TI, informa a la Unidad de Soporte y Comunicaciones para la toma de decisiones.
3	Equipo de Respuesta ante Incidentes de Seguridad Digital	Evalúa y determina si el incidente corresponde a una contingencia. En este caso informa al responsable del Plan de contingencias de TI.
4	Gerente de Tecnologías de la Información y Comunicaciones	Autoriza la puesta en marcha del Plan de Contingencia de TI, notificando a las áreas afectadas y a los Niveles Estratégico y Táctico del Plan de Contingencias de TI.

5	Gestores del Plan de Contingencia Jefatura de Soporte, Redes y Telecomunicaciones Oficial de Seguridad y Confianza Digital	Gestiona las actividades del Plan de Contingencia de TI, asignando al personal que realizaran las labores operativas de recuperación según el tipo de interrupción y los servicios y/o infraestructura afectada.
6	Líder del Plan de Contingencia de TI Equipos de atención de la contingencia de acuerdo con la especialidad	Ejecuta las actividades de recuperación junto con el equipo de atención e informa al Gestor del Plan de Contingencia de TI (según lo descrito en el escenario de contingencia a solucionar). Realiza pruebas de recuperación del servicio y/o infraestructura afectada y reporta al Gestor del Plan de Contingencia la finalización de las actividades implementadas.
7	Gestores del Plan de Contingencia Jefatura de Soporte, Redes y Telecomunicaciones Oficial de Seguridad y Confianza Digital	Informa al Gerente de Tecnologías de la Información y Comunicaciones la finalización de las actividades de recuperación. Coordina las actividades para el restablecimiento de la operación normal de los servicios de TI.
8	Líder del Plan de Contingencia de TI Equipos de atención de la contingencia de acuerdo con la especialidad	Inicia las acciones pertinentes para el restablecimiento del proceso normal (según lo descrito en el escenario de contingencia a solucionar).
9	Líder del Plan de Contingencia de TI	Actualiza Hoja de vida del equipo, servidor o del sistema de información sobre la incidencia presentada.
10	Gerente de Tecnologías de la Información y Comunicaciones Gestores del Plan de Contingencia Oficial de Seguridad y Confianza Digital Líder del Plan de Contingencia de TI	Realizar análisis de las fallas presentadas y de los indicadores del proceso. Documenta los resultados y lecciones aprendidas.
11	Gerente de Tecnologías de la Información y Comunicaciones	Autoriza la finalización del plan. Informa a las unidades orgánicas afectadas la normalización en la prestación de los servicios de TI. Autoriza el cierre de la contingencia e informa al Comité de Gobierno Digital y a la Gerencia Municipal, el balance de la situación de contingencia atendida.

Fuente: Elaboración propia.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALTAMIRANO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

1. Es Sistemas de Información y Aplicaciones

a. Realizar inventario de los Sistemas de Información y/o Aplicativos afectados de acuerdo con las características relacionadas en el documento Plan de Contingencias de TI.
b. Preparar y configurar un equipo de cómputo de acuerdo con las características y condiciones de conectividad especificadas relacionadas en el documento Plan de Contingencias de TI del Sistema de Información y/o Aplicación afectado.
c. Restaurar copia de seguridad de la base de datos correspondiente, así como la copia de respaldo más reciente del código fuente o del archivo de instalación o ejecutable.
d. Revisar permisos de acceso y cuentas de usuario del sistema de información afectado.
e. Verificar la conexión entre la base de datos y el sistema y/o aplicativo.
f. Realizar pruebas de procesamiento y transaccionalidad de datos entre los sistemas y/o aplicativos en el equipo dispuesto para la atención de la contingencia.
g. Paralelo a estas actividades, en el sistema afectado, se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan de Contingencias de TI.
h. En caso de que la contingencia se presente en un servicio, sistema de información y/o aplicativo que cuente con un soporte técnico y/o garantía, se debe informar al proveedor la contingencia presentada, monitorear los acuerdos de niveles de servicio establecidos contractualmente y gestionar la atención y restauración del servicio con el proveedor.

2. Recursos Tecnológicos e Infraestructura

a. Realizar inventario físico de la infraestructura afectada de acuerdo con las características relacionadas en el documento Plan de Contingencia de TI.
b. Determinar las características técnicas de la infraestructura física afectada.
c. Con la infraestructura no afectada y dependiendo la situación presentada, realizar las actividades planteadas en los diferentes escenarios para atender la contingencia y restaurar el servicio de TI afectado.
d. Verificar las conexiones entre servicios de TI y la infraestructura dispuesta para la atención de la contingencia.
e. Realizar pruebas de transaccionalidad de datos y/o conexiones en el equipo dispuesto para la atención de la contingencia.
f. Paralelo a estas actividades, en la infraestructura afectada se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan de Contingencia de TI.
g. En caso de que la contingencia se presente en infraestructura que cuente con un soporte técnico y/o garantía, se debe informar al contratista la

contingencia presentada, monitorear los acuerdos de niveles de servicio establecidos contractualmente y gestionar la atención y restauración del servicio con el contratista.

3. Recurso Humano

El personal asignado por parte de la Unidad de Soporte y Comunicaciones para la atención de una contingencia que afecte un servicio de TI, deberá de existir un directorio de contacto, el mismo que será distribuido en todas las unidades orgánicas de la entidad, de acuerdo al siguiente formato.

Tabla 21 – Directorio de Contacto del Equipo Designado para la Atención de Contingencias de TI en la MDSM

REPONSABLE	ROL	CANAL DE CONTACTO		
		COREO ELECTRONICO	TELÉFONO	ANEXO
Gerente de OTIC	Responsable del Plan de Contingencia de TI.			
Jefe de la Jefatura de Soporte, Redes y Telecomunicaciones	Gestor del Plan de Contingencia de TI			
Oficial de Seguridad y Confianza Digital	Gestor del Plan de Contingencia de TI			
Profesional de TI	Líder del Plan de Contingencia			
Profesional de TI	Administrador de Redes			
Profesional de TI	Administrador de Base de Datos y Servidores			
Profesional de TI	Administrador de Sistemas de Información y/o Aplicativos			
Profesional de TI	Administrador del Data Center			

Fuente: Elaboración propia.

4. Aspectos Logísticos

Cuando ocurra una situación inesperada que conlleve a la materialización de un riesgo identificado en este Plan de Contingencia de TI, el usuario afectado, funcionario afectado, deberán reportarlo de inmediato mediante un Correo Electrónico, WhatsApp o Teléfono a la Oficina de Tecnologías de la Información. Una vez reportada, la contingencia se activará por parte de la Oficina de TIC, el respectivo procedimiento para el manejo de la interrupción.

X. ESTRATEGIAS DE RECUPERACION

Se proponen las posibles soluciones de recuperación de los escenarios de riesgos, incluyendo estrategias preventivas y correctivas. En ese sentido se han seleccionado alternativas para los escenarios de amenaza identificados que cumplen con los tiempos de recuperación, seguidamente, se indican las posibles estrategias de recuperación:

1. **Destrucción de los recursos informáticos alojados en el centro de datos como resultado de un sismo, inundación o incendio.**

   a. Implementar un Data Center de contingencia en las instalaciones de la central de operaciones del sector 10 (base Julio C. Tello), se deberá analizar costo beneficio para implementar con un proveedor de hosting, además que en caso se presente un escenario de sismo, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos.
   b. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware.
   c. Realizar copias de respaldo de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
   d. Almacenar las copias de respaldo diarias en un ambiente separado del Data Center.
   e. Analizar costo beneficio y confidencialidad para contratar el servicio de almacenamiento de las copias de respaldo a cargo de proveedor externo, con un periodo mínimo semanal de retiro de copias de respaldo hacia las instalaciones externas.
   f. Asegurarse de contar con conexión redundantes el Data Center en Palacio Municipal (Sede Principal).
   g. Contar con Switches de respaldo que como mínimo sean de capa 3 de modelo OSI para uso de Core y Distribución.
   h. Eliminar todo material inflamable del ambiente del Data Center y la sala de UPS.
   i. Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías.

2. **Indisponibilidad de servidores críticos por falla de hardware o software.**

   a. Implementar alta disponibilidad en los servidores virtualizados.
   b. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware.
   c. Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los servidores físicos
   d. Programación de revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

3. **Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque.**

   a. Mantener actualizado los parches de seguridad en servidores y estaciones de trabajo.
   b. Mantener actualizado el software de protección anti-malware en cada servidor y estación de trabajo.
   c. Mantener controles de seguridad perimetral como Firewall, UTM gestionado, AntiDoS, etc.
   d. Contratar el servicio de seguridad de aplicaciones Web como WAF.

