VILLA EL SALVADOR
MUNICIPALIDAD
CENTRAL TELEFÓNICA 319-2530
www.munives.gob.pe

RESOLUCIÓN DE GERENCIA MUNICIPAL Nº 598- 2022-GM-MVES.

Villa el Salvador, 11 de noviembre del 2022.

VISTOS; *Los Informes N° 318-2022-OAJ/MVES de fecha 10 de noviembre del 2022 de la Oficina de Asesoría Jurídica; Informe N° 0158-2022-UDT-OGA/MVES, de fecha 19 de octubre de 2022, de la Subgerencia de la Unidad de Desarrollo Tecnológico; sobre Revisión y Aprobación del Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa El Salvador y;*

CONSIDERANDO;

Que, el artículo 194° de la Constitución Política del Perú, establece que: "Las Municipalidades provinciales y distritales son los órganos de gobierno local. Tienen autonomía política, económica y administrativa en los asuntos de su competencia (...)", lo cual concuerda con el articulo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, que establece que los gobiernos locales gozan de autonomía política, económica y administrativa, en los asuntos de su competencia; siendo que esta autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico;

Que, mediante Ley N° 27658, se aprueba la Ley Marco de Modernización de la Gestión del Estado disponiéndose en el artículo 1° de dicha Ley "Declarese al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestíon pública y construir un Estado, descentralizado y al servicio del ciudadano"

Que, mediante Decreto Supremo N° 029-2021-PCM; se aprueba el Reglamento del Decreto Legislativo N°1412 que aprueba la Ley de Gobierno Digital; se establece el gobierno digital; es el uso estrategico de las tecnologías digitales y datos en la administración pública para la creación de valor público; asi mismo comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la administración pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para la ciudadanía;

Que, el articulo 30° del Decreto Legislativo N 1412 ***De la Seguridad Digital*** *señala que "La seguridad digital 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."* ***Artículo 32°*** *Gestión del Marco de Seguridad Digital del Estado Peruano señala:" El marco de Seguridad D igital del Estado Peruano tiene los siguientes ámbitos: (...)* ***d. Institucional:*** *Las entidades de la Administarción Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI)."*

Que, en los artículos 1°, 2°, 3°, 4° y 5° del Decreto Supremo N° 123-2018-PCM, Decreto Supremo que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, se establece que: ***"Artículo 1.- Objeto*** *El presente Reglamento tiene por objeto desarrollar el Sistema Administrativo de Modernización de la Gestión Pública, estableciendo los principios, normas y procedimientos que aplican al proceso de modernización de la gestión pública, en concordancia con la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado;"*

VILLA EL SALVADOR
MUNICIPALIDAD
CENTRAL TELEFÓNICA 319-2530
www.munives.gob.pe

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 598- 2022-GM-MVES.

Villa el Salvador, 11 de noviembre del 2022.

*"**Artículo 2.- Ámbito de aplicación** **2.1** El presente Reglamento es de aplicación a toda entidad pública que forma parte de la Administración Pública, incluyendo aquellas que ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público. **2.2** En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da solo en aquello que le resulte aplicable." **"Artículo 4.- Proceso de modernización de la gestión pública 4.1** La modernización de la gestión pública consiste en la selección y utilización de todos aquellos medios orientados a la creación de valor público en una determinada actividad o servicio a cargo de las entidades públicas. Se crea valor público cuando: **a)** Las intervenciones públicas, que adoptan la forma de bienes, servicios o regulaciones, satisfacen las necesidades y expectativas de las personas, generando beneficios a la sociedad. **b)** Se optimiza la gestión interna a través de un uso más eficiente y productivo de los recursos públicos, para, directa o indirectamente, satisfacer las necesidades y expectativas de las personas, generando beneficios a la sociedad. **4.2** Los objetivos y contenidos principales del proceso de modernización de la gestión pública se desarrollan en la Política Nacional de Modernización de la Gestión Pública, cuya conducción recae en la Presidencia del Consejo de Ministros y requiere la intervención articulada de todas las entidades públicas;" **"Artículo 5.-** Gestión para resultados Las entidades públicas aplican la gestión para resultados como un modelo de gestión que permite identificar y adoptar decisiones sobre todos aquellos aspectos que contribuyan a la creación de valor público;"*

Que, Dicho Plan de Contingencias de Tecnologías de la Información, tiene como finalidad la Protección de la Información Tecnológica de esta Corporación Edil, evitando lo más posible la pérdida de dicha Información, y salvaguardar la Infraestructura de la Red , Sistemas de Información Base de Datos, extremando las medidas de Seguridad para protegernos y estar preparados ante una contingencia respecto al rubro, ya que lo único que permite a la Institución reaccionar adecuadamente ante diversos procesos críticos, es por medio de la elaboración , y mantenimiento de un Plan de Contingencia, que servirá para responder de manera efectiva y eficaz ante una eventual emergencia; asimismo, el presente Plan, tiene congruencia con las normas legales previamente citadas, y se encuentra encaminada al cumplimiento de la Ley de Gobierno Digital;

Que, Mediante Informe N°158-2022-UDT-OGA/MVES de fecha 19 de Octubre del 2022, la Subgerencia Unidad de Desarrollo Tecnológico remite a la Gerencia Municipal, la Revisión y Aprobación del Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa el Salvador, esto en cumplimiento a lo solicitado por el órgano de Control Institucional, en la Recomendación N° 06 y N° 20 de la "Carta de Control Interno de la Auditoria Financiera Gubernamental por el Periodo 2019" y la "Carta de Control Interno de la Auditoria Financiera Gubernamental por el Periodo 2020".

Que, mediante Informe N° 318-2022-OAJ/MVES, de fecha 10 de noviembre de 2022, la Gerencia de Asesoría Jurídica opina que es legalmente procedente la Aprobación mediante Resolución de Gerencia Municipal el "Plan de Contingencia de tecnología de la Información de la Municipalidad Distrital de Villa El Salvador" en conformidad al artículo 27°, y 39°, de la Ley N° 27972, Ley Orgánica de Municipalidades; y en amparo del numeral 4.1, del artículo 4° del Decreto Supremo N° 123-2018-PCM, Decreto Supremo que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública; y del artículo 30°, y del inciso D) del artículo 32°, del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital;

VILLA EL SALVADOR
MUNICIPALIDAD
CENTRAL TELEFÓNICA 319-2530
www.munives.gob.pe

RESOLUCIÓN DE GERENCIA MUNICIPAL Nº 598- 2022-GM-MVES.

Villa el Salvador, 11 de noviembre del 2022.

Que, conforme a las atribuciones conferidas en el articulo 27° de la Ley Nº 27972 - Ley Orgánica de Municipalidades y al amparo del numeral 14.9 y 14.12 del artículo 14° de la Ordenanza Nº 441-MVES, que aprueba el Texto Íntegro del Reglamento de Organización y Funciones -ROF con enfoque de gestión de resultados de la Municipalidad Distrital de Villa El Salvador, aprobado mediante Ordenanza Nº 369-MVES ; que señala: "14.9) Emitir Resoluciones de Gerencia Municipal, (...), y "14.12) Dirigir los Procesos de Modernización y fortalecimiento Institucional acorde con las Políticas Nacionales y los objetivos de estratégicos de desarrollo local";

SE RESUELVE:

***ARTICULO PRIMERO. – APROBAR**; el Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa El Salvador; según lo expuesto en la parte considerativa presente Resolución.*

MUNICIPALIDAD DE VILLA EL SALVADOR V°B° ASESORIA JUDIRICA

***ARTICULO SEGUNDO.- DELEGAR** al Subgerente de la Unidad de Desarrollo Tecnologico de la Entidad el desarrollo, ejecución y cumplimiento del Plan de Contingencia de Tecnología de la Información; el mismo que deberá ejecutarse en cumplimiento de la normatividad legal vigente; bajo responsabilidad..*

***ARTICULO TERCERO. - ENCARGAR** a la Unidad de Desarrollo Tecnológico, efectuar la publicación de la presente Resolucion de Gerencia Municipal, en el Portal Institucional de la Municipalidad Distrital de Villa El Salvador (www.munives.gob.pe).*

MUNICIPALIDAD DE VILLA EL SALVADOR V°B° Unidad de Desarrollo Tecnológico

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

MUNICIPALIDAD DE VILLA EL SALVADOR
GERENCIA MUNICIPAL
JOSÉ LUIS ESPICHAN PÉREZ
GERENTE

MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORÍA JURÍDICA

MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR
GERENCIA MUNICIPAL
10 NOV 2022
RECIBIDO
FOLIO 65 HORA 17:00

INFORME N° 318-2022-OAJ/MVES

A : **Abog. José Luis Espichan Pérez**
Gerente Municipal

DE : **Abog. Shirlet Marley Castro Gonzales**
Gerente de la Oficina de Asesoría Jurídica

ASUNTO : Opinión Legal sobre la Revisión y Aprobación del Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa el Salvador

REF. : Memorando N° 1090-2022-GM/MVES

FECHA : Villa el Salvador, 10 de Noviembre del 2022

Por medio del presente, y en atención al documento de la referencia, mediante la cual se solicita se emita opinión legal relacionada con el asunto del rubro, procedemos a la emisión de este, en los términos siguientes:

I. ANTECEDENTES:

1. Memorando N° 1090-2022-GM/MVES de fecha 20 de Octubre del 2022, la Gerencia Municipal remite a la Oficina de Asesoría Jurídica, el Informe N°158-2022-UDT-OGA/MVES de la Unidad de Desarrollo Tecnológico, por el cual se requiere la Revisión y Aprobación del Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa el Salvador, esto en cumplimiento a lo solicitado por el órgano de Control Institucional, en la Recomendación N° 06 y N° 20 de la "Carta de Control Interno de la Auditoria Financiera Gubernamental por el Periodo 2019" y la "Carta de Control Interno de la Auditoria Financiera Gubernamental por el Periodo 2020".

2. Informe N°158-2022-UDT-OGA/MVES de fecha 19 de Octubre del 2022, la Unidad de Desarrollo Tecnológico requiere a la Gerencia Municipal, la Revisión y Aprobación del Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa el Salvador, esto en cumplimiento a lo solicitado por el órgano de Control Institucional, en la Recomendación N° 06 y N° 20 de la "Carta de Control Interno de la Auditoria Financiera Gubernamental por el Periodo 2019" y la "Carta de Control Interno de la Auditoria Financiera Gubernamental por el Periodo 2020".

MUNICIPALIDAD DE VILLA EL SALVADOR V°B° ASESORIA JUDIRICA

3. Memorando Múltiple N° 046-2022-OGA/MVES de fecha 06 de octubre del 2022, la Oficina General de Administración requiere a la Unidad de Desarrollo Tecnológico, remita el Reporte Bimestral de "Seguimientos a la Implementación de las recomendaciones de los Informes de Servicio de Control Posterior del 01 al 31 de agosto del 2022".

4. Memorando N° 035-2022-GM/MVES de fecha 29 de setiembre del 2022, la Gerencia Municipal requiere a la Oficina General de Administración y a sus Subgerencias Encargadas, que se remita el Reporte Bimestral de "Seguimientos a la Implementación de las recomendaciones de los Informes de Servicio de Control Posterior del 01 al 31 de agosto del 2022"

II. BASE LEGAL:

- ✓ Constitución Política del Perú.
- ✓ Ley N° 27972, Ley Orgánica de Municipalidades.
- ✓ Ley N°27658, Ley Marco de Modernización de la Gestión del Estado
- ✓ Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital
- ✓ Decreto Supremo Nº 123-2018-PCM, Decreto Supremo que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública
- ✓ La Ordenanza N° 441-MVES, que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa el Salvador, aprobado con Ordenanza N° 369-MVES

III. ANALISIS:

1. Que, el artículo 194 de la Constitución Política del Perú, establece que: *"Las municipalidades provinciales y distritales son los órganos de gobierno local. Tienen autonomía política, económica y administrativa en los asuntos de su competencia (…)"*, lo cual concuerda con el Articulo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, que establece que los gobiernos locales gozan de autonomía política, económica y administrativa, en los asuntos de su competencia; siendo que esta autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico.

2. Que, en el artículo 27°, y 39°, de la Ley N° 27972, Ley Orgánica de Municipalidades, se establece que:

   *"**Artículo 27**.- Gerencia Municipal*

   ***La administración municipal está bajo la dirección y responsabilidad del gerente municipal**, funcionario de confianza a tiempo completo y dedicación exclusiva designado por el alcalde (…)."*

   *"**Artículo 39**.- Normas Municipales*
   (…)
   ***Las gerencias resuelven los aspectos administrativos a su cargo a través de resoluciones** y directivas."*

3. Que, en los artículos 1°, 2°, 3°, y 5A° de la Ley N°27658, Ley Marco de Modernización de la Gestión del Estado, se establece que:
   "Artículo 1.- Declárase al Estado en proceso de modernización

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

1.2. El proceso de modernización de la gestión del Estado será desarrollado de manera coordinada entre el Poder Ejecutivo a través de la Dirección General de Gestión Pública de la Presidencia del Consejo de Ministros y el Poder Legislativo a través de la Comisión de Modernización de la Gestión del Estado, con la participación de otras entidades cuando por la materia a desarrollar sea ello necesario."

"Artículo 2.- Objeto de la ley

La presente Ley tiene por objeto establecer los principios y la base legal para iniciar el proceso de modernización de la gestión del Estado, en todas sus instituciones e instancias."

"Artículo 3.- Alcance de la ley

La presente Ley es de aplicación en todas las dependencias de la Administración Pública a nivel nacional."

"Artículo 4.- Finalidad del proceso de modernización de la gestión del Estado

El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos. El objetivo es alcanzar un Estado:

a) Al servicio de la ciudadanía.
b) Con canales efectivos de participación ciudadana.
c) Descentralizado y desconcentrado.
d) Transparente en su gestión.
e) Con servidores públicos calificados y adecuadamente remunerados.
f) Fiscalmente equilibrado"

"Artículo 5-A.- Sistema Administrativo de Modernización de la Gestión Pública

5-A.1 El Sistema Administrativo de Modernización de la Gestión Pública tiene por finalidad velar por la calidad de la prestación de los bienes y servicios; propiciar la simplificación administrativa; promover y mejorar la calidad en las regulaciones en el ámbito de competencia de la Presidencia del Consejo de Ministros; el gobierno abierto; la coordinación interinstitucional; la racionalidad de la estructura, organización y funcionamiento del Estado; y la búsqueda de mejoras en la productividad y en la gestión de procesos; la evaluación de riesgos de gestión y la gestión del conocimiento, hacia la obtención de resultados."

MUNICIPALIDAD DE VILLA EL SALVADOR V°B° ASESORIA JURIDICA

4. Que, en los artículos 1°, 2°, 4°, 6°; 7°, 30°, inciso D) del artículo 32°, y el artículo 34°, del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se establece que:

*"**Artículo 1.- Objeto***

La presente Ley tiene por objeto establecer el marco de gobernanza del gobierno digital para 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."

"Artículo 2.- Ámbito de aplicación

2.1. La presente Ley es de aplicación a toda entidad que forma parte de la Administración Pública a que se refiere el artículo I del Título Preliminar del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General. Sus regulaciones también alcanzan a las personas jurídicas o naturales que, por mandato legal, encargo o relación contractual ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público, en los términos dispuestos por la Presidencia del Consejo de Ministros.

2.2. En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da en todo aquello que le resulte aplicable."

"Artículo 4.- Finalidad

La presente Ley tiene por finalidad:

4.1 Mejorar la prestación y acceso de servicios digitales en condiciones interoperables, seguras, disponibles, escalables, ágiles, accesibles, y que faciliten la transparencia para el ciudadano y personas en general.

4.2 Promover la colaboración entre las entidades de la Administración Pública, así como la participación de ciudadanos y otros interesados para el desarrollo del gobierno digital y sociedad del conocimiento."

MUNICIPALIDAD DE VILLA EL SALVADOR V°B° ASESORIA JURIDICA

"Artículo 6.- Gobierno Digital

6.1. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

6.2. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la

digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos."

"Artículo 7.- Objetivos del Gobierno Digital

Los objetivos del gobierno digital son:

7.1 Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.

7.2 Coordinar, integrar y promover la colaboración entre las entidades de la Administración Pública.

7.3 Promover la investigación y desarrollo en la implementación de tecnologías digitales, identidad digital, servicios digitales, interoperabilidad, seguridad digital y datos.

7.4 Promover y orientar la formación y capacitación en materia de gobierno digital y tecnologías digitales en todos los niveles de gobierno."

"Artículo 30.- De la Seguridad Digital

La seguridad digital 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."

"Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano

El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:
(...)
***d. Institucional:** Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI)."*

"Artículo 34.- Financiamiento

La implementación de lo establecido en el presente Decreto Legislativo se financia con cargo al presupuesto institucional de las entidades involucradas, sin demandar recursos adicionales al Tesoro Público."

Que, en los artículos 1°, 2°, 3°, 4° y 5° del Decreto Supremo N° 123-2018-PCM, Decreto Supremo que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, se establece que:

MUNICIPALIDAD DE VILLA EL SALVADOR V°B° ASESORÍA JURÍDICA

"Artículo 1.- Objeto

El presente Reglamento tiene por objeto desarrollar el Sistema Administrativo de Modernización de la Gestión Pública, estableciendo los principios, normas y procedimientos que aplican al proceso de modernización de la gestión pública, en concordancia con la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado."

"Artículo 2.- Ámbito de aplicación

2.1 El presente Reglamento es de aplicación a toda entidad pública que forma parte de la Administración Pública, incluyendo aquellas que ejercen potestades administrativas, y por tanto su accionar se encuentra sujeto a normas de derecho público.

2.2 En el caso de las empresas que conforman la actividad empresarial del Estado, su aplicación se da solo en aquello que le resulte aplicable."

"Artículo 4.- Proceso de modernización de la gestión pública

4.1 La modernización de la gestión pública consiste en la selección y utilización de todos aquellos medios orientados a la creación de valor público en una determinada actividad o servicio a cargo de las entidades públicas. Se crea valor público cuando:

a) Las intervenciones públicas, que adoptan la forma de bienes, servicios o regulaciones, satisfacen las necesidades y expectativas de las personas, generando beneficios a la sociedad.

b) Se optimiza la gestión interna a través de un uso más eficiente y productivo de los recursos públicos, para, directa o indirectamente, satisfacer las necesidades y expectativas de las personas, generando beneficios a la sociedad.

.2 Los objetivos y contenidos principales del proceso de modernización de la gestión pública se desarrollan en la Política Nacional de Modernización de la Gestión Pública, cuya conducción recae en la Presidencia del Consejo de Ministros y requiere la intervención articulada de todas las entidades públicas."

"Artículo 5.- Gestión para resultados

Las entidades públicas aplican la gestión para resultados como un modelo de gestión que permite identificar y adoptar decisiones sobre todos aquellos aspectos que contribuyan a la creación de valor público."

MUNICIPALIDAD DE VILLA EL SALVADOR V°B°6. ASESORIA JURIDICA

Que en el numeral 14.9), y 14.12) del artículo 14° de la Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con Enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa El Salvador, aprobado con Ordenanza N° 369-MVES, que señala: *"14.9)* ***Emitir Resoluciones de Gerencia Municipal,*** *(...), y "14.12)* ***Dirigir los Procesos de Modernización y fortalecimiento***

Institucional ACORDE CON las Políticas Nacionales y los objetivos de estratégicos de desarrollo local".

7. Que, existiendo una probabilidad en la cual, una Organización sea susceptible a encontrarse frente a una situación de emergencia que puede originar efectos adversos ocasionando pérdidas de vidas humanas, ambientales, materiales, entre otros. **El tiempo y la capacidad de respuesta con que cuenta la Entidad son piezas Fundamentales para enfrentar, controlar cualquier situación de emergencia que se presente, tanto externo como internamente; en tal sentido, y como buena práctica la Unidad de Desarrollo Tecnológico, ha elaborado el Plan de Contingencia de Tecnologías de la Información, dado que la Institución es Susceptible a diferentes hechos que pueden interrumpir los servicios informáticos y afectar el normal funcionamiento de las actividades en la Institución; en consecuencia el presente Plan contiene medidas Técnicas, Humanas y Organizativas necesarias para amparar y custodiar la Integridad y Seguridad de la Información que maneja esta Corporación Edil, con relación con contingencias producidas en los Servidores de Base de Datos, los Equipos de Comunicación de Datos y Enlaces de Comunicación, el Software de Aplicación**. Asimismo, el citado Plan, establece los objetivos Generales y Específicos, al alcance y metodología del Plan, a fin de lograr minimizar el impacto negativo de la interrupción de los servicios informáticos, contribuyendo a que la Institución esté preparada ante cualquier eventualidad, o contingencia a nivel de tecnología de información, toda vez que se está considerando acciones del antes, durante y después de los incidentes.

8. Por lo tanto, es menester de este Despacho de Asesoría Jurídica, Precisar que conforme a los Fundamentos expuestos en el párrafo precedente, **se confirma la necesidad de contar con un Plan de Contingencias de Tecnologías de la Información, el cual tiene como finalidad la Protección de la Información Tecnológica de esta Corporación Edil, evitando lo más posible la pérdida de dicha Información, y salvaguardar la Infraestructura de la Red , Sistemas de Información y Base de Datos, extremando las medidas de Seguridad para protegernos y estar preparados ante una contingencia respecto al rubro**, ya que lo único que permite a la Institución reaccionar adecuadamente ante diversos procesos críticos, es por medio de la elaboración , y mantenimiento de un Plan de Contingencia, que servirá para responder de manera efectiva y eficaz ante una eventual emergencia; asimismo, el presente Plan, tiene congruencia con las normas legales previamente citadas, y se encuentra encaminada al cumplimiento de la Ley de Gobierno Digital; por lo tanto corresponde la aprobación de la misma mediante Resolución de Gerencia Municipal.

MUNICIPALIDAD DE VILLA EL SALVADOR V°B° ASESORÍA JURÍDICA

9. Estando a lo expuesto, en amparo de los fundamentos fácticos y jurídicos contenidos en el presente informe; esta **Oficina de Asesoría Jurídica** opina que **ES LEGALMENTE PROCEDENTE**, la Aprobación mediante **Resolución de Gerencia** del Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa el Salvador; en conformidad al artículo 27°, y 39°, de la Ley N° 27972, Ley Orgánica de Municipalidades, y en amparo del numeral 4.1, del artículo 4° del Decreto Supremo Nº 123-2018-PCM, Decreto Supremo que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, y del artículo 30°, y del inciso D) del artículo 32°, del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; esto, con el fin de lograr minimizar el impacto

negativo de la interrupción de los servicios informáticos, contribuyendo a que la Institución esté preparada ante cualquier eventualidad, o contingencia a nivel de tecnología de información, toda vez que se está considerando acciones del antes, durante y después de los incidentes.

IV. OPINIÓN:

En virtud a lo expuesto en el análisis del presente informe, esta Oficina de Asesoría Jurídica, es de la OPINION que:

1) **ES LEGALMENTE PROCEDENTE**, la Aprobación mediante **Resolución de Gerencia** del Plan de Contingencia de Tecnología de la Información de la Municipalidad Distrital de Villa el Salvador; en conformidad al artículo 27°, y 39°, de la Ley N° 27972, Ley Orgánica de Municipalidades; y en amparo del numeral 4.1, del artículo 4° del Decreto Supremo Nº 123-2018-PCM, Decreto Supremo que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública; y del artículo 30°, y del inciso D) del artículo 32°, del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; esto en concordancia al numeral 14.12 del artículo 14° de la Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con Enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa El Salvador, aprobado con Ordenanza N° 369-MVES; Por lo tanto, **el presente Plan tiene como finalidad la Protección de la Información Tecnológica de esta Corporación Edil, evitando lo más posible la pérdida de dicha Información, y salvaguardar la Infraestructura de la Red , Sistemas de Información y Base de Datos, extremando las medidas de Seguridad para protegernos y estar preparados ante una contingencia respecto al rubro, para así poder responder de manera efectiva y eficaz ante una eventual emergencia, considerando acciones del antes, durante y después de los posibles incidentes.**

2) Corresponde que la Gerencia Municipal, de acuerdo a su función normativa y reguladora establecida en el numeral 14.9, y 14.12 del artículo 14° de la Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con Enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa El Salvador, aprobado con Ordenanza N° 369-MVES, que señala: *"14.9) **Emitir Resoluciones de Gerencia Municipal**, (...), y "14.12) **Dirigir los Procesos de Modernización y fortalecimiento Institucional acorde con las Políticas Nacionales y los objetivos de estratégicos de desarrollo local.***

MUNICIPALIDAD DE VILLA EL SALVADOR
Abg. Shirlet M. Castro Gonzales
Gerente de Asesoría Jurídica

MEMORANDO N° 1090 -2022-GM/MVES

MUNICIPALIDAD DE VILLA EL SALVADOR
RECIBIDO
OFICINA DE ASESORÍA JURÍDICA
20 OCT. 2022
Folios: 4 Hora:

A : Abg. Shirlet Marley Castro Gonzales
Gerente de Asesoría Jurídica

DE : Abg. José Luis Espichán Pérez
Gerente Municipal

ASUNTO : Revisión y Aprobación del Plan de Contingencia de Tecnologías de la Información de la Municipalidad Distrital de Villa el Salvador

REF. : a) Informe N° 0158-2022-UDT-OGA/MVES
b) Memorando Múltiple N° 046-2022-OGA/MVES
c) Memorando N° 035-2022-GM-MVES

FECHA : Villa El Salvador, 19 de octubre del 2022

Me es grato dirigirme a usted, en atención al documento de la referencia a); por el cual el Subgerente de la Unidad de Desarrollo Tecnológico traslada los actuados; por lo que; le solicito a fin que su despacho sirva emitir opinión legal relacionado a la Revisión y Aprobación del Plan de Contingencia de Tecnologías de la Información de la Municipalidad Distrital de Villa El Salvador; en relación al documento de la referencia b) y c).

En tal sentido, se remiten los actuados para la opinión jurídica correspondiente; de acuerdo a su competencia como órgano de asesoramiento establecida en el artículo **24.6** del Reglamento de Organización y Funciones (ROF) de la entidad.

Atentamente,

MUNICIPALIDAD DE VILLA EL SALVADOR
GERENCIA MUNICIPAL
JOSÉ LUIS ESPICHÁN PÉREZ
GERENTE

MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR	OFICINA GENERAL DE ADMINISTRACIÓN	UNIDAD DE DESARROLLO TECNOLÓGICO

MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR
GERENCIA MUNICIPAL
19 OCT 2022
RECIBIDO
FOLIO 56 HORA

INFORME N° 0158-2022-UDT-OGA/MVES

A	:	**JOSE LUIS ESPICHAN PEREZ** Gerente Municipal
DE	:	**ING. JOSE MANUEL GUIZADO CASTILLO** Sub Gerente de la Unidad de Desarrollo Tecnológico
ASUNTO	:	**Revisión y Aprobación del Plan de Contingencia de Tecnologías de la Información de la Municipalidad Distrital de Villa el Salvador**
REF.	:	a). Memorando Múltiple N°035-2022-GM//MVES b). Memorando Múltiple N°046-2022-OGA/MVES
FECHA	:	Villa El Salvador, 10 de octubre del 2022

Mediante documento de referencia a) y b), de fecha 28SET22 y 06OCT22 respectivamente, la Oficina General de Administración remitió a esta Unidad, el *"Reporte de Seguimiento a la implementación de las recomendaciones de los informes de servicios de control posterior"* del 1 al 31 de agosto de 2022, en solicitud de cumplir con los plazos establecidos con la entrega de la documentación solicitada y se adopten medidas necesarias a fin de culminar la implementación de las recomendaciones advertidas por el OCI.

Que, la recomendación Nro.06 de la Carta de Control Interno – Reporte de Deficiencia Significativas N°006-2020-3-0550 – periodo 2019, señala que; *"La Gerencia Municipal disponga al Subgerente de la Unidad de Desarrollo Tecnológico, el desarrollo del Plan de Contingencia, de Seguridad de la Información, así como el Plan de Desarrollo Tecnológico. Asimismo, elabore un informe Técnico de las necesidades tecnológicas de la Municipalidad"* y la recomendación Nro.20 de la Carta de Control Interno – Reporte de Deficiencias Significativas N°019-2021-3-0550 – periodo 2020 señala que; *"Se recomienda a la UDT de la Municipalidad, iniciar la actualización de su plan de contingencias, plan operativo, y PETI, por lo menos hasta que el Plan de Gobierno Digital inicie a funcionar"*.

I. ANTECEDENTES:

- Mediante el Memorando Múltiple N°086-2020-GM-MVES de fecha 07 de agosto del 2020, la Gerencia Municipal traslada a la Oficina General de Administración las *"Conclusiones Finales de la S.O.A. (Sociedad de Auditoria), de 38 folios, que ha comunicado: Deficiencias de Control Interno en relación al periodo 2019"*, solicitando remitir un informe de acciones a ejecutar referente a Plan de Contingencia de Seguridad de la Información entre otros.

- Mediante el Memorando N°345-2020-OGA/MVES de fecha 10 de agosto de 2020, la Oficina General de Administración solicita a esta Unidad, se remita el Plan de Acción para la implementación de las recomendación Nro.06 correspondiente a la *"Carta de Control Interno de la Auditoria Financiera Gubernamental por el periodo 2019"*, en respuesta a la recomendación nro. 06 entre otros contenidas en el carta de control interno; señala que, *"a la Gerencia Municipal disponga a la Gerencia al Subgerente esta unidad, el desarrollo del Plan de Contingencia, de Seguridad de la Información, así como el Plan de Desarrollo Tecnológico. Asímismo, elabore un Informe Técnico de las necesidades tecnológicos de la municipalidad"*.

- Mediante el Memorando Múltiple Nro.0606-2021-GM/MVES de fecha 27 de mayo de 2021, la Gerencia Municipal traslada a esta Unidad, la Carta de Control Interno – Auditoria Financiera Gubernamental por el periodo 2020 emitido por la Sociedad Auditora Ventosilla Vásquez &

Asociados", solicitando implementar las recomendaciones dadas e informar directamente a la Sociedad Auditora.

- Mediante el Memorando Múltiple Nnro.039-2021-OGA/MVES de fecha 03 junio de 2021, la Oficina General de Administración, solicita a esta Unidad, se remita el Plan de Acciones para la implementación de la recomendación Nro.20 correspondiente a la Carta de Control Interno – Auditoría Financiera Gubernamental por el periodo 2020, en respuesta a la recomendación Nro. 20 entre otros contenida en la carta de control interno, señala que *"Se recomienda a la UDT de la Municipalidad, iniciar la actualización de su Plan de Contingencias, plan operativo y PETI, por lo menos hasta que el Plan de Gobierno Digital inicie a funcionar"*

- Mediante el Memorando Múltiple N.° 039-2022-OGA/MVES de fecha 12 de agosto del 2022, la Oficina General de Administración, solicita remitir *"Reporte de Seguimiento a la Implementación de las Recomendaciones de los Informes de Servicio de Control Posterior"* al 31 de Julio 2022, solicitando concretar la recomendación Nro.06, Nro.20 entre otros correspondiente al Control Interno de Auditoria periodo 2019 y Control Interno de Auditoria periodo 2020 respectivamente, señala que; esta Unidad desarrolle e implemente el Plan de Contingencia de la Municipalidad Distrital Villa El Salvador.