Municipalidad Distrital de San Miguel V°B° RICARDO ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

e. Desarrollar planes de sensibilización en materia de seguridad de la información y buenas prácticas en el uso de los sistemas informáticos.
f. Mantener el monitoreo del rendimiento y consumo de los recursos en los servidores.
g. Realizar pruebas anuales de Hacking Ético de terceros especializados.

4. Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos.

a. Contratar un servicio de mantenimiento preventivo y correctivo para el UPS, pozo a tierra y banco de baterías.
b. Implementar un sistema de UPS redundante con circuitos independientes que alimenten a los servidores y quipos críticos del Centro de Datos.
c. Configurar el monitoreo remoto del UPS con alertas en caso de detectarse falla en el suministro eléctrico y/o banco de baterías.
d. Realizar el apagado de los equipos, mientras se cuente con energía del UPS.
e. Evaluar el implementar un generador eléctrico para proveer energía al Data Center en casos de falla de la red eléctrica pública.
f. Realizar pruebas del tablero de transferencia (Bypass) en el suministro eléctrico, para asegurar una mínima interrupción de energía ante trabajos de mantenimiento.

5. Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal crítico.

a. Eliminar la dependencia funcional de los puestos críticos, capacitando a un reemplazo para cada rol, de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto.
b. Entrenar al personal de la Oficina de TIC 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 se ha logrado sus objetivos.
c. Elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de la Oficina de TIC, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.

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

6. Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones.

a. Contar con Switches de respaldo que como mínimo sean de capa 3 de modelo OSI, almacenados en un ambiente separado del Data Center.
b. Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones.

c. Mantener los Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los equipos de comunicaciones del Data Center.

Es importante precisar, para la contratación de los bienes y servicios que se requiera para la implementación del presente Plan de Contingencia de TI, el requerimiento del bien o servicio (adjuntando las especificaciones técnicas o términos de referencia, según sea el caso), deberán ser remitidos a la Oficina de Administración y Finanzas, para que la Subgerencia de Logística y Patrimonio, continúe con el proceso de contratación correspondiente, de conformidad a la Ley N° 30225, Ley de Contrataciones del Estado (y modificatorias) y el Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado (y modificatorias).

XI. PLAN DE RECUPERACION

El plan de recuperación es la clave para asegurar que la entidad municipal pueda seguir operando y prestando sus servicios a los contribuyentes y ciudadanía en general, así como para minimizar pérdidas económicas y de reputación, derivadas por eventos de incidentes.

1. Invocación del Plan

Este mecanismo define cuándo, cómo y por quién se pone en ejecución el proceso de recuperación de los Servicios de TI que se encuentran en el Data Center.

Tabla 22 – Invocación para la Ejecución del Plan de Contingencias de TI en la MDSM

N°	ESCENARIO	DETECTA SITUACIÓN	ESTRATEGIA	EJECUTA EL PLAN	AUTORIZA LA ACTIVACIÓN DEL PLAN
1	Destrucción del Data Center como resultado de un sismo, inundación o incendio.	Personal de la MDSM	Activación del Plan de Contingencia de TI	Equipo de Atención de la Contingencia de TI	OTIC
2	Indisponibilidad de servidores críticos físicos por falla de hardware o software.	Personal de la MDSM	Activación del Plan de Contingencia de TI	Equipo de Atención de la Contingencia de TI	OTIC
3	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque.	Personal de la MDSM	Activación del Plan de Contingencia de TI	Equipo de Atención de la Contingencia de TI	OTIC
4	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Data Center.	Personal de la MDSM	Activación del Plan de Contingencia de TI	Equipo de Atención de la Contingencia de TI	OTIC
5	Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal crítico.	Personal de la MDSM	Activación del Plan de Contingencia de TI	Equipo de Atención de la Contingencia de TI	OTIC
6	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones.	Personal de la MDSM	Activación del Plan de Contingencia de TI	Equipo de Atención de la Contingencia de TI	OTIC

Fuente: Elaboración propia.

2. Notificación de Invocación del Plan

La notificación es responsabilidad del Gerente de la OTIC, quien está autorizada para invocar el Plan de Contingencia de TI e informar a los Gestores del Plan de Contingencia de TI y al Líder del Plan de Contingencia de TI, quien liderara la ejecución de las actividades en coordinación con el Equipo de Atención de la Contingencia de TI, para adoptar las acciones necesarias de la contingencia. Así mismo el Oficial de Seguridad y Confianza Digital, deberá realizar el seguimiento de todo el proceso de la contingencia.

3. Plan de Contingencia y Recuperación de Servicios de TIC

El Plan de Recuperación de los Servicios de Tecnología de la Información está alineado a los escenarios de mayor nivel de riesgo, identificados en la Matriz de Riesgos, los cuales serán abordados en planes independientes, tal como se indica en el siguiente cuadro.

Tabla 23 – Invocación para la Ejecución del Plan de Contingencias de TI en la MDSM

N°	ESCENARIO	NIVEL DE RIESGO	PLAN DE RECUPERACIÓN
1	Destrucción del Data Center como resultado de un sismo, inundación o incendio.	Alto	PR-01
2	Indisponibilidad de servidores críticos físicos por falla de hardware o software.	Alto	PR-02
3	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque.	Alto	PR-03
4	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Data Center.	Alto	PR-04
5	Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal crítico.	Medio	PR-05
6	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones.	Alto	PR-06

Fuente: Elaboración propia.

Nota:

Los Planes de Recuperación (PR-01, PR-02, PR-03, PR-04, PR-05, y PR-06), se encuentra establecido en el **Anexo 01 – "Planes de Recuperación"**

XII. 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 si pueden ser empleados y replicados en una hipotética situación de contingencia.

Esta estrategia define los aspectos básicos que requieren ser probados periódicamente, a fin de medir el comportamiento integral e individual de los recursos asignados y/o los procedimientos definidos para la atención de una interrupción de un servicio de TI.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por el Equipo de Atención de la Contingencia de TI, 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 de Contingencia de TI.

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 / lugar de prueba / personal involucrado)
- Resultado Esperado
- Resultado Obtenido

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 municipal, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado en el **Anexo 02 – "Formato de Documentación de Pruebas del Plan de Contingencia de TI"**.

1. Propósito y Alcance

El propósito del Plan de Pruebas es validar las actividades del Plan de Contingencia de TI, las capacidades del personal de TI en la ejecución del plan y verificar que el desarrollo de las actividades sea correcto.

El alcance de las pruebas del Plan de Contingencia de TI, es probar el restablecimiento de la operatividad de los recursos que forman parte de los escenarios de riesgo.

2. Tipos y Frecuencia de Pruebas

La programación de las pruebas obedece a varios factores entre los cuales se pueden mencionar:

a. Programación periódica establecida con los equipos de administración de sistemas de información y plataforma tecnológica como mecanismo de control de calidad de la función de contingencia. (por ejemplo, después de la terminación de un proyecto, a los tres (3) meses y posteriormente cada 6 meses).

b. Cuando se realicen modificaciones de hardware, software operativo, de infraestructura y/o aplicativos; o cuando existan cambios significativos en la plataforma tecnológica cubierta por el Plan de Contingencia de TI.

c. También pueden realizarse cuando se prevea el riesgo de que suceda un evento que afecte la entidad municipal, como problemas laborales o de orden público.

Desde el punto de vista del cubrimiento o alcance, los tipos de pruebas pueden ser:

2.1. Pruebas de Escritorio (Detallada y Documental)

Se trata de un tipo de prueba programada y controlada que consiste en una revisión detallada del Plan de Contingencia de TI y los procedimientos implicados. Para su ejecución se verifica la existencia del plan y sus procedimientos, y se convoca al personal de la Unidad de Soporte y Comunicaciones responsables del proceso o sistema de información a participar en un taller en donde se da lectura al Plan en forma ordenada, bajo la moderación del responsable del Plan de Contingencia de TI, con el fin de determinar fallas y omisiones con el criterio experto de quienes participan. En este ejercicio se tienen en cuenta las dependencias de las diferentes actividades.

Es recomendable ejecutar este tipo de prueba antes de ejecutar una prueba real y una vez sea publicada alguna actualización del presente Plan de Contingencia de TI.

2.2. Pruebas Reales (Tecnológicas)

Municipalidad Distrital de San Miguel V°B° RENATO ALVAREZ LLAMOCCA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Este tipo de prueba puede ser parcial o total, donde se prueban secciones o elementos individuales del Plan de Contingencia de TI, como puede ser, un aplicativo o una plataforma o se prueban todos los componentes. Las pruebas reales, lo determinará el Líder del Plan de Contingencia de TI en coordinación con el responsable del Plan de Contingencia de TI (Gerente de OTIC).

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Asimismo, las Pruebas Reales, lo cual se consideran las principales para realizar, se describen a continuación:

a. **Prueba General:** Consiste en probar el desempeño de la plataforma tecnológica designada para la contingencia de TI en un ambiente de interrupción total, la cual consiste en realizar un simulacro donde se compruebe de manera integral la ejecución de las siguientes actividades:

- Prueba de Conocimiento del Plan de Contingencia de TI, para verificar que el personal de la contingencia quede familiarizado con el plan y que asuma sus responsabilidades asignadas exitosamente ante una suspensión de servicio de TI. ***Anexo 03 - "Formato de Evaluación de Conocimiento del Plan de Contingencia de TI".***

- Pruebas de suministro de energía eléctrica con UPS. (Corte del servicio de energía y verificación de la entrada de las UPS en funcionamiento). ***Anexo 02 – "Formato de Documentación de Pruebas del Plan de Contingencia de TI".***

- Prueba de Conexión Alterna Sede Principal (Palacio Municipal). ***Anexo 02 – "Formato de Documentación de Pruebas del Plan de Contingencia de TI".***

- Prueba de Puesta en producción de los equipos de respaldo y sistemas de información de la entidad municipal. ***Anexo 02 – "Formato de Documentación de Pruebas del Plan de Contingencia de TI".***

- Prueba de Recuperación de la información de las copias de respaldo de información, para verificar su correcto proceso de restauración (de acuerdo con lo descrito en el Procedimiento para la Realización y Control de Copias de Respaldo). ***Anexo 02 – "Formato de Documentación de Pruebas del Plan de Contingencia de TI".***

b. Prueba de Conocimiento del Plan de Contingencia de TI: Esta prueba se enfoca principalmente en entrenar al equipo que ejecutara con éxito el plan de contingencia de TI, solucionando el problema y reestableciendo a la normalidad las actividades realizadas.

La prueba consiste en enfocar los procesos críticos, usuarios de los procesos críticos, equipamiento, software y servicios que utilizan los procesos críticos.

Definir el ambiente donde se realizará las reuniones del equipo de recuperación de la contingencia. No dejar de lado los resultados obtenidos, la meta es aprender y descubrir las vulnerabilidades, no dejar fracaso y frustración, y finalmente repasar continuamente el Plan de Contingencia de TI.

c. Pruebas de Suministro de Energía Eléctrica con UPS: Los sistemas de alimentación ininterrumpida - UPS (Uninterruptible Power Supply), son el sistema que garantiza la energía eléctrica a los equipos de informáticos de la entidad municipal cuando haya una suspensión de este servicio.

La prueba consiste en verificar la activación automática de la puesta en marcha de la UPS cuando se suspende la energía eléctrica. Adicionalmente se puede realizar prueba de autonomía, la debe mantener el suministro energía a los equipos conectados a la red eléctrica regulada.

Esta prueba se realiza manteniendo una cantidad determinada de equipos de cómputo y servidores activos, se corta el fluido eléctrico normal.

d. **Prueba de Conexión Alterna en la Sede Principal (Palacio Municipal):** Consiste en desconectar el canal de conexión principal fibra óptica, para que entre en servicio la redundancia de este, la prueba se realiza con servicios activos e inactivos y estos deberán continuar funcionando en tiempo real sin inconvenientes.

e. **Prueba de Puesta en Producción de los Equipos de Respaldo:** Consiste en instalar y preparar los equipos de contingencia de los sistemas definidos por el equipo de contingencias, los cuales serán ubicados en la sede alterna o en la locación definida para la prueba, con las características técnicas requeridas de acuerdo con los servicios de TI que se requieran con el fin de verificar el funcionamiento y puesta en producción.

f. **Prueba de Restauración de Información:** Consiste en realizar una restauración de las copias de seguridad más reciente que se tienen de los sistemas de información y/o aplicativos informáticos, que seleccione el Líder del Plan de Contingencia de TI, utilizando los procedimientos existentes de restauración y verificar la comunicación entre los aplicativos y las bases de datos.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

2.3. Evaluación de la Prueba

Una vez se haya realizado la prueba y como actividad final, es necesario efectuar una evaluación o revisión de su desarrollo en la cual estén analizados los objetivos, los parámetros, los criterios establecidos, las fallas y fortalezas.

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

2.4. Etapas de la Prueba

A continuación, se presentan las etapas que se deben realizar para el desarrollo de una prueba al Plan de Contingencias de TI.

Tabla 24 – Etapa de Pruebas al Plan de Contingencias de TI en la MDSM

ITEM	ETAPA	DESCRIPCIÓN
1	Planeamiento de la prueba.	Definir los equipos participantes, los objetivos específicos de la prueba y confirmar con la localidad alterna la fecha y hora de realización.
2	Notificación de la prueba a los equipos de trabajo.	Notificar a los equipos participantes la realización de la prueba y verificar que todos ellos estén enterados.
3	Alistamiento y habilitación de los sitios alternos para la prueba.	Incluye contar con todos los elementos necesarios para iniciar el proceso de prueba.
4	Puesta en producción de los equipos de cómputo o sistemas de información en la sede alterna que se haya determinado para la prueba.	Actividades de los equipos de recuperación tendientes a restaurar y sincronizar los Aplicaciones.
5	Operación en los sitios alternos para la prueba.	Actividades de los equipos de recuperación tendientes a probar la operación en los sitios alternos para los equipos de contingencia.
6	Limpieza de los datos después de la prueba.	Borrar todos los archivos sensibles en la localidad alterna de contingencia.
7	Evaluación de la prueba.	Reunirse con el personal que participó en la prueba para identificar problemas y aciertos del plan de contingencia de TI.

Fuente: Elaboración propia.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

2.5. Escenarios y Estrategias

Los escenarios de pruebas deben simular la inhabilitación de las operaciones en el Data Center, con el fin de realizar una prueba que contemple la ejecución de los planes de acción descritos en Plan de Contingencia de TI, es importante que estas pruebas se coordinen con las áreas usuarias.

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALBUJADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Ejemplo de escenarios que se deberán considerar en la en las pruebas del Plan de Contingencia de TI:

Tabla 25 – Escenario 01 – Prueba de Conocimiento del Plan de Contingencia de TI

ESCENARIO 01	PRUEBA DE CONOCIMIENTO DEL PLAN DE CONTINGENCIA DE TI
RESPONSABLE	Gestor del Plan de la Contingencia de TI
PERIOCIDAD	Semestral / Anual
DESCRIPCIÓN	

Este escenario consiste en evaluar mediante un test escrito el nivel de conocimiento del Equipo del Plan de Contingencia de TI, así como sus responsabilidades.

Después de la Prueba:

El responsable debe elaborar un informe de los resultados obtenidos que contenga los siguientes puntos:

- Tipo de prueba.
- Día.
- Duración.
- Participantes.
- Resultados.
- Acciones Correctivas

De ser necesario se deberá actualizar el Plan de Contingencia de TI con las lecciones aprendidas de ésta prueba.

Nota:

Considerar lo establecido en el Anexo 03 – "Formato de Evaluación de Conocimiento del Plan de Contingencia de TI"

Fuente: Elaboración propia.

Tabla 26 – Escenario 02 – Prueba de Falta de Suministro Eléctrico en el Data Center.

ESCENARIO 02	PRUEBA DE FALTA DE SUMINISTRO ELÉCTRICO EN EL DATA CENTER
RESPONSABLE	Gestor del Plan de la Contingencia de TI Equipo de la Atención de la Contingencia de TI (Profesional de TI)
PERIOCIDAD	Semestral / Anual
DESCRIPCIÓN	
Este escenario consiste en simular la falta de energía eléctrica en el Data Center. **Antes de la Prueba:** - Informar a las áreas usuarias la fecha y hora de la indisponibilidad de los servicios de TI. - Si es necesario solicitar la participación de usuarios de las unidades orgánicas, para realizar pruebas en el escenario de contingencia. - Coordinar con la subgerencia de Servicios Generales y Maestranza para la suspensión del fluido eléctrico mientras dure la prueba - Validar la existencia de copias de respaldo de las máquinas virtuales, equipos de comunicaciones, equipos de seguridad perimetral, entre otros. **Día de la Prueba:** - Confirmar la asistencia del personal de TI. - Baja del suministro eléctrico en el tablero principal del Data Center. - Supervisión de estado de carga de UPS. - Apagado progresivo de servidores y equipamiento de comunicaciones. - Validar el apagado total de los equipos del Data Center. - Realizar las actividades descrita en el Plan de Recuperación (PR-04) del presente Plan de Contingencia de TI. - Realizar pruebas de conectividad de los sistemas, así como al servidor de archivos, acceso a internet y correo electrónico. - Documentar todos los problemas identificados.	