II. BASE LEGAL:

- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 27815, Ley del Código de Ética de la Función Pública.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Ley N° 3096, Ley de Delitos Informáticos.
- Resolución Ministerial N°320-2021-PCM, aprueba los Aprobación de Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Publicas de los tres niveles de Gobierno
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Decreto Supremo N°. 004-2013-PCM, publicada el 09 de enero del 2013, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la

Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".

- Resolución de Contraloría N° 320-2006-CG, "Normas de Control Interno para las Entidades del Estado"
- NTP-ISO/IEC 27003:2019 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Orientación. 2ª Edición
- NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

III. ANALISIS:

- Con el Informe N°0109-2020-UDT-OGA/MVES, la Unidad de Desarrollo Tecnológico remite a la Oficina General de Administración el Plan de Acción para la Implementación de Recomendaciones de la Carta de Control Interno de la Auditoria Financiera Gubernamental por el periodo 2019, señalando un plazo establecido y acciones concretas a ejecutar para el desarrollo del Plan de Contingencia de Seguridad de la Información.
- Con el Carta Nro.005-2021-UDT-OGA/MVES, la Unidad de Desarrollo Tecnológico remite al Sr. Jorge Ventocilla Ventocilla Apoderado (Sociedad de Auditoria Ventosilla Vásquez & Asociados S.C.R.L.) el Plan de Acción para la Implementación de las Recomendaciones de la Carta de Control Interno de la Auditoria Financiera Gubernamental pro el periodo 2020, señalando plazo establecido y acciones concretas a ejecutar para iniciar la actualización del Plan de Contingencia de Seguridad.
- Con Memorando múltiple N.° 046-2022-OGA/MVES, la Oficina General de Administración remite a la Unidad de Desarrollo Tecnológico el *"Reporte de Seguimiento a la implementación de las recomendaciones de los informes de servicios de control posterior"* del 1 al 31 de agosto de 2022, solicitando cumplir con la ejecución de los Planes de Acción de las Recomendaciones Nro. 06 y Nro.20 entre otros remitidas a OCI.
- La ISO 22301 es la norma internacional para la Gestión de la Continuidad de Negocio (SGCN). Publicado por la Organización Internacional de Normalización, la ISO 22301 está diseñada para ayudar a las organizaciones a prevenir, preparar, responder y recuperarse de incidentes inesperados. Para ello, la norma proporciona un marco práctico con el fin de establecer y gestionar un sistema de gestión de continuidad de negocio eficaz. La ISO 22301 tiene como objetivo proteger a la organización de una amplia gama de posibles amenazas e interrupciones.
- Cabe precisar que, los puntos 1) y 4) del artículo 36 de Reglamento de Organización y Funciones (ROF) de la Municipalidad Distrital de Villa El Salvador, señala "*Diseñar el Plan de Contingencia Informático, el Plan de Seguridad de la Información, y otros planes que sean de su competencia*", y, "*Proponer proyectos de normas municipales en materia de su competencia para la mejora de la gestión*", como las funciones de Planeamiento y Normativa de la unidad, respectivamente.

En este sentido, en cumplimiento a lo solicitado por el Órgano de Control Institucional, se traslada el Plan de Contingencia de Tecnologías de la Información para su revisión y aprobación, correspondiente a la Recomendación Nro.06 y Nro.20 de la "*Carta de Control Interno de la Auditoria Financiera Gubernamental por el periodo 2019*" y "*Carta de Control Interno de la Auditoria Financiera Gubernamental por el periodo 2020*", respectivamente, en cincuenta (50) folios.

Atentamente,

Municipalidad Distrital de Villa El Salvador
V°B°
OGA

MUNICIPALIDAD DE VILLA EL SALVADOR
UNIDAD DE DESARROLLO TECNOLÓGICO
Ing. José Manuel Guizado Castillo
SUB - GERENTE

21

OFICINA GENERAL DE ADMINISTRACIÓN
MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR

MEMORANDO MÚLTIPLE N° 046-2022-OGA/MVES

A : **Abog. SHIRLET MARLEY CASTRO GONZALES**
Subgerente de la Unidad de Gestión de Recursos Humanos (e)
CPC. DERRY CHAVEZ SALAZAR
Subgerente Encargado de la Unidad de Abastecimiento
Ing. JOSÉ MANUEL GUIZADO CASTILLO
Subgerente de la Unidad de Desarrollo Tecnológico
CPC. JOSE JAUREGUI BASOMBRIO
Subgerente de la Unidad de Contabilidad
Bach. YETTY ZAVALLOS MAMANI
Subgerente de la Unidad de Tesorería

MUNICIPALIDAD DE VILLA EL SALVADOR
06 OCT 2022
RECIBIDO
Folio: ..... Hora: .....

Asunto : Reporte bimestral de "*Seguimiento a la implementación de las recomendaciones de los informes de servicio de control posterior del 1 al 31 de agosto de 2022*"

Referencia : a) Memorando Múltiple N° 035-2022-GM-MVES
b) Oficio N° 000082-2022-CG/OC2696
c) Proveído N°0087-2022-ALC/MVES

Fecha : Villa El Salvador, 06 de octubre de 2022

Que, con documento de la referencia a), de fecha 29SET2022, la Gerencia Municipal, traslada a vuestras Unidades Orgánicas y a esta Oficina el documento de la referencia b), de fecha 22SET2022, mediante el cual, la Jefa del Órgano de Control Institucional pone en conocimiento el Reporte de "*Seguimiento a la implementación de las recomendaciones de los informes de servicio de control posterior del 1al 31 de agosto de 2022*", derivado por Alcaldía con el documento de la referencia c), de fecha 26SET2022.

Al respecto, la Gerencia Municipal, exhorta cumplir con los plazos establecidos con la entrega de la documentación solicitada por el OCI y se adopten las medidas pertinentes, a fin de culminar con la implementación de las recomendaciones, acompañando el sustento documental; teniendo presente que, la dilación o no entrega de la documentación e información, puede ser sujeta a la aplicación de sanciones de conformidad a los Artículos 41° y 42° de la Ley N° 27785 "Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República"; ***bajo responsabilidad administrativa y funcional; bajo expreso apercibimiento de remitir los actuados a la Secretaría Técnica de Procesos Disciplinarios para las acciones correspondientes.***

En ese sentido, se **DISPONE** a las Unidades de Contabilidad, Tesorería, Abastecimiento, Gestión de Recursos Humanos y Desarrollo tecnológico, remitir vuestros informes a este despacho respecto de la implementación de las recomendaciones de los Informes de Servicios de control Posterior del 1 al 31 de Agosto de 2022, **hasta el martes 11OCT2022, *bajo responsabilidad***. Se adjunta el Anexo N° 01 con las acciones realizadas y dispuestas por esta oficina.

Atentamente;

MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA GENERAL DE ADMINISTRACIÓN

ING. LUZ ZANABRIA LIMACO
GERENTE

MEMORÁNDUM MULTIPLE N° 035 - 2022 - GM-MVES

MUNICIPALIDAD DE VILLA EL SALVADOR
Oficina General de Administración
UNIDAD DE DESARROLLO TECNOLÓGICO
29 SEP 2022
RECIBIDO
Folio: 10 Hora: 10:20

A : Gerente de la Oficina General de Administración
SubGerente de la Unidad de Gestión Recursos Humanos
SubGerente de la Unidad de Contabilidad
SubGerente de la Unidad de Abastecimiento
SubGerente de la Unidad de Tesorería
SubGerente de la Unidad de Desarrollo Tecnológico
Gerente de la Oficina de Planeamiento y Presupuesto
SubGerente de la Unidad de Planeamiento Estratégico, Modernización
Gerente de Desarrollo Urbano
SubGerente de Proyectos y Obras Públicas
SubGerente de Obras Privadas, Catastro y Control Urbano
Gerente de Rentas y Administración Tributaria
SubGerente de Recaudación, Control y Ejecutoria Coactiva
SubGerente de Fiscalización Tributaria
Gerente de Desarrollo e Inclusión Social
Gerente de la Oficina de Asesoría Jurídica
Procuraduría Pública Municipal

DE : Abg. José Luis Espichán Pérez
Gerente Municipal

ASUNTO : **Seguimiento a la implementación de las recomendaciones de los informes de servicios de control posterior a julio de 2022**

REF. : a) Proveído Nº 0087-2022-ALC/MVES
b) Oficio Nº 000082-2022-CG/OC2696 de fecha 22.09.2022

FECHA : Villa El Salvador, 28 de setiembre de 2022

Me Dirijo a Usted, con relación al documento a) de la referencia; recepcionado con fecha 26.09.2022; por el cual el despacho de Alcaldía traslada el requerimiento solicitado por el **OCI**, a través del documento de la referencia b); en la que remite el reporte del **"Seguimiento a la Implementacion de las recomendaciones de los informes de servicios de control posterior, del 01 al 31 de agosto de 2022"**; que a la fecha se encuentran **pendientes o en proceso**; por lo que; se les **EXHORTA** a cada área de acuerdo a su competencia; deberá cumplir dentro los plazos establecidos la entrega de la documentos solicitados y que adopten las medidas necesarias a fin de culminar las implementaciones de las aludidas recomendaciones advertidas por el **OCI**; acompañando el sustento documental; teniendo presente que la dilación o no entrega de la documentación e información, puede ser sujeta a la aplicación de sanciones de conformidad a los Artículos 41° y 42 de la Ley Nº 27785 Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.

En tal sentido, proceda a remitir de manera **urgente** lo solicitado por el **OCI,** dentro el plazo de cinco **(5)** días; dando cuenta a este despacho bajo responsabilidad administrativa y funcional; bajo expreso apercibimiento de remitir los actuados a la Secretaría Técnica de Procesos Disciplinarios para las acciones correspondientes. (Se adjunta reporte del OCI de las recomendaciones de cada área de su competencia).

Atentamente,

MUNICIPALIDAD DE VILLA EL SALVADOR
GERENCIA MUNICIPAL
JOSÉ LUIS ESPICHAN PEREZ
GERENTE

PLAN DE CONTINGENCIA DE TECNOLOGIA DE LA INFORMACION

2022

CONTROL DE CAMBIOS

N° Versión	Fecha	Descripción de cambio	Responsable del Documento

1. INTRODUCCION

El presente documento define el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información de la Municipalidad de Villa El Salvador, el plan es como procesos continuos de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso que ocurre una emergencia que interrumpa la operatividad de los sistemas.

En el marco de la Resolución Ministerial N.° 028-2015-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno, se señala que el Plan de Continuidad Operativa comprende, entre otros planes específicos, el Plan de Contingencia y el Plan de Recuperación de Servicios Tecnológicos de la Información.

Por lo tanto, el plan contiene medida técnicas, humanas y organizativas necesarios para amparar y custodiar la integridad y seguridad de la información que maneja la Municipalidad con relación con contingencias producidas en los Servidores de Base de Datos, los Equipos de Comunicación de Datos y enlaces de Comunicación, el Software de Aplicación y los datos, y garantizar su continuidad en las operaciones.

Como instrumento de gestión apoya en el buen trabajo manejo de las Tecnologías de información y de las Comunicaciones (TIC's)

El Plan de contingencias deberá ser actualizado anualmente. Así mismo, es revisado/evaluado cuando se materializa u ocurre.

2. OBJETIVO

2.1. Objetivo General

Determinar las funciones que deberán ser ejecutadas ante determinados eventos que podrían alterar sus obligaciones laborales, con la finalidad de garantizar la continuidad operativa de los servicios críticos de tecnologías de la información que brinda la institución; por ello es que se definen procesos técnicos con la intención de salvaguardar y reestablecer los servicios en forma eficiente, rápida y oportuna, reduciendo el impacto negativo en las funciones de cada usuario.

2.2. Objetivo Especifico

- Restablecer y/o recobrar el servicio informático al presentarse alguna contingencia grave en la Municipalidad de Villa El Salvador, ocasionado por fallas de la plataforma informática (infraestructura de res, servidores, PCs, dispositivos de comunicación, y software de aplicaciones)
- Definir acciones y procedimientos a ejecutar en caso fallas de los elementos que componen un Sistema de Información.
- Disponer de personal capacitado y organizado para afrontar los eventos de contingencias que puedan presentarse.

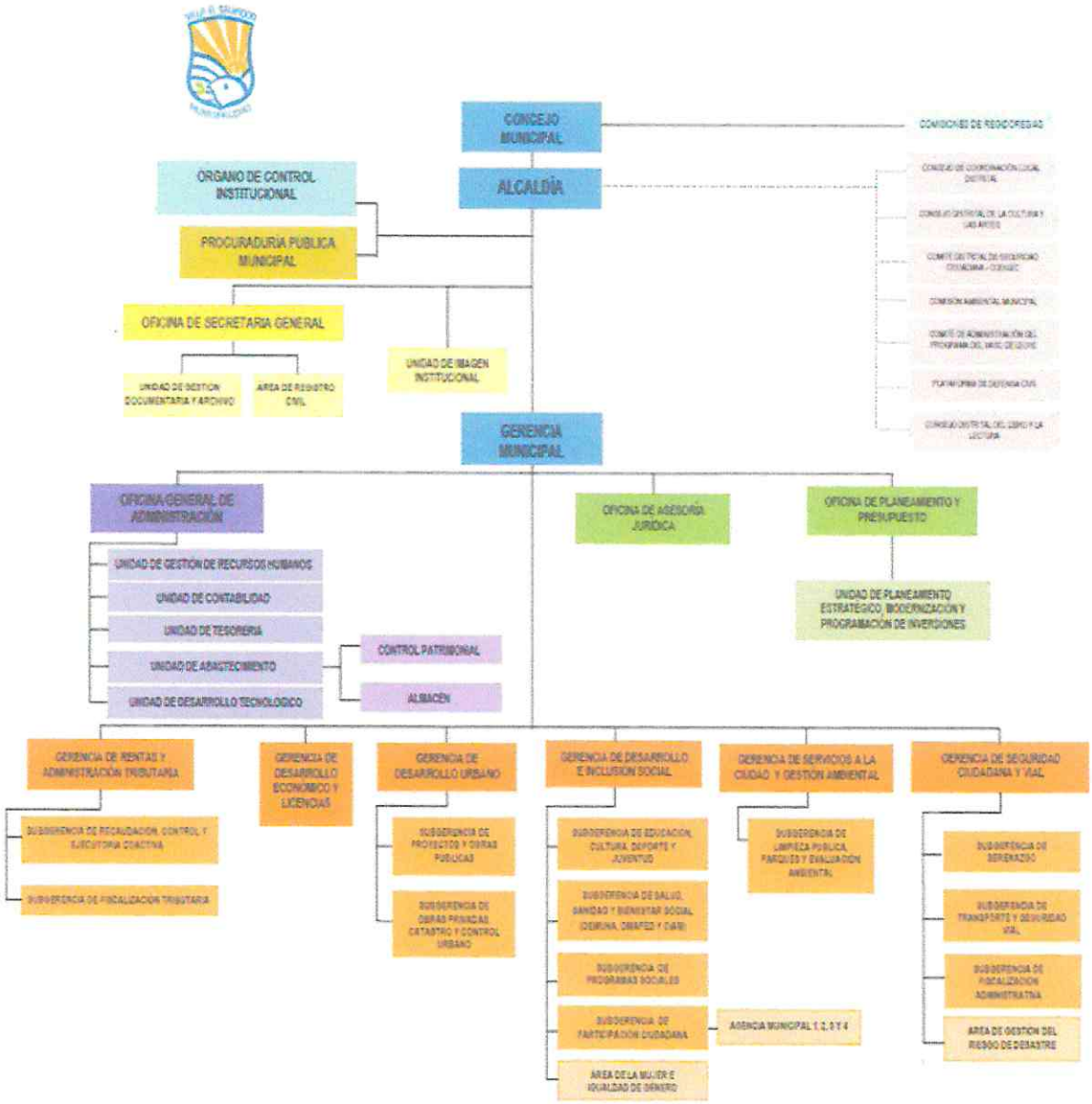
3. ALCANCE

El presente Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalación tecnologías, personal, servicios y otros administrados por la Unidad de Desarrollo Tecnológico, direccionado a minimizar eventuales riesgos antes situaciones adversas que atentan contra el normal funcionamiento de los servicios informativos de la entidad.