Después de la Prueba:
El responsable debe elaborar un informe de los resultados obtenidos que contenga los siguientes puntos:

- Tipo de prueba.
- Día.
- Duración.
- Participantes.
- Resultados.
- Acciones Correctivas

De ser necesario se deberá actualizar el Plan de Contingencia de TI con las lecciones aprendidas de ésta prueba.

Nota:
Documentar de acuerdo a lo establecido en el Anexo 02 – "Formato de Documentación de Pruebas de Contingencia de TI"

Fuente: Elaboración propia.

Tabla 27 – Escenario 03 – Prueba de Suspensión de los Servicios Informáticos.

ESCENARIO 03	PRUEBA DE SUSPENSIÓN DE LOS SERVICIOS INFORMÁTICOS
RESPONSABLE	Gestor del Plan de la Contingencia de TI Equipo de la Atención de la Contingencia de TI (Profesional de TI)
PERIOCIDAD	Semestral / Anual
DESCRIPCIÓN	

Este escenario consiste en simular la caída de los servidores poniendo en marcha la activación de servidores de contingencia (máquinas virtuales o hosting alterno).

Antes de la Prueba:

- Informar a las áreas usuarias la fecha y hora de indisponibilidad de los servicios de TI relacionados con los servidores involucrados.
- Si es necesario solicitar la participación de usuarios de las unidades orgánicas, para realizar pruebas en el escenario de contingencia.
- Realizar copias de respaldo de las máquinas virtuales alojadas en el Storage principal.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Día de la Prueba:

- Confirmar la asistencia del personal de TI.
- Bajar los sistemas informáticos de la plataforma TI.
- Apagar o desconectar el servidor de Base de Datos.
- Apagar los servidores involucrados.
- Realizar la actividad descrita en el Plan de Contingencia de TI.
- Realizar pruebas de conectividad de los sistemas, así como al servidor de archivos, acceso a internet y correo electrónico.
- Documentar todos los problemas identificados.

Municipalidad Distrital de San Miguel V°B° RICARDO G. ARRIAGADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Después de la Prueba:
El responsable debe elaborar un informe de los resultados obtenidos que contenga los siguientes puntos:

- Tipo de prueba.
- Día.
- Duración.
- Participantes.

- Resultados.
- Acciones Correctivas

De ser necesario se deberá actualizar el Plan de Contingencia de TI con las lecciones aprendidas de ésta prueba.

Nota:
Documentar de acuerdo a lo establecido en el Anexo 02 – "Formato de Documentación de Pruebas de Contingencia de TI"

Fuente: Elaboración propia.

2.6. Documentación de las Pruebas

Para realizar el registro de la ejecución de las pruebas al Plan de Contingencia de TI, se utilizará el formato descrito en el **Anexo 02 – "Formato de Documentación de Pruebas del Plan de Contingencia de TI"** y el **Anexo 03 - "Formato de Evaluación de Conocimiento del Plan de Contingencia de TI"**.

XIII. IMPLEMENTACION DEL PLAN DE CONTINGENCIA DE TI

El Plan aplica las actividades necesarias para mantener operantes y/o reestablecer los servicios de TI, sistemas de información, aplicativos y la infraestructura tecnológica que los soporta.

La implementación del presente plan iniciará en un plazo no mayor de treinta (30) días calendarios después de su aprobación.

Para tal efecto los Gestores del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital y la Jefatura de Soporte, Redes y Telecomunicaciones), con la autorización del responsable del Plan de Contingencia de TI (Gerente de TIC), coordinará con el 'Líder del Plan de Contingencia de TI para la ejecución de actividades del Plan de Contingencia de TI, en tan sentido, el Oficial de Seguridad y Confianza Digital, realizará 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.

XIV. MONITOREO

Cada vez que se da o realiza un cambio en la infraestructura, lo mismo que los bienes informáticos, incluido los equipos informáticos del Data Center, debemos de realizar la adaptación respectiva, es importante que se realice una verificación del Plan de Contingencia de TI.

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. Por lo que, es importante la ejecución de simulacros de interrupción de servicios informáticos, los cuales deben estar definidos, de forma que se pueda determinar el nivel de éxito de los mismos. Para dichos simulacros se debe considerar lo siguiente:

a. Definir a los responsables del simulacro por las diferentes áreas interesadas.
b. Evaluar los riesgos, validar el inventario de recursos.
c. Elaborar un plan de atención del Data Center, y según corresponda un plan de atención que abarque todos los bienes informáticos de la entidad municipal.
d. Se debe comunicar a todo el personal de la entidad municipal sobre los simulacros.
e. Se debe realizar una evaluación conjunta con todos los responsables definidos para el simulacro, y plasmar en un documento las mejoras que se requieren plantear.
f. Comunicar a todos los interesados el resultado de la evaluación del simulacro.

Ésta etapa de Monitoreo, permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta; es primordialmente de mantenimiento, permitiendo realizar siguientes actividades principales:

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

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

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

En base a los resultados obtenidos, realizar las modificaciones y mantenimiento del presente Plan de Contingencia de TI, para lo cual deberán establecer controles formales para dichas modificaciones. Asimismo, todos los responsables mencionados en el presente documento (Plan de Contingencia de TI), deberán tener conocimiento de los cambios.

Como parte del mantenimiento del Plan de Contingencia de TI, se deberá contemplar el entrenamiento al personal de la Unidad de Soporte y Comunicaciones, mediante capacitaciones presenciales o virtuales de acuerdo a lo planificado por los Gestores del Plan de Contingencia, que deberá realizarse de manera semestral o anual, a fin de que puedan dar una respuesta apropiada a las eventualidades que puedan afectar los Servicios de TI.

XV. ANEXOS

- Anexo 01 – "Planes de Recuperación"
- Anexo 02 - "Formato de Documentación de Pruebas del Plan de Contingencia de TI".
- Anexo 03 - "Formato de Evaluación de Conocimiento del Plan de Contingencia de TI".

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
V°B°
RENATO ALVAREZ LLOSA
SUBGERENTE
UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel
V°B°
RICARDO G. ALVARADO BUSTOS
GERENTE
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

ANEXO 01
"Planes de Recuperación"

PLAN DE RECUPERACIÓN	PR-01
ESCENARIO	DESTRUCCIÓN DEL DATA CENTER COMO RESULTADO DE UN SISMO, INUNDACIÓN O INCENDIO
	En este escenario se considera que los recursos informáticos alojados en el Centro de Datos se encuentran indisponibles a causa de la destrucción originada por un sismo, inundación o un incendio.
ESTRATEGIA	1. Implementar un centro de contingencia en las instalaciones del Palacio Municipal, también del análisis de costo beneficio se puede implementar en las instalaciones de un proveedor de hosting, además que en caso se presente un escenario de contingencia, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos. 2. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware. 3. Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc. 4. Contar con Switches de respaldo que como mínimo sean de capa 3 de modelo OSI.
SERVICIOS DE TI	Analizando el escenario de riesgo y considerando la lista de servicios y activos, se determina que los servicios de TI a recuperar se pueden agrupar y recuperar en el siguiente orden de prioridad: 1. Red de datos (Equipos de comunicaciones) 2. Internet y Seguridad Perimetral 3. Servicio de Autenticación de Red 4. Base de datos. 5. Sistema de almacenamiento (Storage) 6. Servidores Físicos 7. Sistema de Virtualización (Hypervisor) 8. Servidores Virtuales

PLAN DE ACCION - 01	RED DE DATOS (EQUIPOS DE COMUNICACIONES)

COMPONENTES:

- Switches Core, Switches de Servidores, Switches de Distribución.
- Enlace de datos con proveedor de hosting.

ETAPAS

ANTES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Contratar servicios de enlace de datos y servicio de enlace de contingencia hacia el Data Center de un proveedor de hosting, o se restablece el servicio en las instalaciones del Palacio Municipal, donde se recuperarán los servicios críticos. 2. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación. 3. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos. 4. Mantener un switch administrable de contingencia, que mínimo sea de capa3 del modelo OSI.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Revisar el cumplimiento de las copias de respaldo y de la operatividad del equipo de contingencia.

DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Revisar la operatividad del Switch Core y equipos de comunicación del Data Center. En caso de estar inoperativos realizar el punto2, caso contrario ir al punto 3. 2. Realizar las configuraciones de red en el Switch capa 3 de contingencia. 3. Verificar la conectividad con el Data Center de contingencia.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados. 2. Configurar el hardware nuevo o reparado.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN – PR-01	
PLAN DE ACCION - 02	**INTERNET Y SEGURIDAD PERIMETRAL**
COMPONENTES: • UTM (parte del servicio de Internet y Seguridad Perimetral).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Supervisar que el administrador de red esté realizando respaldos periódicos de la configuración de los equipos UTM. 2. Mantener actualizado un diagrama de conexiones de los equipos que estén en el Centro de Datos y el documento con la relación de políticas implementadas.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Reportar al proveedor de Servicio de Internet y Seguridad Perimetral la falla en el servicio. 2. Revisar el correcto funcionamiento de las políticas de navegación en el servicio de Internet de Contingencia. 3. Verificar la comunicación desde Internet hacia los servicios publicados.

Municipalidad Distrital de San Miguel V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ARANADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados. 2. Revisar el correcto funcionamiento del nuevo hardware. 3. Verificar la comunicación desde Internet hacia los servicios publicados. 4.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Verificar el cumplimiento del procedimiento de recuperación. 6. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN – PR-01	
PLAN DE ACCION - 03	**SERVICIO DE AUTENTICACIÓN DE RED (DIRECTORIO ACTIVO)**
COMPONENTES: • Servidor del directorio activo • Sistema de almacenamiento (Storage)	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Cumplir con el procedimiento de Respaldo de la Información. 2. Guardar una copia de respaldo en un servidor local y enviar una copia al lugar de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Restablecer la copia de respaldo del servidor de directorio activo. 2. Configurar parámetros de red y verificar. 3. Realizar pruebas sobre el servicio de directorio activo.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	7. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados. 8. Realizar una copia de respaldo del Directorio Activo de Contingencia 9. Restaurar el Directorio Activo de Contingencia en el Directorio Activo de producción recuperado.

Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	10. Verificar el cumplimiento del procedimiento de recuperación. 11. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN – PR-01	
PLAN DE ACCION - 04	**BASE DE DATOS**
COMPONENTES: • Servidor de Base de Datos • Conexión al Sistema de almacenamiento (Storage)	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Administrador de BD)	1. Cumplir con el Respaldo de la Información. 2. Monitorear el correcto funcionamiento del SQL Server, PostgreSQL. 3. Guardar una copia de respaldo en un servidor local y enviar copia al lugar de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Administrador de BD)	1. Activar una máquina virtual como parte del hosting y restaurar la base de datos. 2. Validar que la información puede ser consultada.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica)	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados. 2. Instalar recursos afectados.
Profesional de TI (Administrador de BD)	3. Configurar Base de Datos. 4. Validar que la información puede ser consultada en hardware nuevo o reparado.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Verificar el cumplimiento del procedimiento de recuperación. 6. Comunicar al Responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALCANTARA BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-01	
PLAN DE ACCION - 05	**SISTEMA DE ALMACENAMIENTO (STORAGE)**
COMPONENTES: • Sistema de almacenamiento (Storage, Switches de Fibra Canal).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica)	1. Mantener copias de respaldo de la configuración del sistema de almacenamiento. 2. Mantener copias de respaldo de la configuración de Switches de fibra canal.
Profesional de TI (Administrador de BD)	3. Cumplir con el Respaldo de la Información 4. Mantener actualizada la copia en el sistema de almacenamiento de contingencia (Storage de contingencia en Hosting)
Profesional de TI (Infraestructura Tecnológica)	5. Mantener actualizado el diagrama de la configuración y conexiones del sistema de almacenamiento.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	6. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Revisar la operatividad del sistema almacenamiento de contingencia (Storage) y promoverlo como sistema de almacenamiento principal. 2. Configurar parámetros de red y verificar. 3. Verificar la comunicación desde los servidores.
Profesional de TI (Aplicaciones)	1. Realizar pruebas de los Sistemas de Información.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados. 2. Configurar el hardware y software de los recursos afectados. 3. Actualizar las configuraciones del Sistema de almacenamiento (Storage).
Profesional de TI (Aplicaciones)	4. Realizar pruebas sobre las aplicaciones involucradas.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Verificar el cumplimiento del procedimiento de recuperación. 6. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN – PR-01	
PLAN DE ACCION - 06	**SERVIDORES FÍSICOS**
COMPONENTES: • Respaldo de información • Licencias de sistemas operativos de servidores • Conexión al Sistema de almacenamiento (Storage)	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Cumplir con el Respaldo de la Información. 2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar la restauración del servidor físico en un servidor virtual. 2. Configurar parámetros de red y verificación.
Profesional de TI (Aplicaciones)	3. Realizar pruebas de los servicios en el servidor virtual.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Verificar el cumplimiento del procedimiento de recuperación.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados.
Profesional de TI (Aplicaciones)	2. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información.
Profesional de TI (Administrador de BD)	3. En caso lo soliciten, ejecutar el pase a producción para actualización de información.
Profesional de TI (Aplicaciones)	4. Realizar pruebas sobre los servicios del servidor virtual.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Verificar el cumplimiento del procedimiento de recuperación. 6. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-01	
PLAN DE ACCION - 07	**SISTEMA DE VIRTUALIZACIÓN**
COMPONENTES: • Servidor virtual • Hypervisor: Hyper-V. • Conexión al Sistema de almacenamiento (Storage).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Contratar servicio de hosting bajo demanda, asegurando la disponibilidad de máquinas virtuales para ser activadas en un escenario de contingencia. 2. Cumplir con el Respaldo de la Información. 3. Guardar una copia de respaldo en un servidor local y enviar otra copia al lugar de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Revisar que se ejecute el Respaldo de la Información.
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Comunicar a proveedor de hosting la activación de la contingencia y solicitar el aprovisionamiento de los recursos para las máquinas virtuales necesarias. 2. Verificar la conectividad con el sistema de almacenamiento (Storage) 3. Configurar la plataforma de Virtualización (Hypervisor) 4. Verificar la comunicación a nivel de red de cada Hypervisor.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Verificar el cumplimiento del procedimiento de recuperación.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados. 2. Configurar la plataforma de Virtualización en el recurso nuevo o reparado. 3. Actualizar las configuraciones de red dé cada Hypervisor
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Verificar el cumplimiento del procedimiento de recuperación. 5. Comunicar al Responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-01	
PLAN DE ACCION - 08	**SERVIDORES VIRTUALIZADOS**
COMPONENTES: • Máquinas virtuales. • Licencias de sistemas operativos de servidores. • Conexión al Sistema de almacenamiento (Storage).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica)	1. Cumplir con el Respaldo de la Información. 2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información.
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar la restauración del servidor virtual. 2. Configurar parámetros de red y verificación.
Profesional de TI (Aplicaciones)	3. Realizar pruebas de los servicios del servidor virtual.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Verificar el cumplimiento del procedimiento de recuperación.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Aplicaciones)	1. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información.
Profesional de TI (Infraestructura Tecnológica) **Profesional de TI (Administrador de BD)**	2. En caso lo soliciten, ejecutar el pase a producción para actualización de información.
Profesional de TI (Aplicaciones)	3. Realizar pruebas sobre los servicios del servidor virtual.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Verificar el cumplimiento del procedimiento de recuperación. 5. Comunicar al Responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO D. [illegible] GERENTE

PLAN DE RECUPERACIÓN	PR-02
ESCENARIO	INDISPONIBILIDAD DE SERVIDORES CRÍTICOS FÍSICOS POR FALLA DE HARDWARE O SOFTWARE
	En este escenario se considera la indisponibilidad de los servicios críticos causados por una falla física o lógica de los servidores.
ESTRATEGIA	1. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware. 2. Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los servidores físicos y central telefónica 3. Implementar un procedimiento de respaldos que considere los RTO obtenidos en las reuniones con las áreas de negocio. 4. Programación de dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
SERVICIOS DE TI	Servicios críticos alojados en Servidores Físicos.

PLAN DE ACCION - 01	SERVIDORES FÍSICOS

COMPONENTES:

- Servidores.
- Copias de Respaldo de información.
- Licencias de sistemas operativos de servidores.
- Conexión al Sistema de almacenamiento (Storage).