4. BASE LEGAL

- Ley N° 27658 – Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 23716 – Ley de Control Interno de las Entidades del Estado.
- Decreto Supremo N° 018-2017-PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la inscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ordenanza N°435-MVES que modifica la Ordenanza Nº 369-MVES, que aprueban el Reglamento de Organización y Funciones (ROF) de la Municipalidad de Villa El Salvador – MVES.
- Resolución Ministerial N° 004-2016-PCM - Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 028-2015-PCM, Aprueban Lineamientos para la gestión de la Continuidad Operativa en entidades públicas en los tres niveles de gobierno.
- Resolución de Contraloría General Nº 320-2006-CG, que aprueba las "Normas de Control Interno", que son de aplicación a las entidades del Sector Publico.
- ISO:22301-2020: Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301.La ISO 22301 es la norma internacional para la Gestión de la Continuidad de Negocio (SGCN). Publicado por la Organización Internacional de Normalización, diseñada para ayudar a las organizaciones a prevenir, preparar, responder y recuperarse de incidentes inesperados.

5. ORGANIGRAMA DE LA MUNICIPALIDAD DE VILLA EL SALVADOR



6. MARCO TEORICO

6.1. Plan de Contingencia Informático:

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización. Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

- Antes, como un plan de prevención para mitigar los incidentes.
- Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.

- Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

6.2. Incidente

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

6.3. Método de análisis de riesgos

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

6.4. Plan de Prevención

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

6.5. Plan de Ejecución

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

6.6. Plan de Recuperación

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

6.7. Plan de Pruebas

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

6.8. Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6.9. Riesgo Operativo

Riesgo vinculado a la administración y supervisión del personal.

6.10. Servicio critico

Servicio de gran valor para el cumplimiento de los objetivos de la Municipalidad.

7. FASES DE LA METODOLOGIA PARA EL DESARROLLO DE UNA PLAN DE CONTINGENCIA INFORMATICA

Debemos de tener presente que dependerá de la infraestructura de la Municipalidad y de los servicios que ofrezca para determinar un modelo de desarrollo de plan, no existe un modelo único para todos, lo que se intenta determinar los puntos más importantes.

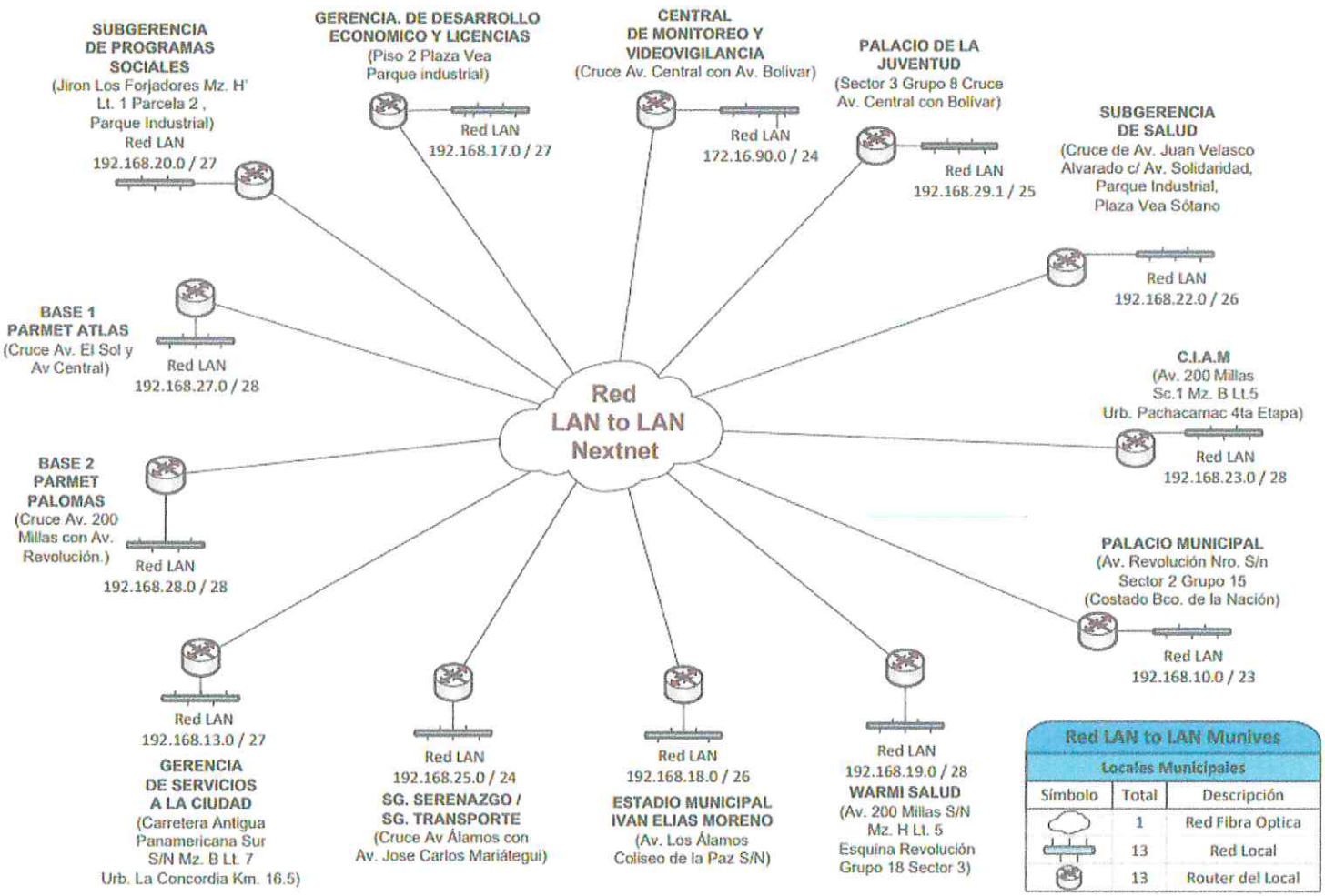
- Planificación: preparación y aprobación de esfuerzos y costos.
- Identificación de riesgos y escenario de contingencia: Evaluación de Riesgos de fallas o interrupciones.
- Estrategias: otras opciones, soluciones alternativas, procedimientos manuales.
- Documentación del proceso: creación de un manual del proceso y/o actividades en las etapas de prevención, ejecución y recuperación desarrollada en cada evento
- Definición y Realización de pruebas: selección de casos, soluciones que podrían funcionar.
- Implementación del Plan de Contingencia
- Monitoreo: probar nuevas soluciones o validar los casos

7.1. Fase 1 : Planificación

7.1.1. Diagnostico Actual

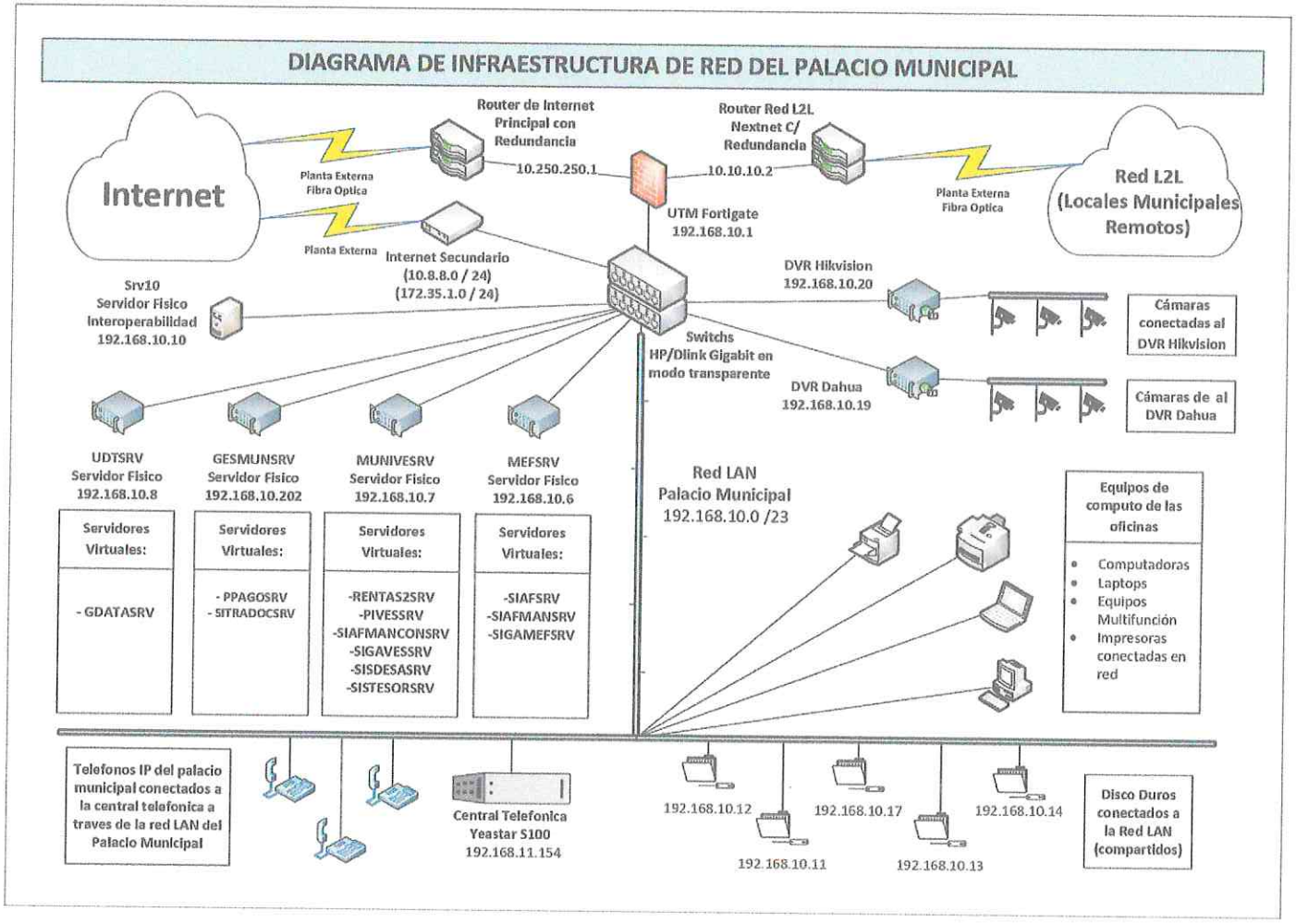
La Unidad de Desarrollo Tecnológico (UDT) depende directamente de la Oficina General de Administración (OGA), y tiene dentro de sus funciones es administrar la integridad, confiabilidad, y seguridad en el acceso de la base de datos institucional, así como establece mecanismos de registro histórico de modificaciones, autenticación de usuarios, auditoría y control de accesos a la base de datos; además de diseñar, construir, implantar, mantener los sistemas informáticos e infraestructura tecnológica necesaria para el cumplimiento de los objetivos de la Municipalidad, así como asegurar la disponibilidad y brindar soporte a los mismos.

Arquitectura de Red de la Municipalidad de Villa El Salvador



Infraestructura Tecnológica

MUNIVES posee una configuración de red jerarquizada, conformada por dos switches de marca D-Link



- Inventario de recursos informáticos e Infraestructura tecnológica.

La Municipalidad de Villa El Salvador cuenta con la siguiente infraestructura

Elemento	Descripción
Servidores	03 servidores tipo Torre (SIAF – Interoperabilidad, SigaMEF)
Equipos de Comunicación	Equipos del Servicio de la empresa de Telecomunicaciones
Conectividad	Switch
Servicio de acceso a la Internet	Si
Ancho de Banda	
Certificados Digitales	No
Protocolos	No
Computadoras Personales y otros	388 computadoras de escritorio
Software de Base / Ofimática	Windows 10 LTSC y Office Standard 2019

- Inventario de Equipos de computo

Nombre	Descripción / Alcance
Computadoras	341
Impresoras	135
All in One	8
Computadora personal portátil	39
Servidor	15
Acumulador de Energía - Equipo UPS	3
Banco de baterías	1
Impresora Multifuncional Laser	23

Impresora Multifuncional Tina	75
Impresora Fotocheck	1
Impresora Para Planos - Plotters	3
Proyector	2
Gabinete de metal	2
Grupo electrógeno	2
Detector Biométrico	1
Marcador de Asistencia	1
Access Point	1
Anexos	144

- Sistemas Operativos Instalados

Descripción	Estaciones de Trabajo	
	Munives	BYOD
Microsoft Windows 10 Enterprise LTSC	109	-
Microsoft Windows 10 Home Single Language	8	7
Microsoft Windows 10 Pro	132	5
Microsoft Windows 11 Home	0	2
Microsoft Windows 7 profesional	26	-
Microsoft Windows 7 Ultimate	1	1
Microsoft Windows 8.1 PRO	4	1

- Servidores

EPAL: En Proceso de Adquisición de Licencia.

Descripción	Operativos	Inoperativo	Sistema Operativo	Licenciado
Servidor HP Proliant DL380 Gen10	4		Microsoft Windows Server 2016 DC	En Proceso de Adquisición de Licencia
Servidor HP Proliant ML350p Gen8	1		Microsoft Windows Server 2016 Standar	
Sevidor HP Proliant ML350p	1		Microsoft Windows Server 2012 R2	
Servidor Dell Inc. PowerEdge R640	5		Windows Server 2019 Standard 64-bit	Licenciado
Servidor Dell Inc. Precision 3930 Rack	1		Microsoft Windows 10 Enterprise	
Servidor Dell EMC. GT28R009-02	1		Firmware: Version: GT280R009-02	
Servidor American Megatrends Inc. 38508	1		Centos Linux Release 7.7.1908 (core)	
Servidor Dell Inc. PowerEdge T40 (095B)	1		Centos Linux Release 7.9.2009 (core)	
Servidor HP Proliant DL380 Gen9		2	-	-

- Gestor de Base de Datos

Descripción	Servidores Instalados	Licenciada
Microsoft SQL Server 2014	1	En Proceso de Adquisición de Licencia

- Gestor de Base de Datos Virtualizado

Descripción	Cantidad	Licenciada
Microsoft SQL Server 2008	1	En Proceso de Adquisición de Licencia
Microsoft SQL Server 2017.9.1	1	
Microsoft SQL Server 2018	2	
MySQL	1	

- Correo electrónico corporativo.