ETAPAS

ANTES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica)	1. Cumplir con el procedimiento de Respaldo de Información. 2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información

DURANTE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Profesional de TI (Infraestructura Tecnológica)	1. Realizar la restauración del servidor físico en un servidor virtual. 2. Configurar parámetros de red y verificación.
Profesional de TI (Aplicaciones)	3. Realizar pruebas de los servicios en el servidor virtual.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Revisar la seguridad de la Información en la etapa de contingencia.

DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados.
Profesional de TI (Aplicaciones)	2. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información.
Profesional de TI (Infraestructura Tecnológica) Profesional de TI (Administrador BD)	3. En caso lo soliciten, ejecutar el pase a producción para actualización de información.
Profesional de TI (Aplicaciones)	4. Realizar pruebas sobre los servicios del servidor virtual.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Verificar el cumplimiento del procedimiento de recuperación. 6. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN	**PR-03**
ESCENARIO	**INDISPONIBILIDAD EN LOS SERVICIOS CRÍTICOS POR LA OCURRENCIA DE UN CIBERATAQUE**
	En este escenario se considera la Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque.
ESTRATEGIA	1. Mantener actualizado los parches de seguridad en servidores y estaciones de trabajo 2. Mantener actualizado el software de protección anti-malware en cada servidor y estación de trabajo. 3. Mantener controles de seguridad perimetral como Firewall, UTM, etc. 4. Desarrollar planes de sensibilización en materia de seguridad de la información y buenas prácticas en el uso de los sistemas informáticos. 5. Realizar el monitoreo del rendimiento y consumo de los recursos en los servidores. 6. Realizar pruebas anuales de Hacking Éticos de terceros especializados.
SERVICIOS DE TI	Analizando el escenario de riesgo y considerando la lista de servicios y activos, se determina el orden de recuperación de los siguientes servicios de TI: 1. Sistema de Almacenamiento 2. Bases de Datos 3. Sistemas de información
PLAN DE ACCION - 01	**SISTEMA DE ALMACENAMIENTO (STORAGE)**
COMPONENTES: • Sistema de almacenamiento (Storage)	
ETAPAS	

ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con **Profesional de TI (Infraestructura Tecnológica)**	1. Mantener la copia de respaldo del sistema de almacenamiento. 2. Mantener actualizada la copia en el sistema de almacenamiento de contingencia (Storage de contingencia en Hosting).
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Supervisar el cumplimiento de las copias de respaldo.
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Aislar los sistemas de almacenamiento. 2. Comunicar al proveedor del Servicio Antimalware y/o al Proveedor del Servicio de Seguridad Gestionada sobre el suceso para que identifique la fuente y otros posibles equipos comprometidos. 3. Revisar el estado del sistema de almacenamiento de contingencia y en caso no se encuentre comprometido será promovido como sistema de almacenamiento principal en cuanto el proveedor antimalware y/o de seguridad gestionada hayan aislado la fuente del ataque. 4. En caso ambos sistemas de almacenamiento se encuentren comprometidos se deberá restaurar la última copia de respaldo en uno de los sistemas de almacenamiento. 5. Validar con el proveedor antimalware y/o proveedor de Seguridad Gestionada sobre la factibilidad de habilitación del sistema de almacenamiento. 6. Realizar la habilitación de la comunicación hacia el sistema de almacenamiento.
Profesional de TI (Aplicaciones)	7. Gestionar las pruebas con los usuarios principales de los sistemas de información.
Profesional de TI (Infraestructura Tecnológica)	8. Gestionar las pruebas sobre las unidades de red.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	9. Revisar los controles principales de seguridad configurados para la contingencia.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar la configuración del sistema de almacenamiento de contingencia (replicación)
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	2. Actualizar las configuraciones del Sistema de almacenamiento (Storage). 3. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-03	
PLAN DE ACCION - 02	**BASE DE DATOS**

COMPONENTES:

- Servidor de Base de datos
- Conexión al Sistema de almacenamiento (Storage).

ETAPAS

ANTES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica)	1. Cumplir con el procedimiento de Respaldo de Información (Bases de Datos).
Profesional de TI (Administrador de BD)	2. Mantener actualizado los parches de seguridad en los servidores.
Profesional de TI (Infraestructura Tecnológica)	3. Guardar una copia de respaldo en un servidor local y enviar otra copia al proveedor de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Supervisar el cumplimiento de las actividades establecidas en esta etapa "Antes de la Contingencia".

DURANTE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Profesional de TI (Infraestructura Tecnológica)	1. Aislar el servidor de base de datos afectado. 2. Comunicar al proveedor del Servicio Antimalware y/o al Proveedor del Servicio de Seguridad Gestionada sobre el suceso para que identifique la fuente y otros posibles equipos comprometidos.
Profesional de TI (Administrador de BD)	3. Evaluar el nivel de compromiso en el servidor y posibilidad de restablecerlo. 4. Para el caso donde el servidor no pueda restablecerse, deberá reinstalarse. 5. Levantar la copia de respaldo en el servidor de Base de Datos reinstalado. 6. Realizar las configuraciones necesarias para la comunicación entre la base de datos y storage.
Profesional de TI (Aplicaciones)	7. Gestionar las pruebas con los usuarios principales de los sistemas de información.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	8. Supervisar el cumplimiento de las actividades durante la contingencia. 9. Revisar los controles principales de seguridad para la configuración en contingencia.

DESPUES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Profesional de TI (Aplicaciones)	1. Revisar el funcionamiento, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo y solicitar el pase a producción de base de datos en caso corresponda.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ ULLOA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

Profesional de TI (Administrador de BD)	2. Ejecutar el pase a producción con los cambios solicitados. 3. Validar que la información puede ser consultada en el servidor configurado.
Profesional de TI (Aplicaciones)	4. Gestionar las pruebas con los usuarios principales de los sistemas de información.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Revisar el restablecimiento de los controles de seguridad. 6. Supervisar el cumplimiento de las actividades 7. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN – PR-03	
PLAN DE ACCION - 03	**SISTEMAS DE INFORMACIÓN**
COMPONENTES: • Código fuente de aplicaciones. • Conexión al Sistema de almacenamiento (Storage).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Aplicaciones)	1. Mantener el registro de cambios y versiones del código fuente de las aplicaciones.
Profesional de TI (Infraestructura Tecnológica) **Profesional de TI (Administrador de BD)**	2. Cumplir con el Respaldo de Información (servidores de aplicaciones, códigos fuente de las aplicaciones).
Profesional de TI (Infraestructura Tecnológica)	3. Revisar que el antimalware instalado en los servidores se encuentre actualizado. 4. Mantener actualizado los parches de seguridad en servidores.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	5. Supervisar el cumplimiento de las actividades, establecidas en esta etapa.
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Aislar el servidor afectado. 2. Comunicar al proveedor del Servicio Antimalware y/o al Proveedor del Servicio de Seguridad Gestionada sobre el suceso para que identifique la fuente y otros posibles equipos comprometidos. 3. Validar con el proveedor antimalware y/o proveedor de Seguridad Gestionada sobre la factibilidad de recuperación del equipo(s) o servicio(s) comprometido(s).
Profesional de TI (Administrador de BD)	4. Para el caso donde el servicio o equipo comprometido no pueda restablecerse, se deberán levantar las copias de respaldo de los servidores más recientes.
Profesional de TI (Aplicaciones)	5. Realizar las configuraciones necesarias para la comunicación con la base de datos y storage.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

	6. Gestionar las pruebas con los usuarios principales de los sistemas de información.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	7. Revisar los controles principales de seguridad para la configuración de contingencia.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Aplicaciones)	1. Coordinar con el dueño del proceso soportado por el sistema de información, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo.
Profesional de TI (Aplicaciones) **Profesional de TI (Administrador de BD)**	2. En caso lo soliciten, ejecutar el pase a producción para actualización de información.
Profesional de TI (Aplicaciones)	3. Realizar pruebas sobre la aplicación.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Supervisar el cumplimiento de la actividad. 5. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN	**PR-04**
ESCENARIO	**INDISPONIBILIDAD EN LOS SERVICIOS CRÍTICOS POR FALLA EN LA ENERGÍA ELÉCTRICA EN EL DATA CENTER**
	En este escenario se considera que el suministro de energía eléctrica del Data Center, se encuentre indisponible ocasionando la indisponibilidad de los servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
ESTRATEGIA	1. Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías. 2. Implementar un tablero de transferencia automático (Bypass) en el Data Center, para asegurar la continuidad eléctrica ante fallas del sistema de UPS. 3. Implementar un sistema de UPS redundante con circuitos independientes que alimenten a los servidores y quipos críticos del Data Center. 4. Configurar el monitoreo remoto del UPS con alertas en caso de detectarse falla en el suministro eléctrico y/o banco de baterías. 5. Realizar el apagado de los equipos en forma ordenada 6. Implementar un tablero de transferencia (Bypass) en el suministro eléctrico, para asegurar una mínima interrupción de energía ante trabajos de mantenimiento. 7. Evaluar el implementar un generador eléctrico para proveer energía al Data Center en casos de falla de la red eléctrica pública.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBSERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

SERVICIOS DE TI	Analizando el escenario de riesgo, mientras se cuenta con energía del UPS, se debe realizar el apagado de los equipos. Una vez que retorne la energía eléctrica se realizara el encendido de los equipos en el siguiente orden: 1. Red de datos (Equipos de comunicaciones) 2. Internet y Seguridad Perimetral 3. Sistema de almacenamiento (Storage) 4. Sistema de Virtualización (Hypervisor) 5. Servicio de Autenticación de Red 6. Base de datos. 7. Servidores Virtuales 8. Servidores Físicos

PLAN DE ACCION - 01	RED DE DATOS (EQUIPOS DE COMUNICACIONES)

COMPONENTES:

- Switches Core, Switches de Servidores, Switches de Distribución.
- Enlace de datos con proveedor de hosting.

ETAPAS

ANTES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación. 2. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos. 3. Mantener un switch administrable de contingencia, que mínimo sea de capa3 del modelo OSI.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Revisar el cumplimiento de las copias de respaldo y de la operatividad del equipo de contingencia.

DURANTE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Profesional de TI (Redes y Comunicaciones)	1. Realizar el apagado de los equipos de comunicación

DESPUES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Profesional de TI (Redes y Comunicaciones)	1. Realizar el encendido de los equipos de comunicaciones.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	2. Verificar el cumplimiento del procedimiento de recuperación. 3. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-04	
PLAN DE ACCION - 02	**INTERNET Y SEGURIDAD PERIMETRAL**
COMPONENTES: • UTM (parte del servicio de Internet y Seguridad Perimetral).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Supervisar que el administrador de red esté realizando respaldos periódicos de la configuración de los equipos UTM. 2. Mantener actualizado un diagrama de conexiones de los equipos que estén en el Centro de Datos y el documento con la relación de políticas implementadas.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Reportar al proveedor de Servicio de Internet y Seguridad Perimetral el corte de energía eléctrica. 2. Realizar el apagado de los equipos del proveedor.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Realizar el encendido de los equipos 2. Revisar el correcto funcionamiento del servicio de internet y políticas de navegación. 3. Verificar la comunicación desde Internet hacia los servicios publicados.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Verificar el cumplimiento del procedimiento. 5. Comunicar al Responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-04	
PLAN DE ACCION - 03	**SISTEMA DE ALMACENAMIENTO (STORAGE)**
COMPONENTES: • Sistema de almacenamiento (Storage, Switches de Fibra Canal).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica)	1. Mantener copias de respaldo de la configuración del sistema de almacenamiento. 2. Mantener copias de respaldo de la configuración de Switches de fibra canal.
Profesional de TI (Administrador de BD)	3. Cumplir con el Respaldo de la Información 4. Mantener actualizada la copia en el sistema de almacenamiento de contingencia (Storage de contingencia en Hosting)
Profesional de TI (Infraestructura Tecnológica)	5. Mantener actualizado el diagrama de la configuración y conexiones del sistema de almacenamiento.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	6. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar el apagado del sistema de almacenamiento (Storage)
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar el encendido del Storage.
Profesional de TI (Aplicaciones)	2. Realizar pruebas sobre las aplicaciones involucradas.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al Responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-04	
PLAN DE ACCION - 04	**HIPERVISORES DE VIRTUALIZACIÓN**
COMPONENTES: • Servidor virtual • Hypervisor: Hyper-V. • Conexión al Sistema de almacenamiento (Storage).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Cumplir con el Respaldo de la Información. 2. Guardar una copia de respaldo en un servidor local y enviar otra copia al lugar de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información.
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar el apagado de los servidores de virtualización.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar en encendido de los servidores de virtualización. 2. Revisar el correcto funcionamiento del servicio de virtualización.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-04	
PLAN DE ACCION - 05	**SERVICIO DE AUTENTICACIÓN DE RED (DIRECTORIO ACTIVO)**
COMPONENTES: • Servidor del directorio activo • Sistema de almacenamiento (Storage)	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones)	1. Cumplir con el procedimiento de Respaldo de la Información. 2. Guardar una copia de respaldo en un servidor local y enviar una copia al lugar de custodia.

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información.
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Redes y Comunicaciones)	1. Realizar el apagado de los servidores de Directorio Activo.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Redes y Comunicaciones)	1. Realizar el encendido de la máquina virtual de Directorio Activo. 2. Revisar el correcto funcionamiento de las máquinas virtuales.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN – PR-04	
PLAN DE ACCION - 06	**BASE DE DATOS**
COMPONENTES: • Servidor de Base de Datos • Conexión al Sistema de almacenamiento (Storage)	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Administrador de BD)	1. Cumplir con el Respaldo de la Información. 2. Monitorear el correcto funcionamiento del SQL Server, PostgreSQL. 3. Guardar una copia de respaldo en un servidor local y enviar copia al lugar de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica) **Profesional de TI (Administrador de BD)**	1. Realizar el apagado de la base de datos.

DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica) **Profesional de TI (Administrador de BD)**	1. Encender la base de datos.
Profesional de TI (Administrador de BD)	2. Validar que la información puede ser consultada.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN – PR-04	
PLAN DE ACCION - 07	**SERVIDORES VIRTUALIZADOS**
COMPONENTES: • Máquinas virtuales. • Licencias de sistemas operativos de servidores. • Conexión al Sistema de almacenamiento (Storage).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica)	1. Cumplir con el Respaldo de la Información. 2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información.
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar el apagado de la máquina virtual
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Encender la máquina virtual. 2. Realizar pruebas sobre los servicios del servidor virtual
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al Responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE RECUPERACIÓN – PR-04	
PLAN DE ACCION - 08	**SERVIDORES FÍSICOS**
COMPONENTES: • Servidores físicos. • Respaldo de información. • Conexión al Sistema de almacenamiento (Storage).	
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Cumplir con el Respaldo de la Información. 2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar que se ejecute el Respaldo de la Información
DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Realizar el apagado del servidor físico.
DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica)	1. Encender el servidor físico. 2. Realizar pruebas sobre los servicios del servidor virtual.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN	PR-05
ESCENARIO	**INDISPONIBILIDAD DE LOS SERVICIOS CRÍTICOS POR AUSENCIA O INDISPONIBILIDAD DEL PERSONAL CRÍTICO**
	En este escenario se considera que no se encuentra disponible el personal necesario para la administración y gestión de la infraestructura tecnológica y servicios de tecnología, lo cual puede traer como consecuencia la indisponibilidad de los mismos.

ESTRATEGIA	1. Eliminar la dependencia funcional de los puestos críticos, capacitando a un reemplazo para cada rol (personal alterno), de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto. 2. Entrenar al personal de la Unidad de Soporte y Comunicaciones 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 se ha logrado sus objetivos. 3. Elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de la OTIC, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información. 4. Elaborar una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

PLAN DE ACCION - 01	**PERSONAL CRÍTICO DE TI**

ETAPAS

ANTES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación con Profesional de TI (Infraestructura Tecnológica) Profesional de TI (Aplicaciones) Profesional de TI (Redes y Comunicaciones) Profesional de TI (Base de Datos)	1. Establecer instructivos y/o procedimientos para la administración de los servicios críticos. 2. Mantener los accesos remotos para que en caso se requiera se puedan administrar los servicios informáticos desde lugares externos. 3. Capacitar a personal alterno en la gestión y operación de los servicios críticos para garantizar la continuidad de la operación.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Revisar el cumplimiento de los puntos 1, 2 y 3.

DURANTE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación	1. Comunicar al Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital), sobre la ausencia del personal (Profesional de TI). 2. Coordinar la conexión remota a los equipos y sistemas, por parte de personal alterno.