Servidor de Correo Electrónico	Plan	Cantidad
Gmail	Google WorkSpace Business Starter	300

- Servidores Virtualizados

Descripción	Operativos	Licenciada
Windows Server 2016	3	Licencia
Windows Server 2016	6	En Proceso de Adquisición de Licencia
Windows Server 2012 R2	5	
Windows Server R Estándar	2	
Windows 10 pro 32 bits	1	
Windows Server 2019 DC	1	
Linux	3	

- Sistema de Información y/o Aplicativos

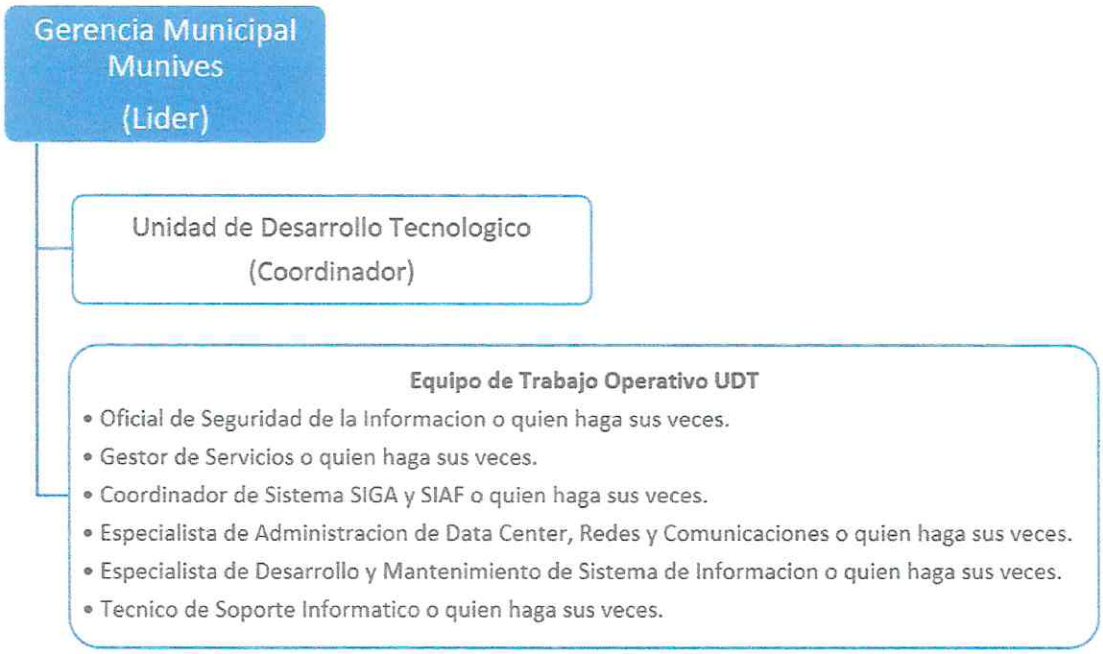
Nombre	Descripción	Alcance	Arquitectura	Observaciones
Sistema Integrado de Gestión Administrativa **(SIGA)**	Todas las Unidades Orgánicas	Permite la gestión para la programación, ejecución y control de los procesos administrativos bajo un enfoque integral en una entidad del Estado.	Desarrollado en Lenguaje Microsoft Visual FoxPro 9.0 con Gestor de Datos SQL Server 18.9	En producción desde el año 2022
Sistema de Rentas **(GESMUN)**	Gerencia de rentas, sub gerencia de recaudación, sub gerencia de fiscalización tributaria, sub gerencia de fiscalización administrativa, gerencia de desarrollo económico y licencias, unidad de tesorería, unidad de contabilidad.	Permite realizar la determinación y liquidación de los tributos que se administran. también administra procedimientos de gestión y administración tributaria como generación de valores, proceso de fiscalización, fraccionamiento, procedimiento de ejecución coactiva y prescripción de deudas; los que han sido desarrollados en función a la normatividad vigente.	Desarrollado en Lenguaje C# con Gestor de Datos SQL Server 2014	En producción desde el año 2020
Sistema **SIAF** municipalidad	Oficina general de administración, unidad de gestión de recursos humanos, unidad de contabilidad, unidad de tesorería, unidad de abastecimiento, oficina de planeamiento y presupuesto, unidad de planeamiento	Permite automatizar los procedimientos financieros necesarios para registrar los recursos públicos recaudados y aplicarlos a la concreción de los objetivos del sector público.	Desarrollado en Lenguaje Microsoft Visual FoxPro 9.0 con DBF's	En producción desde el año 2005

	estratégico, modernización y programación de inversiones			
Sistema de Tramite Documentario **(SITRADOC)**	Todas las unidades orgánicas	Permite regular y gestionar la recepción, registro, derivación y atención de documentación, así como el control y seguimiento de los documentos presentados.	Desarrollado en Lenguaje Asp.net (C# web) con Gestor de Datos SQL Server 2014	En Producción desde el año 2020
Sistema **RUOS** (registro único de organizaciones sociales)	Sub gerencia de participación ciudadana	Permite contar con un registro de las organizaciones sociales del distrito.	Desarrollado en Lenguaje PHP con Gestor de Datos MySQL	En Producción desde 2007
Sistema de marcación de asistencia **(Zicron)**	Unidad de gestión de recursos humanos	Permite registrar y gestionar el marcado de entrada y salida a la entidad para efectos de realizar la planilla de pagos.		En Producción desde 2000
Libro de Reclamaciones	Sistema de libro de Reclamaciones	Unidad de Gestión Documentaria y Archivo.	Desarrollado en Lenguaje PHP con Gestor de Datos MySQL	En Producción desde 2021
Mesa de Partes Digital	Sistema de Mesa de Partes Virtual			
Sistema **SIGA-VES**	Todas las unidades orgánicas	Permite simplificar y automatizar los procesos administrativos en la entidad siguiendo las normas establecidas por los órganos rectores.	Desarrollado en Lenguaje Microsoft Visual FoxPro 9.0 con DBF's	Solo para consultas entre los años 2016 - 2021
Sistema de Rentas Anterior **(SIM)**	Gerencia de rentas, sub gerencia de recaudación, sub	Permite realizar consultas: sobre determinaciones, estados de cuentas corrientes tributarias, procesos	Desarrollado en Lenguaje Power	Solo para consultas entre los años 2012 - 2020

	gerencia de fiscalización tributaria, sub gerencia de fiscalización administrativa, unidad de tesorería.	de fiscalizaciones, fraccionamientos, procedimientos de ejecución coactiva etc.	Builder con Gestor de Datos SQL Server 2008	
Sistema de Rentas antiguo (Marquina y Asociados)	Gerencia de desarrollo económico y licencias	Permite hacer procesos de licencias de funcionamiento.	Desarrollado en Lenguaje DOS Clipper	Solo para consultas entre los años 1994 - 2012
	Gerencia de rentas, sub gerencia de recaudación, sub gerencia de fiscalización tributaria.	Permite realizar consultas: sobre determinaciones, estados de cuentas corrientes tributarias, procesos de fiscalizaciones, fraccionamientos, procedimientos de ejecución coactiva etc.		
Sistema de Tramite Documentario (**SISTRADOC**)	Unidad de gestión documentaria y archivo, gerencia de rentas, sub gerencia de recaudación, sub gerencia de fiscalización tributaria, sub gerencia de fiscalización administrativa.	Permite regular y gestionar la recepción, registro, derivación y atención de documentación, así como el control y seguimiento de los documentos presentados.	Desarrollado en Lenguaje PHP con Gestor de Datos MySQL	Solo para consultas entre los años 2007 - 2020

7.1.2. Roles, funciones y responsabilidades dentro del Plan

Para el funcionamiento del Plan de Contingencia de los servicios de tecnología de la información, se ha establecido la siguiente organización operativa, conformado por el personal de la UDT.



El subgerente de la Unidad de Desarrollo Tecnológico debe asignar un miembro titular y un alterno, por cada integrante de los tres equipos mencionados previamente. Para tal efecto, se debe contar con la relación de la OTIC que forman estos equipos, quienes serán requeridos en el momento de la contingencia.

La relación del personal de la UDT que forma parte del Plan de contingencia debe ser actualizada de manera constante y socializada al siguiente personal:

a. **Gerencia Municipal** *(Líder)*
   - Participar en las reuniones periódicas propuestas por el subgerente de UDT
   - Proponer, aprobar o rechazar la incorporación y/o modificaciones del Plan de Contingencia TI.
   - Aprobar los informes presentados por el subgerente de UDT.
   - Realizar las coordinaciones para contar con la disponibilidad de recursos necesarios para soportar la operativa y la restauración de los servicios afectados por algún evento imprevisto.
   - Asegurar la provisión de esquemas de recuperación de los servicios y equipos de tecnología de la Información, tales como:
     - Infraestructura
     - Aplicaciones
     - Comunicaciones

- Servicios
- Centro de Datos

b. La Unidad de Desarrollo Tecnológico *(Coordinador)*

- Propiciar la aplicación de metodología de los planes de ejecución, recuperación y de las pruebas que conforman el Plan de Contingencia de la Tecnología de la Información.
- Tomar la decisión de activar el Plan de Contingencia TI y Recuperación de Servicios de Tecnologías de la Información y Comunicación.
- Gestionar los recursos necesarios para el correcto desempeño del Plan de Contingencia TI.
- Informar a la Dirección Ejecutiva sobre la materialización de algún evento de contingencia y sus resultados
- Activar/Desactivar la ejecución del Plan de Contingencia de TI
- Informar a las Unidades Orgánicas sobre la ocurrencia del evento de contingencia y coordinar las acciones necesarias.
- Dirigir y promover el desarrollo integral e implementación del Plan de Contingencia de TI, así como verificar el cumplimiento de las actividades encargadas a cada uno de los responsables.
- Asignar los responsables, así como la prioridad para el desarrollo de tareas.
- Propiciar las capacitaciones y entrenamientos internos al equipo de contingencia de TI con respecto a temas de continuidad y recuperación tecnológica.
- Informar al líder del Proyecto, los avances y ocurrencias durante el cumplimiento de las tareas de los responsables.

c. Equipo de Trabajo Operativo UDT

- **El Oficial de Seguridad de la Información o quien haga sus veces.**
  - Elaborar, revisar, presentar y mantener actualizado el Plan de Contingencia de TI.
  - Ejercer control y seguimiento del Plan de Contingencia de TI.
  - Informar a la Jefatura de TI sobre los resultados obtenidos en el desarrollo del Plan de Contingencia de TI.
  - Coordinar simulacros periódicos en la relación con el Plan de Pruebas con el fin de mantener activos a los miembros del equipo y la vigencia del Plan de Contingencia de TI.
  - Verificar que el personal involucrado este permanentemente capacitado respecto a su función dentro del Plan de Contingencia de TI.
  - Validar la información documentada de los procedimientos de restauración utilizados.
  - Verificar las tareas de copias de respaldo (Backus)
  - Participar en las pruebas y simulacros de desastres.

- **Gestor de Servicios de TI o quien haga sus veces.**
  - Mantener permanentemente actualizado el Plan de Contingencia
  - Coordinar la ejecución del Plan de Contingencia cuando se presentan los eventos que lo activan
  - Evaluar el impacto de las contingencias que se presenten
  - Elaborar los informes mensuales referidos al Plan de Contingencia.
  - Proponer, al Comité de Contingencia, la incorporación de nuevos eventos de riesgo en el Plan de Contingencia.
  - Capacitar al personal nuevo de servicios sobre las actividades que deben de ejecutar cuando se presenta la contingencia.
  - Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el Plan de Contingencia.
  - Proponer reuniones periódicas sobre el Plan de Contingencia.
  - Mantener actualizado el inventario de los equipos informáticos instalado en el Palacio Municipal y las sedes externas.

- **Especialista en administración de Data Center. Redes y Comunicaciones o quien haga sus veces.**
  - Verificar la activación automática de los equipos de energía.
  - Comunicar a todas las Unidades Orgánicas de MUNIVES del evento.
  - Apagar los servicios de los equipos de seguridad perimetral, comunicaciones y servidores que alojen los Sistemas.
  - Monitorear el uso de equipos de energía para el restablecimiento
  - Coordinar con las Unidades Orgánicas afectadas de tomar las medidas necesarias.
  - Realizar la evaluación de condiciones de los equipos de comunicaciones, telecomunicaciones y los componentes del Centro de Datos del MUNIVES.
  - Iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento de los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos del MUNIVES.
  - Notificar al proveedor de Servicios de telecomunicaciones.
  - Supervisar al proveedor para el restablecimiento de los servicios.
  - Monitorear que los servicios se encuentren en línea.
  - Realizar las pruebas previas de recuperación.
  - Actualizar los diagramas de servidores, los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones.
  - Mantener actualizado el inventario de hardware y software utilizado en el Centro de Datos de la entidad.

- **Coordinador del Sistema SIGA y SIAF o quien haga sus veces.**
  - Verificar el funcionamiento correcto del Servidor donde se ejecutar el Sistema SIGA y Gestor de Datos.
  - Coordinar acciones de mantenimiento de sistemas de información existentes asegurando el cumplimiento del ciclo de vida del software.
  - Comunicar al proveedor de soporte SIGA del MEF para validación del servicio.
  - Supervisar al proveedor para el restablecimiento de los servicios.
  - Validar el acceso del Sistema SIGA a través de la Red Municipal.
  - Validar el funcionamiento correcto del Servidor donde esta implementado el Sistema SIGA y el Gestor de Datos.
  - Restaurar las copias de respaldo correspondiente respetando la prioridad establecida para cada escenario.
  - Verificar el funcionamiento correcto de otros sistemas a su cargo como: SIAF Municipalidad, SIAF Mancomunidad de Lima Sur, BD Sistema de Marcación, RUOS y Sistemas Antiguos (Rentas, Letras del Parque Industrial de VES, Sistema de Tramite)
  - Comunicar al proveedor de servidor de correo electrónico en caso falla o caída de servicio.
  - Coordinar y verificar que se realicen las copias de respaldo de la fuente del SIGA.

- **Especialista de Desarrollo y Mantenimiento de Sistema Informático o quien haga sus veces.**
  - Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
  - Hacer pruebas al sistema de información o aplicativo una vez solucionado la falla.
  - Verificar los permisos sobre el sistema de información o aplicativo.
  - Informar a los usuarios la ruta del servidor del aplicativo.
  - Verificar el estado de las Base de Datos de los sistemas de información o aplicativo.
  - Restaurar las copias de respaldo correspondiente respetando la prioridad establecida para cada escenario.

- **Técnico de Soporte Informático o quien haga sus veces.**
  - Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros)
  - Preparar los equipos de cómputo para su reemplazo
  - Solicitar conformidad de la atención.
  - Notificar los casos críticos en cuanto a equipos de usuarios final, que afecte a la continuidad de operaciones y/o la perdida de información de los usuarios.
  - Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner, entre otros.

7.2. Fase 2: Identificación de Riesgos y Escenario

Los riesgos son sucesos inciertos que pueden llegar a presentarse en un futuro, dependiendo las variables externas o internas. Es entonces la cuantificación de una amenaza.

El Plan de Contingencia abarca todos los aspectos que forman parte del servicio informático, en tal sentido, se consideran todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia

7.2.1. Procesos y recursos críticos

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

Proceso Critico	Aplicaciones y/o recursos críticos
Gestión de redes e infraestructura de TI	Equipos de comunicación.
	Equipos de protección eléctrica del Centro de Datos (UPS)
	Sistema de aire acondicionado del Centro de Datos
	Infraestructura del Centro de Datos
	Cableado de red de datos
	Enlaces de cobre y fibra óptica para interconexión entre la sede central y el centro de datos
	Dispositivo para comunicación remota
	Pozo a tierra
	Servidores de red críticos: Directorio Activo, Base de Datos, etc.
	Servidores de red en general: Central telefónica
Gestión de sistemas de información y base de datos	Sistemas de información y aplicativo
	Sistemas de información administrativos
	Base de datos y repositorios utilizados por los sistemas y aplicativos
Soporte Técnico	Estaciones de trabajo del personal critico (computadoras personales y portátiles)
Operación y mantenimiento de TICS	Personal critico responsable de los procesos de TIC.

7.2.2. Identificación de amenazas

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

Nº	EVENTO/AMENAZA	DESCRIPCION
E1	Caída energía eléctrica	Corte de suministro eléctrico, falla en grupo electrógeno
E2	Caída de Internet y telefonía	Por corte de internet y/o servicios de telefónica, falta de renovación de servicio.
E3	Infección masiva por software malicioso	Falta de Antivirus, o Firewall para contrarrestar virus, troyanos, etc.
E4	Suspensión de las funciones por desastres naturales o accidentales	Terremotos, fuego fortuito, aniego, etc.
E5	Accesos no autorizados al Centro de Datos	Falta políticas de seguridad de acceso al centro de datos.
E6	Falla técnica en equipos servidores.	Falla de suministro eléctrico, falla en las conexiones a internet, virus, etc.
E7	Falla técnica en Sistema de Información crítico.	Falta de conocimiento y experticia, error humano, etc.
E8	Ausencia de personal de la UDT	Ausencia de personal por pandemia, enfermedad, accidente, etc.
E9	Calentamiento del centro de datos	Falta de sistema de refrigeración de aire.
E10	Falla técnica en equipos de comunicación.	Falla de suministro eléctrico, obsolescencia tecnológica, falta de procesos, cableado de red no estructurado, etc.
E11	Falla técnica en equipos de estación de trabajo.	Falla de suministro eléctrico, obsolescencia tecnológica, falta de procesos, error humano, falta de conocimiento y experticia, etc.
E12	Ataque informático	Delito informático

7.2.3. Evaluación del Nivel de Riesgo

El análisis de riesgo es un proceso formal por el cual la organización toma conciencia de cuáles son sus activos de información, de cuál es el valor de la perdida de uno de sus atributos (confidencialidad, integridad o disponibilidad) de cómo estos activos son vulnerables.

		PROBABILIDAD				
		Raro	Poco probable	Posible	Muy probable	Casi seguro
CONSECUENCIAS	Despreciables	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy Alto
	Catastróficas	Medio	Alto	Alto	Muy Alto	Muy Alto

Mapa de Calor de Riesgo (Fuente: Gestión de riesgos ISO 31000)

Para la valoración de los eventos identificados, se categorizan los niveles de probabilidad y niveles de severidad. La descripción de cada categoría se muestra a continuación:

Niveles de probabilidad.

- **Casi seguro:** probabilidad muy alta
- **Muy probable:** probabilidad alta
- **Posible:** probabilidad media
- **Poco probable:** probabilidad baja
- **Raro:** seria especialmente raro que ocurriera

Niveles de impacto.

Se identifican los servicios y sistemas de tecnología de información que son utilizados para apoyar la misión, visión, objetivos y metas de la institución.

- **Critica:** Afecta la operación y a las instalaciones, este no es recuperable en corto tiempo y puede suceder porque no existen normas preventivas o bien porque estas no son suficientes. También puede suceder por ocurrir algún tipo de desastre natural como un terremoto. (Catastrófica)
- **Grave:** Es la que causa daños a las instalaciones, pero puedan reiniciar las operaciones en menos de 24 horas. (Mayor)

- **Moderado:** El daño se revierte en un tiempo menor a 8 horas. (Moderado)
- **Menor:** Es la que tiene repercusiones solo en la operación diaria y se puede revertir inmediatamente después de lo ocurrido. (Menor)

Cálculo de Nivel de Riesgo

La determinación del impacto, probabilidad y del evento de contingencia se realizarán según lo establecido en la Política de Seguridad de la información de Municipalidad de Villa El Salvador. Y se Calcula considerando el mayor Nivel de Riesgo del Recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz.

			Impacto			
			Menor	Moderado	Grave	Critica
			(1)	(2)	(3)	(4)
Probabilidad	Casi Seguro	(5)	Alto	Muy Alto	Muy Alto	Muy Alto
	Muy Probable	(4)	Alto	Alto	Muy Alto	Muy Alto
	Posible	(3)	Medio	Alto	Muy Alto	Muy Alto
	Poco Probable	(2)	Bajo	Medio	Alto	Muy Alto
	Raro	(1)	Bajo	Medio	Alto	Alto

Nivel de Probabilidad Estimada	Interpretación
Muy Alto	Probabilidad de ocurrencia alta (Evaluación de prioridad alta)
Alto	Probabilidad de ocurrencia intermedia (Evaluación de prioridad baja
Medio	Probabilidad de ocurrencia muy baja (Evaluación sin prioridad)
Bajo	No se cree que ocurra (Desestimar evaluación)

La valoración de riesgos tiene 4 posibles resultados: bajo, medio, alto y muy algo. En función a ello, los eventos de contingencia precedente tienen la siguiente valoración:

Nº	EVENTO	PROBABILIDAD	SEVERIDAD	VALORACION DE RIESGO
E1	Caída de energía eléctrica	Posible	Critica	ALTO
E2	Caída de Internet y telefonía	Poco probable	Moderado	MEDIO
E3	Infección masiva por software malicioso	Raro	Grave	MEDIO
E4	Suspensión de las actividades por desastres naturales o accidentales	Poco probable	Critica	ALTO
E5	Accesos no autorizados al Centro de Datos del MUNIVES	Raro	Critica	MEDIO
E6	Falla técnica en equipos servidores.	Raro	Grave	MEDIO
E7	Falla técnica en Sistema de Información critico	Raro	Critica	MEDIO
E8	Escaso o Ausencia de personal de la Unidad de Desarrollo Tecnológico	posible	Moderado	MEDIO
E9	Calentamiento del centro de datos	Raro	Critica	MEDIO
E10	Falla técnica en equipos de comunicación.	Muy Probable	Moderado	MEDIO
E11	Falla técnica en equipos de computo	Posible	Grave	ALTO
E12	Ataque informático	Raro	Menor	BAJO

7.2.4. Escenario de Riesgos

A continuación, se presenta el consolidado de los escenarios de riesgo.

TIPO		EVENTO	ESCENARIO
EXTERNO	TECNOLOGICO	**Caída de energía electica. (E1)**	Corresponde al corte del servicio de energía eléctrica desde la misma planta de servicios eléctricos, otras averías externas y la falta de mantenimiento pozo a tierra y la infraestructura eléctrica de la municipalidad por sobrevoltajes encantados, generando así, interrupción al funcionamiento a los servidores, caídas de servicios informáticos y perdidas de comunicación en los equipos de infraestructura tecnológica.
		Infección masiva por software malicioso. (E3)	Es el riesgo de infección de los equipos de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de las unidades de trabajo.
		Ataque informático. (E12)	Consiste en aprovechar alguna debilidad en el software o hardware, para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización.
	OPERATIVO	**Suspensión de funciones por desastres naturales o accidentales. (E4)**	Referencia al riesgo que pueda ocurrir en la entidad, causado por desastres naturales o por la negligencia del hombre afectando a la Unidad de Desarrollo Tecnológico (UDT), generando a la destrucción total o parcial del funcionamiento del Centro de Datos o la prestación de servicios de TI
	TECNICO	**Caída de Internet y telefonía. (E2)**	Consiste en las fallas técnicas por parte del proveedor del servicio de internet y/o telefonía en el Palacio Municipal de Villa El Salvador, lo que ocasionaría suspensión de los servicios de TI incluyendo correo, red, sistemas y aplicativos de información de MUNIVES.

INTERNO	TECNOLOGICO	**Falla técnica en equipos servidores. (E6)**	Corresponde al daño físico o lógico de un equipo servidor, que afecta el funcionamiento de un sistema de información crítico por falta de mantenimiento predictivo, preventivo y correctivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o Inestable.
		Falla técnica en equipos de comunicación. (E10)	Corresponde al daño físico o lógico de un equipo de comunicación, que afecta el funcionamiento de los servicios de información crítico por falta de mantenimiento predictivo, preventivo y correctivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o Inestable.
		Falla técnica en equipos de cómputo. (E11)	Corresponde al daño físico o lógico de una estación de trabajo, que afecta a las actividades de los usuarios de la entidad, por falta de mantenimiento predictivo, preventivo y correctivo a los equipos de cómputo o por mal uso por parte del usuario.
		Falla técnica en Sistema de Información crítico. (E7)	Representa una falla técnica en alguna funcionalidad de los sistemas de información y aplicativos críticos de la entidad que se vea afectada la integridad de la información.
	OPERATIVO	**Accesos no autorizados al Centro de Datos del MUNIVES. (E5)**	Consiste en el acceso al Centro de Datos de personal no autorizadas que pueden ocasionar sabotaje, robo, alteración o extracción de información que es considerada confidencial o clasificada, así como también el daño a los componentes informáticos. El impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional.

TECNICO		**Escaso o Ausencia de personal de la Unidad de Desarrollo Tecnológico. (E8)**	Referencia a la falta de trabajador en un momento crítico generando inoperatividad o inestabilidad en los servicios de TI.
		Calentamiento del centro de datos. (E9)	Consiste en el aumento de temperatura dentro del centro de datos y falta de ventilación, por falta de mantenimiento preventivo del sistema de ventilación acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos

7.3. Fase 3: Estrategias de Plan de Contingencia y Documentación de Procesos.

Desarrollamos las estrategias relacionadas con cada evento o incidente que provoque alto impacto en la continuidad de los servicios TI de la UDT. Para lo cual se está dividiendo en 3 partes:

a. **Prevención:** Mecanismos para prevenir dichos eventos antes de que sucedan; ayudan a reducir el impacto y estar siempre preparados ante eventualidades de desastres.

b. **Ejecución:** Después de iniciado el evento y ayuda a la recuperación de las funciones críticas, se considera los tiempos de continuidad.

c. **Recuperación:** Procedimiento para retomar las actividades ya recuperadas en su lugar de origen.

7.3.1. E1: Caída o falla de Energía Eléctrica.

- **Plan de Prevención**
  - Descripción del evento: Falla general del suministro de energía eléctrica por parte del proveedor de servicios, fallo y/o indisponibilidad del grupo electrógeno por falta de mantenimiento por proveedor o personal especializado. Este evento incluye los siguientes elementos identificados, los mismos que pueden ser considerados como causa de la contingencia:
    - Servicios Público
    - Grupo Electrógeno
    - Hardware
    - Servidores
    - Estaciones de Trabajo
    - UPS

- Equipos Diversos
  - Valoración: Alto
  - Entorno: Se delimita al Centro de Datos ubicado en la sede Central de la Municipalidad de Villa El Salvador.
  - Personal encargado: Oficial de Seguridad de la Información o quien haga sus veces y Especialista en la administración del Data Center, redes y comunicaciones o quien haga sus veces.
  - Condiciones de Prevención:
    - Verificar que durante las operaciones diarias de servicios o actividades de MUNIVES se contara con los servicios de UPS necesarios para asegurar el suministro electrónico en el Centro de Datos de MUNIVES.
    - Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 40 minutos como mínimo.
    - Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del MUNIVES (puertas, contactos magnéticos, etc.)
    - Verificación de cableado eléctrico de todas las sedes del Ministerio de Ambiente, una a dos veces por año.
    - Coordinar el mantenimiento preventivo de pozo a tierra, aire acondicionado del Centro d Datos, UPS, transformador bimestralmente.
    - Verificar que la red eléctrica utilizada en el Centro de Datos y la red de cómputo de la sede principal sea estabilizada. En caso que no existan se debe gestionar la implementación de lo requerido con el área respectiva.

- **Plan de Ejecución**
  - Eventos que activan la Contingencia: Corte de suministro de energía en el Palacio Municipal por un tiempo mayor a 10 minutos.
  - Personal que autoriza la Contingencia: El/la Jefe/Jefa de la Unidad de Desarrollo Tecnológico
  - Personal encargado: Especialista en administración de Data Center, redes y comunicaciones.
  - Procedimientos después de activar la contingencia:
    - Informar a el jefe/la jefa de la Unidad de Abastecimiento del evento presentado.
    - Verificar la activación automática de los UPS.
    - Comunicar a todas la Unidades Orgánicas de MUNIVES del evento y coordinar las acciones necesarias.
    - En caso la interrupción de energía sea mayor a 20 prender a grupo electrógeno.
    - Si persiste la caída de energía eléctrica mayor a 90 minutos se deberá apagar los servidores (Virtuales y físicos) que alojen los sistemas, aplicaciones, servicios de TI y demás servidores en siguiente orden:

- Servidores de aplicación, Base de Datos, servicios Ti, otros, servicios de Directorio Activo y finalmente los servidores físicos.
- Apagar los servicios los equipos de seguridad perimetral y comunicaciones.

- Monitorear el uso de equipos UPS para el restablecimiento de energía en los servidores de soporte a los sistemas críticos.

- **Plan de Recuperación**
  - Personal operativo encargado:
    - Especialista de administración del Centro de Datos, redes y comunicaciones o quien haga sus veces.
    - Personal de desarrollo de sistemas.
  - Descripción de actividades:
    - Verificar el estado de la infraestructura tecnológica impactada por el evento.
    - Verificar el restablecimiento de la energía eléctrica y el funcionamiento del Centro de Datos.
    - En caso de que se cuente con energía eléctrica, se procederá la activación de los servicios en la siguiente secuencia:
      - Encendido de los equipos de seguridad perimetral y comunicaciones.
      - Encendido de los servidores físicos.
      - Encender servidores de Directorio Activo, Base de Datos, Aplicaciones, otros.
    - Analizar la necesidad de usar las copias de respaldo.
    - Verificar el restablecimiento de los sistemas críticos de información.
    - Comunicar a las Unidades Orgánicas afectadas el restablecimiento de los sistemas de información críticos.
    - Comunicar a todas la Unidades Orgánicas de MUNIVES a fin de constatar el correcto funcionamiento de los sistemas de información.
    - Revisar y evaluar el sistema eléctrico de la Municipalidad, por parte de la Unidad de Abastecimiento y proponer una inmediata solución.
    - Elaborar un informe a la Jefatura de la Unidad de Desarrollo Tecnológico de la información sobre el problema presentado y el procedimiento ejecutado para atender el evento.
    - Registrar aquellos procedimientos usados para para actualizar el Plan de Contingencia de TI en caso vuelva a presentar.
  - Desactivación del Plan de Contingencia de TI: El jefe/La jefa de la Unidad de Desarrollo Tecnológico desactivara el Plan de Contingencia una vez se haya reestablecido la energía eléctrica del Centro de Datos y los servicios de TI.
  - Informe de resultados.
  - Proceso de actualización del Plan.
  - Tiempo de Recuperación: Tiempo máximo de duración de la contingencia dependerá

del proveedor externo de energía eléctrica. Para el restablecimiento de la operación del grupo electrógeno se estima un tiempo máximo de 20 minutos.

7.3.2. E2 : Caída de Internet y Telefonía.

- **Plan de Prevención**
  - Descripción del evento: Perdida de servicio de Internet a la conexión de la red externa del servicio principal de MUNIVES.
  - Valoración: Alto
  - Entorno: Se puede producir durante el servicio, o en horario no laborable en el Centro de Datos de MUNIVES.
  - Personal encargado: Especialista en Administración del Data Center, Redes y Comunicaciones o quien sus veces y el Oficial de seguridad de la información o quien sus veces.
  - Condiciones de Prevención de Riesgo:
    - Contar con equipos de comunicación y respaldo ante posibles fallas del router principal, a través del contrato con el proveedor del servicio de internet se contempla el reemplazo de router en caso falle.
    - Contar con mantenimiento preventivo para los equipos de comunicaciones dos veces al año (Equipo alquilado) y otro mantenimiento programado por el proveedor en su nodo de comunicaciones.
    - Contar con ficha de proveedor, donde se detalle la empresa contratista, contacto del técnico (nombres, celular, correo), función del cargo (Servicio de Hosting, Mantenimiento, Internet, etc.), vigencia del contrato (fecha de inicio y finalización) y estado del contrato.

- **Plan de Ejecución**
  - Eventos que activan la Contingencia:
    - Falla del sistema de router principal para el servicio de internet
    - Falla de los circuitos digitales de comunicación de red externa
    - Falla de red telefónica. (anexos)
    - Falla del nodo de comunicación del proveedor de internet.
  - Personal que autoriza la Contingencia: El Jefe/La Jefa de la Unidad de Desarrollo Tecnológico de MUNIVES.
  - Personal encargado: Especialista en Redes y Telecomunicaciones o quien haga sus veces.
  - Procedimientos después de activar la contingencia
    - Verificar la magnitud de fallo o avería al sistema de comunicación a la red externa (Internet).
    - Notificar al proveedor de Servicios de Internet sobre la magnitud de fallos o avería.
    - El proveedor toma control para descartar si es un problema interno. Si es falla del router el proveedor procede con el cambio. (Max. 1 hora)

- En caso de que la falla sea el circuito de comunicaciones, el proveedor se encarga de solucionar el problema de acuerdos a los SLAs comprometidos.
- El proveedor notifica la solución con un informe de la incidencia presentada.
- Validar que los servicios se encuentren en línea a través de la herramienta de Monitoreo.

- **Plan de Recuperación**
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces y Especialista en Administración de Redes y Comunicaciones o quien haga sus veces.
  - Descripción de actividades
    - Validar que los servicios estén conforme por las áreas usuarias.
    - El proveedor del servicio de internet una vez reparado el fallo emitirá un informe a la jefatura de Tecnología de la Información, detallando la causa origen del evento y las acciones realizadas.
    - El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
    - Se informará a la Jefatura de la Unidad de Desarrollo Tecnológico sobre el evento de contingencia presentado y el procedimiento usado.
    - Actualizar el Plan de Contingencia con las acciones correctivas utilizadas.
    - En caso sea falla de Router: El reemplazo por el proveedor no excede a 1 hora
    - En caso de Circuito Digital: El tiempo SLA establecido con el proveedor es de 4 hora.
  - Desactivación del Plan de Contingencia: La Jefatura de la Unidad de Desarrollo Tecnológico desactivara el Plan de Contingencia una vez que se recupere los servicios.

7.3.3. E3 : Infección masiva por software malicioso.

- **Plan de Prevención**
  - Descripción del evento: Los softwares maliciosos son programas informáticos que se propagan de un equipo a otro y que interfieren en su correcto funcionamiento. Además, pueden dañar o eliminar los datos de un equipo. Este evento incluye los siguientes mínimos identificados por el Municipalidad, los mimos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:
    - Servidores
    - Estación de trabajo (PC y Laptops)
    - Software base de datos
    - Aplicativos y sistemas de información de MUNIVES.
  - Valoración: Medio
  - Entorno: Los activos informáticos (PC, Laptops, servidores y sistemas de información) de la Sede de la Municipalidad de Villa El Salvador.

- Personal encargado: Oficial de seguridad de la información o quien haga sus veces, Administrador de Data Center, Redes y Comunicaciones o quien sus veces y Soporte Técnico o quien sus veces.
- Condiciones de prevención de riesgos
  - Establecer políticas de seguridad que regulen el uso correcto de los activos de información.
  - Optar por mecanismos de seguridad que prohíba el acceso a páginas de internet de contenido malicioso
  - Verificar que el antivirus instalado en cada estación de trabajo deba estar actualizado permanentemente.
  - Supervisar la red constantemente a fin de identificar instalaciones de agentes maliciosos.
  - Tener en cuenta con un mínimo de dos equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta la operatividad de equipo cliente afectado.
  - Capacitar y concientizar al personal de MUNIVES sobre temas de seguridad de información.
  - Segmentar la red para aislar los casos activos infectados por Malware malicioso.

- **Plan de Ejecución**
  - Eventos que activan la Contingencia
    - Mensaje de alerta durante la ejecución de los sistemas de información y aplicaciones.
    - Lentitud o paralización de los sistemas de información y aplicaciones.
    - Falla general en los activos de informáticos (PC, Laptops, servidores y sistemas de información)
    - Reporte de usuarios.
  - Personal de autoriza la Contingencia: jefe de la Unidad de Desarrollo Tecnológico
  - Personal encargado: Especialista en administración de Data Center, Redes y Comunicaciones o quien haga sus veces y Soporte Técnico.
  - Descripción de actividades:
    - Comunicar al Jefe o Jefa de UDT para activar al equipo de respuesta de incidentes.
    - Desconectar preventivamente los equipos infectados a la red de MUNIVES
    - Comunicar a los usuarios de los servicios de los equipos impactados.
    - Verificar la infección de los equipos afectados y el alcance de este.
    - Indagar de ser necesario el origen de la infección.
    - En caso de no solucionarse el problema: Formatear el equipo y Personalizar la estación para el usuario.
    - Conectar las estaciones o equipo servidor a la red de MUNIVES.
    - Efectuar las pruebas necesarias con el usuario.

- **Plan de Recuperación**
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces, Especialista en Administrador de Data Center, Redes y Comunicaciones o quien haga sus veces.
  - Descripción de actividades
    - Ejecutar la conformidad del usuario una vez se haya eliminado la amenaza de virus en su estación de trabajo.
    - Ejecutar pruebas de funcionamiento en las estaciones de trabajo.
    - Dar indicaciones de seguridad y prevención a los usuarios.
    - Reportar a la Jefatura de la UDT el tipo de software malicioso encontrado y el procedimiento usado para removerlo.
    - Comprobar que el antivirus funcione correctamente y se encuentra en constante actualización.
    - Revisar que el Sistema Operativo se encuentre con las actualizaciones y parches.
    - Restaurar la información a partir de los Backus almacenados.

  - Desactivación del plan de continuidad: La jefa o jefe de la Oficina de Tecnología de la información desactivara el presente Plan.
  - Tiempo de Recuperación: La duración del evento dependerá de la eficacia en detección de infección masiva. Los usuarios deberán esperar las indicaciones del personal de soporte para reanudar el trabajo.

7.3.4. E4 : Suspensión de las actividades por desastres naturales o accidentales.

- **Plan de Prevención**
  - Descripción de evento: Constituye la situación en la que el Centro de Datos del MUNIVES se encuentra declarada, inhabitable, producto de un desastre de mayores magnitudes, pudiendo provocar derrumbe de la infraestructura, perdida de materiales, recursos informáticos y humanos. Las causas que pueden provocar este evento encontramos las siguientes:
    - Incendio: Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga en manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.
    - Sismo de gran intensidad en Lima: Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento errático del terreno.
    - Inundación: Flujo descontrolado de agua producto de lluvias torrenciales o fugas y/o daños en el sistema hidráulico.

- Valoración: Medio
- Entorno: Se localiza en las instalaciones del Centro de Datos de la sede principal de MUNIVES.
- Personal encargado: Oficial de seguridad de la información o quien haga sus veces, Especialista en Administración de la Data Center, Redes y Comunicaciones o quien haga sus veces, Especialista de Desarrollo y Mantenimiento de Sistemas de Información o quien sus veces.
- Condiciones de prevención de riesgos
  - Incendio de grandes magnitudes en uno o más ambientes:
    - La Unidad de Abastecimiento encargado de brindar a las Unidades usuarias un extintor de gas carbónico, con mantenimiento o reposición de la misma.
    - Llevar a cabo las inspecciones de seguridad periódicamente.
    - Conservar las conexiones eléctricas seguras en el rango de su vida útil.
    - Acatar las indicaciones de Defensa Civil.
    - Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias. Proveedores y personal responsable de las acciones de prevención y ejecución de la contingencia.
    - Verificar el funcionamiento de los detectores de humo en el Centro de Datos del MUNIVES.
    - Identificar la ubicación de las estaciones manuales de alarma contra incendio.
    - Implementar un programa anual de Capacitación para el manejo de extintores al personal de la Municipalidad.
    - Revisar y evaluar el sistema eléctrico de la Municipalidad, por parte de la Unidad de Abastecimiento.
    - Implementar un Sistema de Alarma y contra incendio en el Centro de Datos.

  - Sismo de gran intensidad en Lima
    - Solicitar el plan de evacuación de las instalaciones del MUNIVES, el mismo que debe ser de conocimiento de todo el personal de labora.
    - Participar en los simulacros de evaluación con la participación de todo el personal del MUNIVES.
    - Mantener las salidas libres de obstáculos del Centro de Datos.
    - Señalizar todas las salidas del Centro de Datos.
    - Señalizar las zonas seguras del Centro de Datos.
    - Ubicar adecuadamente el mobiliario informático, teniendo en cuenta las recomendaciones de Defensa Civil.
    - Una Infraestructura adecuada y antisísmica, con gabinetes fijados al piso a la pared en el Centro de Datos.
    - Contar con una lista de contactos de las personas responsables y proveedores de servicios de contingencia.

- Inundaciones de grandes magnitudes
  - Solicitar a Servicios Generales la coordinación del mantenimiento y/o estado de las instalaciones hidráulicas del MUNIVES.
  - Posicionar los activos estratégicos del Centro de Datos en plataforma elevadas.
  - Contar con una lista de contactos de las personas responsables y proveedores de servicios de contingencia.

- **Plan de Ejecución**
  - Personal de autoriza la Contingencia: La Jefatura de la Unidad de Desarrollo Tecnológico con la autorización de la Dirección ejecutiva del MUNIVES.
  - Personal encargado: Especialista en administración de Data Center, redes y comunicaciones o quien haga sus veces y personal de desarrollo de sistemas.
  - Procedimiento para la restauración del Centro de Costo.
    - Utilizar el extintor a una distancia de 2 a 3 metros del fuego, ya que la sustancia alcanza una acción de 3 a 5 metros al momento de usarlo.
    - Determinar los daños ocasionados en el Data Center.
    - Corroborar la disponibilidad de espacio físico que hará las veces de Centro de Datos alterno provisional del MUNIVES, en caso de inoperatividad del Centro de Datos.
    - Mover el equipamiento que se encuentre en buenas condiciones del Centro de Datos, asegurando que las características ambientales sean las mínimas necesarias para su implementación.
    - Salvaguardar las condiciones eléctricas y de refrigeración mínimas para el funcionamiento del Centro de Datos alterno provisional.
    - Configurar la infraestructura tecnológica que soporte el levantamiento de los sistemas de información críticos de MUNIVES.
    - Proceder a recuperar la información a partir de los backup que se encuentran almacenados
    - Ejecutar las pruebas necesarias para asegurar la disponibilidad de los servicios críticos de TI.
    - Informar a la Jefatura de la Unidad de Desarrollo Tecnológico el restablecimiento del Centro de Datos alterno provisional del MUNIVES.

- **Plan de Recuperación**
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces, Especialista en administración de Data Center, redes y comunicaciones o quien haga sus veces, Especialistas en Desarrollo y Mantenimiento de Sistema de la Información o quien haga sus veces.
  - Procedimiento de actividades
    - Verificar los daños a los componentes informáticos del Centro de Datos principal.

- Realizar el inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado.
- Trasladar hacia el Centro de Datos alterno provisional los componentes informáticos en buen estado.
- Habilitar los muebles y logística necesaria para su operatividad.
- Garantizar la habilitación de servicios de fluido eléctrico.
- Reinstalación del personal critico de TI.
- Monitorear constantemente la funcionalidad de los servicios critico de TI.
- Realizar convenios con empresas del medio para que nos alquilen equipos de cómputo en caso de emergencia.
- Proceder a realizar la recarga del extintor y volver a colocar en su respectiva ubicación.
- Después de activar el sistema de alarma y contraincendios, contactar al proveedor para su mantenimiento respectivo.
- Actualización de Plan Contingencia en base al informe presentado a la Dirección Ejecutiva, con las acciones correctivas utilizadas.

- Desactivación del Plan de Recuperación: Se desactivará una vez se tome por superado el desastre y se retome las actividades de origen.
- Tiempo de Recuperación: El proceso de implementar un Centro de Datos provisional (de ser necesario) tomara un tiempo no mayor de 7 días. La duración total del evento dependerá del grado del sismo, la probabilidad de replicas y los daños a la infraestructura.

7.3.5. E5 : Accesos no autorizados al Centro de Datos del MUNIVES.

- **Plan de Prevención**
  - Descripción del evento: Ingreso de personal no autorizado al Centro de Datos, sin previa coordinación o registro de ingreso, poniendo en riesgo la estabilidad física y lógica de los equipos y dispositivos informáticos instalados, provocando inestabilidad en la integridad de la información en los sistemas de información.
  - Entorno: Acceso al Centro de Datos.
  - Personal encargado: Especialista en administración de Centro de Datos, redes y comunicación o quien haga sus veces y el Oficial de seguridad de la información o quien haga sus veces.
  - Condiciones de Prevención de Riesgo
    - Mantenimiento preventivo del sistema Biométrico instalado para seguridad de acceso del Centro de Datos.
    - Registrar los ingresos del personal en Centro de Datos en bitácora.
    - Informar a la Jefatura de la Unidad de Desarrollo Tecnológico los motivos del acceso al Centro de Datos.
    - Si alguna unidad usuaria necesita ingresar o acceder al centro de datos, solicitar mediante un documento a la Unidad, explicando los motivos del acceso.

- Inventariar los equipos informáticos dentro del centro de datos.

- **Plan de Ejecución**
  - Eventos que activan la contingencia: Falla en el Sistema Biométrico de acceso, encontrar la puerta de acceso del Data Center sin supervisión del personal de la Unidad encargada.
  - Personal encargado: El especialista de Administrador de Centro de Datos, redes y comunicaciones o quien haga sus veces.
  - Procedimientos después de activar la Contingencia:
    - Inventariar los equipos informáticos dentro del Data Center.
    - Validar el funcionamiento correcto del sistema de información instalados en los servidores.
    - Validar el correcto funcionamiento de la unidad compartida de información con las áreas correspondientes.
    - Contactar al proveedor para soporte correctivo del Sistema Biométrico.
    - Revisar las cámaras de vigilancia instaladas dentro y fuera del Data Center.
    - Verificar el cuaderno de bitácora el ingreso del personal al Centro de Datos.
    - Validar si solicito acceso al Data Center mediante un memorando autorizando el ingreso.

- **Plan de Recuperación**
  - Personal encargado: El oficial de seguridad de la información o quien haga sus veces, Especialista en Administración de Data Center, redes y comunicaciones o quien haga sus veces, Especialista de Desarrollo y Mantenimiento de Sistema de Información o quien haga sus veces.
  - Procedimiento de actividades:
    - Se informará a la jefatura de la Unidad de Desarrollo Tecnológico la causa del problema suscitado y el procedimiento usado para asistir el problema.
    - El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.
    - Realizar un informe técnico detallado y consolidando las acciones tomadas.
  - Tiempo de Recuperación: aproximadamente 3 horas

7.3.6. E6 : Falla técnica en Equipos de Servidores.

- **Plan de Prevención**
  - Descripción del evento: Falla técnica de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del MUNIVES.
  - Entorno: Centro de Datos, están los servidores de soporte para los servicios críticos de TI, sistemas de información y aplicaciones localizadas en el Centro de Datos del MUNIVES.
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces, Especialista en administración de Data Center, redes y comunicaciones o quien haga

sus veces, Coordinador de Sistema SIGA y SIAF o quien haga sus veces, Especialista de Desarrollo y Mantenimiento de Sistema de la Información o quien haga sus veces.

- Condiciones de Prevención de Riesgo:
  - Revisión periódica a los servidores del Centro de Datos
  - Mantener actualizada la garantía de equipos informáticos y servidores vigentes.
  - Copias de Seguridad de los sistemas de información y programas del MUNIVES.
  - Monitoreo periódico de red del MUNIVES.
  - Adecuada ventilación y refrigeración en el Centro de Datos.
  - Procedimientos para el uso correcto de los activos de información.
  - Copias de respaldo o Backup y custodia en una locación externa.
  - Contar con las copias de respaldo de información disponible para su aplicación en los servidores de contingencia del MUNIVES.
  - Mantenimiento periódico a pozos de puesta a tierra.

- **Plan de Ejecución**
  - Eventos que activan la Contingencia: Fallas en la conexión, servidores no responden. Indisponibilidad de uso de los sistemas y aplicativos del MUNIVES.
  - Personal encargado: Especialista en administración de Data Center, redes y comunicaciones o quien haga sus veces, Personal de desarrollo de sistemas.
  - Procedimientos después de activar la contingencia
    - Analizar la causa resultante o disponer del evento.
    - Realizar un diagnóstico rápido de los sistemas críticos afectados o involucrados en la ejecución. Para este caso se debe revisar el inventario de los sistemas o aplicaciones críticas del MUNIVES.
    - Contactar a las partes interesadas que sean afectadas por la indisponibilidad de los servidores de TI.
    - Comunicar a los proveedores del equipo servidor e informar la incidencia como parte de soporte y garantía.
    - Desconectar de la red el servidor afectado.
    - Activar y configurar el equipo necesario de contingencia para el levantamiento de los servicios de TI en los servidores alternos de contingencia.
    - Ejecutar las restauraciones de los backups de los sistemas y aplicaciones críticos en los servidores alternos de contingencia en caso se requiera.
    - Realizar las pruebas de funcionamiento
    - Comunicar a los usuarios el restablecimiento de los servicios de TI.

- **Plan de Recuperación**
  - Personal encargado; El oficial de seguridad de la información o quien haga sus veces, Especialista en Administración de Data Center, redes y comunicaciones o quien haga sus veces, Especialista de Desarrollo y Mantenimiento de Sistema de Información o quien haga sus veces.

  - Procedimiento de actividades.
    - Conectar a la red el equipo inicial reparado,
    - El especialista de Administrador de Centro de Datos, redes y comunicaciones o quien haga sus veces, verifica el correcto desempeño de los servidores reparados y de los sistemas de información críticos que sostienen.
    - Se informará a la jefatura de la Unidad de Desarrollo Tecnológico la causa del problema suscitado y el procedimiento usado para asistir el problema.
    - El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.
    - Realizar un informe técnico detallado y consolidando las acciones tomadas.
    - Revisar las configuraciones y programar con el proveedor de los equipos, revisiones periódicas a fin de reducir la amenaza.
    - Actualización de Plan Contingencia en base al informe presentado a la Dirección Ejecutiva, con las acciones correctivas utilizadas.
  - Desactivación del Plan de Contingencia: El Jefe o Jefa de la Unida de Desarrollo Tecnológico desactivara el Plan de Contingencia, luego que el especialista de en administración de Data Center, redes y comunicaciones o quien haga sus veces comunique la operatividad de los servidores.
  - Tiempo de Recuperación: Duración: 5 a 8 horas.

7.3.7. E7 : Falla técnica en Sistema de Información Critico.

- **Plan de Prevención**
  - Descripción del evento: El uso inadecuado de los sistemas de información críticos de la MuniVES, corresponde a un elevado riesgo en la integridad de la información.
  - Entorno: Sistema de Información y aplicativos críticos del MuniVES.
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces, Coordinador de Sistema SIGA y SIAF o quien haga sus veces, y Especialista en Desarrollo y Mantenimiento de Sistema de la Información o quien haga sus veces.
  - Condiciones de Prevención de Riesgo.
    - Contar un inventario actualizado de Sistema de Información y programas con los que dispone la Municipalidad de Villa El Salvador.
    - Copia de Seguridad de la información crítica actualizada para salvaguardar la integridad de la información. Del mismo modo obtener las copias de seguridad de la base de datos relacionadas.
    - Mantener actualizado el software de gestión de BD, con todos los parches del

producto según el fabricante y licencias vigentes.
- Eludir el uso de software no licenciado.
- Elaborar Directivas o procedimientos de desarrollo fiable.
- Elaborar y preservar un archivo donde almacene el código fuente de todos los sistemas de información crítica.

- **Plan de Ejecución**
  - Eventos que activan la Contingencia: Fallas en el uso de los sistemas de información que generan su inoperatividad
  - Personal encargado: Coordinador del Sistema SIGA y SIAF o quien haga sus veces y el personal de mantenimiento y desarrollo de sistemas.
  - Procedimientos después de activar la contingencia
    - Desconectar de la red el equipo afectado
    - Asignar y configurar un equipo de respaldo para el sistema de información crítica afectada.
    - Configurar que cada carpeta compartida solicite permisos de acceso
    - Constatar en el servidor el nuevo dominio y colocarlo en producción.
    - Configurar cada en estación de trabajo de las áreas competentes el nuevo dominio.

- **Plan de Recuperación**
  - Personal encargado: Oficial de Seguridad de la Información o quien haga sus veces, Especialista del Centro de Datos, Redes y Comunicaciones o quien haga sus veces, Coordinador de Sistema SIGA y SIAF o quien haga sus veces y el Personal encargado de Desarrollo y Mantenimiento de Sistema de Información o quien haga sus veces.
  - Procedimiento de actividades.
    - Evaluar el sistema de información dañado para determinar la falla o error lógico suscitado.
    - Ejecutar pruebas al sistema de información seguidamente de la solución otorgada por el proveedor.
    - Efectuar copias de seguridad a la base de datos del sistema de información que está funcionando como contingencia.
    - Validar los permisos de acceso sobre el sistema de información.
    - Comunicar a los usuarios la nueva ruta asignada al servidor del sistema de información.
    - Conectar a la red el equipo inicial reparado.
    - Actualización de Plan Contingencia en base al informe presentado a la Dirección Ejecutiva, con las acciones correctivas utilizadas.
  - Tiempo de Recuperación: El tiempo máximo establecido en 24 horas dependiendo de la causa que origino la contingencia.

7.3.8. E8 : Escaso de personal de la Unidad de Desarrollo Tecnológico

- **Plan de Prevención**
  - Descripción del evento: Ausencia de personal (enfermedad, epidemias, renuncias masivas, ceses), que brinda soporte y mantenimiento a los sistemas de información y a la infraestructura tecnológica que mediante su ausencia ocasionaría paralización en las operaciones del MuniVES.
  - Personal encargado: Jefe o Jefa de la Unidad de Desarrollo Tecnológico y el Oficial de seguridad de la información o quien haga sus veces.
  - Condición de Prevención de Riesgo
    - Entrenar a todo el personal de UDT, en el proceso de recuperación de servicios de TI. La Capacitación debe ser planificada, estructurada y acorde a las exigencias de recuperación.
    - Procurar la adecuada capacitación al personal de soporte técnico en su especialidad, Analista de Sistemas, Redes, Infraestructura, Seguridad Informática y Mantenimiento de Sistemas de la información con la finalidad de reemplazar la ausencia de los especialistas.
    - Establecer como unida de sus funciones del personal, informar la inasistencia con anticipación.
    - Elaborar diccionario de datos y/o manuales de procedimientos operativos para contribuir con las actividades del personal suplente.
    - Programar chequeos preventivos médicos al personal en periodos semestrales o anuales por par de la MuniVES.

- **Plan de Ejecución**
  - Eventos que activan la Contingencia: La inasistencia no premeditada del personal crítico. (Encargado de redes y sistema de la información)
  - Personal encargado: Jefe o Jefa de la Unidad de Desarrollo Tecnológico y el Oficial de seguridad de la información o quien haga sus veces.
  - Descripción de las Actividades
    - Comprobada la inasistencia del personal, la Jefatura de la Unidad de Desarrollo Tecnológico asignara al personal indicado como reemplazo temporal.
    - Otorgar los recursos necesarios para que el personal suplente lleve a cabo sus actividades objetivamente.

- **Plan de Recuperación**
  - Personal encargado: Jefe o Jefa de la Unidad de Desarrollo Tecnológico.
  - Procedimiento de actividades:
    - Agilizar la contratación de personal ausente
    - Derivar los servicios pendientes durante la ausencia
    - Verificar los servicios atendidos si es necesario.
    - Derivar informes de desempeño laboral cuando sea requerido por la Jefatura

de la Unidad de Desarrollo Tecnológico.

- Tiempo de Recuperación: Se dispondrá de un reemplazo temporal en un plazo de 24 horas.

7.3.9. E9 : Calentamiento del centro de datos

- **Plan de Prevención**
  - Descripción del evento : Aumento de temperatura dentro del Centro de Datos y falla del sistema de aire acondicionado, en el centro de datos
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces y Especialista en administración de Data Center, redes y comunicaciones o quien haga sus veces.
  - Condiciones de Prevención de Riesgo
    - Disponer de equipos de soporte ante posibles fallas de los servidores.
    - Disponer con un sistema aire acondicionado apropiado para el Centro de Datos.
    - Disponer con mantenimiento preventivo para los equipos de aire acondicionado.
    - Disponer de números de contacto del proveedor al alcance.

- **Plan de Ejecución**
  - Eventos que activan la Contingencia: Falla del sistema de aire acondicionado del Centro de Datos y Falla de los servicios críticos de la MuniVES.
  - Personal encargado: Especialista en administración del Centro de Datos, comunicaciones y redes o quien haga sus veces.
  - Procedimientos después de activar la contingencia
    - Constatar la dimensión del fallo en el sistema de ventilación del Centro de Datos
    - Comunicar al proveedor de aire acondicionado sobre la dimensión del fallo.
    - Conectar el aire acondicionado de contingencia
    - Instalar equipos electrónicos no críticos
    - Apgar los equipos electrónicos no críticos
    - Reestablecer el sistema de aire acondicionado del Centro de Datos.

- **Plan de Recuperación**
  - Personal encargado: Especialista en administración de Centro de Datos, redes y comunicaciones o quien haga sus veces.
  - Descripción de actividades
    - El especialista de administración del Centro de Datos, redes y comunicaciones o quien haga sus veces, examinara que el sistema de Aire Acondicionado funcione con normalidad.
    - El proveedor del sistema de aire acondicionado una vez reparada el fallo emitirá un informe a la Jefatura de Unidad de Desarrollo Tecnológico

- El acontecimiento será avaluado y registrado , de ser necesario
- Tiempo de Recuperación: Tiempo máximo estimado 3 horas.

7.3.10. E10 : Falla Técnica en Equipos de Comunicación.

- **Plan de Prevención**
  - Descripción del evento: Caída de los equipos de comunicación (Switches) o fallas en los enlaces de fibra en la sede central.
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces y el Especialista del Centro de Datos, redes y comunicaciones o quien haga sus veces.
  - Condiciones de Prevención y Riesgo
    - Disponer con equipo de Switches de respaldo antes posibles fallas de los equipos de comunicación para las áreas.
    - Solicitar al proveedor realizar mantenimiento preventivo para los equipos de comunicación (Switch Core y Distribución) para el Centro de Datos.
    - Realizar mantenimiento preventivo a los switches instalados en las unidades orgánicas.

- **Plan de Ejecución**
  - Evento que activan la Contingencia: Falla de Switchs Core, Distribución y acceso a las PC's, y falla de los enlaces de cobre o fibra de red interna.
  - Personal encargado: Especialista del Centro de Datos, redes y comunicaciones o quien haga sus veces.
  - Procedimientos luego de activar la contingencia.
  - Verificación física de la caída de red y evaluar el grado de impacto (usuario y unidades afectadas)
    - Si se trata de un Switch proporcionado por el proveedor, comunicar y solicitar validación, de ser necesario pedir cambio de equipo de comunicación.
    - En caso de ser un Switchs de acceso se reemplaza en caso de garantía, caso contrario se envía a reparación el equipo de comunicación que presenta fallas.
    - Alguna falla o corte de fibra óptica, notificar al proveedor.
    - Se valida el estado de los servicios por usuarios y unidades orgánicas afectadas.

- **Plan de Recuperación**
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces y Especialista administrador en administración de Centro de Datos, redes y comunicaciones o quien haga sus veces.
  - Actividades a ejecutar
    - Validar los equipos de comunicación y enlace de la red interna estén activos para las áreas usuarias.
    - El proveedor de los equipos de comunicaciones una vez reparado el fallo

emitirá un informe a la Subgerencia de la Unidad de Desarrollo Tecnológico, detallando el origen del evento y las acciones realizar.
- Informar a la Jefatura de la Unidad de Desarrollo Tecnológico sobre el evento de contingencia presentado y el procedimiento usado.
- La UDT deberá asegurarse que las pruebas y revisiones periódicas al sistema de comunicaciones de la red internas se lleven a cabo semestralmente.

- Tiempo de recuperación: Falla de switches core y distribución, el tiempo subestimado por el proveedor es de 3 horas. Swiths de acceso PC's máximo 1 hora. En caso de fallas en enlaces digital dependerá de los SLAs del proveedor se estima máximo 48 horas.

7.3.11. E11 : Falla Técnica en Equipos de Cómputo.

- **Plan de Prevención**
  - Descripción: Compete al daño físico o lógico de un equipo computo.
  - Personal encargado: Oficial de seguridad de la información o quien haga sus veces y Especialista en administración de Data Center, redes y comunicaciones o quien haga sus veces.
  - Condiciones de Prevención
    - El inventario de los equipos informáticos y demás bienes está a cargo de la Unidad de Patrimonio.
    - El inventario de solo equipos informáticos también lo gestiona la Unidad de Desarrollo Tecnológico, para identificar la situación funcional de los equipos informáticos.
    - Disponer de una Ficha Técnica por cada Equipo de Cómputo donde detalle, aparte de las especificaciones técnicas, la descripción de los sistemas de información instalados en dicho equipo de cómputo.
    - Identificar e informar los equipos informáticos obsoletos, para renovación de equipos
    - Mantenimiento preventivo anual para los equipos informáticos.

- **Plan de Ejecución**
  - Evento que activa la contingencia: Deficiencia de los equipos informático que soportan los usuarios.
  - Personal encargado: Especialista de Soporte Técnico de UDT.
  - Procedimiento luego de activar la contingencia.
    - Dependerá de la incidencia reportada, se realiza una verificación al equipo asignado para su diagnóstico y solución.
    - Verificar el reporte del inventario elaborado por la Unidad de Desarrollo Tecnológico si cuenta con stock de equipos informático.
    - Configurar el equipo de cómputo asignados como reemplazo para el usuario como estado de préstamo.

10. CONCLUSIONES

- El presente Plan de Contingencia Informático de la Municipalidad Distrital de Villa El Salvador, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red, Sistemas de Información y base de datos, extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.
- Las principales actividades requeridas para la implementación del Plan de Contingencia Informático son: Identificación de riesgos, evaluación de riesgos, asignación de prioridades a las aplicaciones, establecimiento de los requerimientos de recuperación, elaboración de la documentación, verificación e implementación del plan, distribución y mantenimiento del plan.
- Un Plan de Contingencia Informático es la herramienta que la institución debe tener, para desarrollarla habilidad y los medios de sobrevivir y mantener sus operaciones, en caso de que un evento fuera de su alcance le pudiera ocasionar una interrupción parcial o total en sus funciones.
- Las políticas con respecto a la recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.
- No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos más conocido como Centro de Cómputo.
- Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

11. RECOMENDACIONES

- Programar las actividades propuestas en el presente Plan de Contingencias.
- Hacer de conocimiento general el contenido del presente Plan de Contingencias, con la finalidad de instruir adecuadamente al personal de la Municipalidad Distrital Villa El Salvador.
- Adicionalmente al plan de contingencias se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.
- Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la Institución.