DESPUES DE LA CONTINGENCIA

EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación	1. Comunicar el personal reincorporado (Profesional de TI), sobre las acciones tomadas en su ausencia.
Profesional de TI (Infraestructura Tecnológica, Redes y	2. Complementar los instructivos y/o procedimientos en caso sea necesario.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

Comunicaciones, Base de Datos, Infraestructura Tecnológica)	
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Revisar el cumplimiento de los puntos 1, 2 4. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

PLAN DE RECUPERACIÓN	PR-06
ESCENARIO	INDISPONIBILIDAD DE LOS SERVICIOS CRÍTICOS POR FALLA EN LOS EQUIPOS DE COMUNICACIONES
	En este escenario se considera que los equipos de redes y comunicaciones se encuentren indisponibles como resultado de una falla física o lógica, lo cual puede traer como consecuencia la caída de servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
ESTRATEGIA	1. Contar con Switches de respaldo que como mínimo sean de capa 3 de modelo OSI, almacenados en un ambiente separado del Centro de Datos. 2. Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones. 3. Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los equipos de comunicaciones del Centro de Datos.
SERVICIOS DE TI	Red de Datos (Equipos de comunicaciones)
PLAN DE ACCION - 01	RED DE DATOS (EQUIPOS DE COMUNICACIONES)
COMPONENTES:	• Switches Core, Switches de Servidores, Switches de Distribución. • Enlace de datos con proveedor de hosting.
ETAPAS	
ANTES DE LA CONTINGENCIA	
EJECUNTANTE	ACTIVIDAD
Líder del Plan de Contingencia en coordinación con Profesional de TI (Redes y Comunicaciones) Profesional de TI (Infraestructura Tecnológica)	1. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación. 2. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos. 3. Mantener un switch administrable de contingencia, que mínimo sea de capa3 del modelo OSI.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	4. Revisar el cumplimiento de las copias de respaldo y de la operatividad del equipo de contingencia.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO G. ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

DURANTE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Redes y Comunicaciones) **Profesional de TI (Infraestructura Tecnológica)**	1. Revisar la operatividad del Switch Core y equipos de comunicación del Centro de Datos. En caso de estar inoperativos realizar el punto2, caso contrario ir al punto 3. 2. Realizar las configuraciones de red en el Switch capa 3 de contingencia. 3. Reemplazar equipo dañado y probar conectividad con los servidores

DESPUES DE LA CONTINGENCIA	
EJECUNTANTE	**ACTIVIDAD**
Profesional de TI (Infraestructura Tecnológica) **Profesional de TI (Redes y Comunicaciones)**	1. Gestionar con el proveedor de soporte la reparación o reemplazado del equipo averiado 2. Configurar el hardware nuevo o reparado.
Gestor del Plan de Contingencia de TI (Oficial de Seguridad y Confianza Digital)	3. Verificar el cumplimiento del procedimiento de recuperación. 4. Comunicar al responsable del Plan de Contingencia de TI (Gerente de OTIC) y al Comité de Gobierno Digital de las acciones realizadas.

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
V°B°
RENATO ALVAREZ LLOSA
SUBGERENTE
UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel
V°B°
RICARDO G. ALTAMIRANO BUSTOS
GERENTE
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

ANEXO 02
"Formato de Documentación de Pruebas del Plan de Contingencia de TI"

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES

FORMATO DE DOCUMNETACION DE PRUEBAS DEL PLAN DE CONTINGENCIA DE TI

		PRUEBA N°	
DATOS GENERALES			
ESCENARIO DE PRUEBA	*<Describir el escenario de prueba que se va a simular>*		
RESPONSABLE DE LA EJECUCION	*<Nombre del responsable de la ejecución de la prueba>*		
OBJETIVO DE PRUEBA	*<Describir la finalidad de la prueba>*		
RECURSO PARA PROBAR	*<Nombre del sistema informático y/o infraestructura tecnológica y/o servicio de TI que se va a probar>*		
FECHA DE PRUEBA	*<Fecha de realización de la prueba, el formato es: DD/MM/AAAA>*	DURACION DE PRUEBA	*<Tiempo estimado de duración de la prueba>*
ALCANCE	*<Describir el alcance del plan de prueba, identificando el lugar de la prueba, los recursos, servicios de TI que serán sometidos a pruebas,>*		
METODOLOGIA	*<Detallar lo que se va hacer en la prueba, describiendo cada uno de los pasos que se requiera para ejecutar la prueba>*		
REQUISITOS PARA LA PRUEBA			
RECURSO HUMANO	*<Especificar el recurso humano necesario, para la ejecución del plan de pruebas>*		
REQUERIMIENTO DE HARDWARE	*<Especificar los requerimientos de hardware (sistema operativo, memoria, servidor, red, etc. Para la ejecución del plan de prueba)>*		
REQUERIMIENTO DE SOFTWARE	*<Especificar los requerimientos de software y copias de respaldo para la ejecución del plan de pruebas>*		
REQUERIMIENTO DE LOGÍSTICO	*<Especificar los requerimientos logísticos que se requieran, (ejemplo transporte, autorizaciones, entre otros) para la ejecución del plan de prueba>*		
CONDICIONES DE EJECUCIÓN			
EQUIPO	*<Información del servidor>*	APLICACIÓN / SOFTWARE	*<Nombre del aplicativo>*
UBICACIÓN	*<lugar de la prueba>*	FECHA DE BACKUP	*<DD/MM/AAAA>*
RESULTADOS DE LA PRUEBA			
RESULTADO ESPERADO	*<Información que se espera obtener con la ejecución de la prueba, se debe establecer antes de la ejecución>*		

Página 1|2

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO GALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES

RESULTADOS DE LA PRUEBA					
SATISFACTORIO		SATISFACTORIO CON OBSERVACIONES		DEFICIENTE	
DESCRIBIR RESULTADO	*<Indicar detalladamente el resultado de la prueba>*				
OBSERVACIONES	*<Indicar las observaciones presentadas en la prueba con resultado deficiente>*				

ACTUALIZACIÓN DEL PLAN DE CONTINGENCIA DE TI	
REALIZAR CAMBIO O ACTUALIZACION EN EL PLAN DE CONTINGENCIA DE TI	*<Indicará los cambios que se tiene que hacer al Plan de Contingencia de TI de la prueba obtenida>*

PARTICIPANTES DE LA PRUEBA

N°	APELLIDOS Y NOMBRES	CARGO	FIRMA
1			
2			
3			
4			

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO ALVARADO BUSTOS GERENTE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

INFORMACION ADICONAL

<Información adicional de la prueba>

Página 2|2

ANEXO 03

"Formato de Evaluación de Conocimiento del Plan de Contingencia de TI"

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL
OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES

FORMATO DE EVALUACIÓN DE CONOCIMIENTO DEL PLAN DE CONTINGENCIA DE TI

	PRUEBA N°

DATOS GENERALES							
RESPONSABLE DE LA EVALUACIÓN	<Nombres y apellidos del Gestor del Plan de Contingencia de TI>						
FECHA	<Fecha de la evaluación, usar el formato: DD/MM/AAAA>						
PERIODO DE EVALUACIÓN	ANUAL		SEMESTRAL		TRIMESTRAL		

DATOS DEL PARTICIPANTE	
APELLIDOS Y NOMBRES	<Indicar apellidos y nombres del participante>
CARGO	<Indicar el cargo del participante>

DESCRIPCIÓN DE LAS PREGUNTAS

N°	PREGUNTA	RESPUESTA	PUNTAJE
1	Rol que desempeña en el Plan de Contingencia TI.		10
2	Describa sus responsabilidades de acuerdo al Rol asignado.		30
3	Indique cuales son los escenarios que deben cumplirse para invocar la activación del Plan de Contingencia de TI.		30
4	Indique usted quien aprueba o activa el inicio del Plan de Contingencia de TI.		10
5	Si durante la contingencia, el personal de la entidad municipal que no forma parte del Equipo de Atención de la Contingencia de TI, se comunicara con usted para solicitarle información del problema, usted como miembro del equipo de Contingencia Informática estaría en facultad de darle toda la información que tiene a mano sobre el problema suscitado. (Si / No)	<No, Porque, se debe esperar a que se reúnan el Equipo que forma parte de la Contingencia de TI para tener coherencia con lo que se va a comunicar>	10
6	Si durante la contingencia, hay la necesidad de comunicarse con la prensa, usted como miembro del Equipo de Atención de la Contingencia de TI está en facultad de hacerlo como vocero. (Si / No)	<No>	10
		TOTAL	100

PUNTAJE OBTENIDO	<Indicar el Puntaje Total que ha obtenido el participante>

MUNICIPALIDAD DISTRITAL DE SAN MIGUEL V°B° RENATO ALVAREZ LLOSA SUBGERENTE UNIDAD DE SOPORTE Y COMUNICACIONES

Municipalidad Distrital de San Miguel V°B° RICARDO ALTAMIRANO BUSTOS GERENTE OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES