VILLA EL SALVADOR
MUNICIPALIDAD
CENTRAL TELEFÓNICA 319-2530
TELEFAX 287-1071
www.mivves.gob.pe

RESOLUCIÓN DE ALCALDIA N° 0123 -2017-ALC/MVES

Villa el Salvador, 07 ABR 2017

EL ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR

VISTO: El Memorando N°403-2017-GM/MVES y Memorando N°1204-2016-GM/MVES de la Gerencia Municipal, el Informe N°021-2017-OGA/MVES, Memorando N°259-2017-OGA/MVES, Memorando N°678-2016-OGA/MVES, Informe N°076-2016-OGA/MVES, Memorando N°407-2016-OGA/MVES y Memorando N°867-2015-OGA/MVES de la Oficina General de Administración, el Informe N°037-2017-UDT-OGA/MVES, Informe N°090-2016-UDT-OGA/MVES e Informe N°539-2015-UDTE-OGA/MVES de la Unidad de Desarrollo Tecnológico, el Informe N°320-2016–OAJ/MVES de la Oficina de Asesoría Jurídica, Memorando N°268-2016-OPP/MVES de la Oficina de Planeamiento y Presupuesto, y;

CONSIDERANDO:

Que, el Art. 194° de la Constitución Política del Perú, concordado con el Art II del Título Preliminar de la Ley Orgánica de Municipalidades N° 27972, señala que los gobiernos locales gozan de autonomía política, económica.y administrativa en los asuntos de su competencia; autonomía que radica en la facultad de ejercer actos de gobiernos, administrativos y de administración, con sujeción al ordenamiento jurídico;

Que, de acuerdo a lo dispuesto por el Decreto Legislativo N°604, el Instituto Nacional de Estadística e Informática - INEI, es el organismo central y rector de los Sistemas Nacionales de Estadística e Informática, responsable de normar, supervisar y evaluar los métodos, procedimientos y técnicas estadísticas e informáticas utilizados por los órganos del Sistema;

Que, mediante Resolución Jefatural N°076-95-INEI se aprueba las Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública mediante Directiva N°007-95-INEI-SJI, cuyo objetivo es "Asegurar que sólo personal autorizado tenga acceso a la información clasificada como restringida o reservada, así como, evitar la reproducción de la información sin la debida autorización y garantizar la integridad de la información";

Que; con Resolución Jefatural N°340-94-INEI se aprueba la Directiva N°015-94-INEI/SJI sobre "Normas Técnicas para el Almacenamiento y Respaldo de la Información que se procesa en las Entidades del Estado, teniendo como finalidad "*Definir los Procedimientos a ser observados por los trabajadores que utilizan equipos de cómputo en las Entidades del Estado, para el adecuado manejo y control del almacenamiento y respaldo de* la información que se registra en medios magnéticos u ópticos";

Que, el Plan de Contingencia Informático es un instrumento de gestión que define los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres, permitiendo disminuir o minimizar los daños, víctimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos;

Que, el numeral 4.1 del artículo 4° de la Ley N°28551, Ley que establece la obligación de elaborar y presentar planes de contingencia, señala que "*La elaboración del plan de contingencia se formula siguiendo la guía que para estos efectos propone el Instituto Nacional de Defensa Civil - INDECI, previa opinión favorable de los sectores correspondientes (...)*", asimismo, el numeral 4.2 señala que "*Las guías a las que se refiere el presente artículo señalan los contenidos mínimos que deben presentar los planes de contingencia*"

Que, mediante Informe N°539-2015-UDTE-OGA/MVES de fecha 02.10.2015 la Unidad de Desarrollo Tecnológico, remite los actuados a la Oficina General de Administración, a fin de que se emita opinión técnica, en mérito a ello, se presentan observaciones en dicho proyecto, por lo que, mediante Informe N°090-2016-UDT-OGA/MVES, la Unidad de Desarrollo Tecnológico remite el proyecto del Plan de Contingencia Informático, luego de haber levantado las observaciones efectuadas por la Oficina de Planeamiento y Presupuesto planteados mediante Memorando N°268-2016-OPP/MVES de fecha 13.05.2016, elevándose a la Alta Dirección;

Que, la Oficina de Asesoría Jurídica, a través del Informe N°320-2016-OAJ-MVES de fecha 22.08.2016 Opina que resulta viable la aprobación del Plan de Contingencia Informático de la Municipalidad Distrital de Villa El Salvador; en ese sentido, con Memorando N°403-2017–GM/MVES, la Gerencia Municipal, remite lo actuado a la Oficina de Secretaría General a fin de que se proyecte la Resolución de Alcaldía correspondiente;

VILLA EL SALVADOR
MUNICIPALIDAD
CENTRAL TELEFÓNICA 319-2530
TELEFAX: 287-1071
www.munives.gob.pe

RESOLUCIÓN DE ALCALDIA N° 0123 -2017-ALC/MVES

Villa el Salvador, 07 ABR 2017

Estando a lo expuesto y en uso de las facultades conferidas por el numeral 6) del Artículo 20°, así como el Artículo 43° de la Ley Orgánica de Municipalidades N° 27972;

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR el Plan de Contingencia Informático (PCI) de la Municipalidad Distrital de Villa El Salvador, que en Anexo forma parte integrante de la presente Resolución de Alcaldía.

ARTICULO SEGUNDO.- CONFORMAR el "Comité del Plan de Contingencia Informático (CPCI) de la Municipalidad Distrital de Villa El Salvador", el cual estará integrado según se indica:

ROL EN EL "CPCI"	CARGO ACTUAL
Presidente del "CPCI"	Gerente Municipal
Coordinador General	Subgerente de UDT
Coordinador de Redes y Comunicaciones	Administrador de Red
Coordinador de Soporte Técnico	Encargado de Soporte Técnico
Coordinador de Sistemas	Administrador de Base de datos/ Web máster
Personal Clave	Subgerente de Administración Tributaria Subgerente de Tesorería Subgerente de Licencias Subgerente de Unidad de Administración Documentaria y Archivo

ARTÍCULO TERCERO.- CONFORMAR el "Comité de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador", el cual estará integrado según se indica:

AREA	FUCIONARIO ENCARGADO
Gerencia Municipal	Sr. Edgar Jesús Hinojosa Alarcón
Unidad de Desarrollo Tecnológico	Sr. Luis Alberto Álvarez Flores
Oficina General de Administración	Ing. Marina Luz Zanabria Limaco,
Unidad de Abastecimiento	Abog. Eileen Laos Moscoso
Gerente de Planeamiento y Presupuesto	Sr, José Arturo Robles Villafuerte

ARTÍCULO CUARTO.- ENCARGAR a la Gerencia Municipal, a la Oficina General de Administración a través de la Unidad de Desarrollo Tecnológico, a la Oficina de Planeamiento y Presupuesto el fiel cumplimiento y ejecución de la presente Resolución.

ARTÍCULO QUINTO.- ENCARGAR a la la Unidad de Desarrollo Tecnológico, la publicación de la presente Resolución en el Portal Institucional www.munives.gob.pe.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

MUNICIPALIDAD DE VILLA EL SALVADOR
ABOG. LUIS E. SUMARAN SAAVEDRA
SECRETARIO GENERAL

Municipalidad Distrital De Villa El Salvador
GUIDO IÑIGO PERALTA
ALCALDE

PLAN DE CONTINGENCIA INFORMATICO DE LA MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR

30 de Marzo del 2017

UNIDAD DE DESARROLLO TECNOLOGICO

GERENCIA DE ADMINISTRACION

MUNICIPALIDAD DE VILLA EL SALVADOR – MVES
Av. Revolución S/N Sector 2, Grupo 15, Lima – Lima – V.E.S.

INDICE

CAPITULO III: Desarrollo e Implementación del Plan de Contingencia

INTRODUCCIÓN

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

Unidad de Desarrollo Tecnológico en adelante UDT, tiene, entre otros, el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a ello presenta el Plan de Contingencia Informático de la Municipalidad de Villa El Salvador.

En la actualidad, los profesionales y técnicos de la informática tienen como una de sus principales actividades y preocupaciones la seguridad de estos sistemas, que constituyen una base y respaldo a las funciones institucionales realizadas a través de los años, así como en la actualidad facilitan a sobre manera las tareas que se desarrollan en la ejecución de los diferentes procesos administrativos, logísticos, ejecutivos, informativos, sociales de planeamiento y de servicios.

Los responsables del servicio informático están obligados a hacer de conocimiento y explicar con lenguaje entendible a estos directivos las posibles consecuencias que la inseguridad insuficiente o inexistente pueda acarrear; de esa manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse para prevenir los desastres que pueda provocar el colapso de los sistemas.

Objetivos

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos de la UDT, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la UDT.

Alcances

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

Base legal

DL. N° 604, Ley de Organización y Funciones del INEI.
DS. N° 018-91-PMC, Reglamento de Organización y Funciones del INEI.
RJ. N° 340-94-INEI, Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.
RJ. N° 076-95-INEI, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
RJ. N° 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.
Ley orgánica de Municipalidades N° 27972 Artículo 20° inciso 6) del 27-05-2003 (Dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas).
Ordenanza N° 298 del 29 de abril del 2014, que aprueba el Nuevo Reglamento de Organización y Funciones de La Municipalidad de Villa El Salvador.

Definiciones, acrónimos y abreviaturas

a. **Contingencia:** Posibilidad de que suceda una interrupción; incidencia o hecho que se presente de forma imprevista.
b. **Plan de contingencia:** Es un instrumento de gestión para una buena administración de las tecnologías de la información y de las Comunicaciones en el dominio del soporte y desempeño.

c. **Ataque:** Acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, conectividad de una red de computadoras o intento de obtener de modo no autorizado la información confiada a una computadora.

d. **Amenaza:** Evento o acción que pueda interferir con el funcionamiento adecuado de una computadora, red de computadoras o causa la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

e. **Incidente:** Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente como por ejemplo. Las fallas de unos suministros eléctricos o un intento de borrado de un archivo protegido.

f. **Ataque de denegación de servicio:** También llamado ataque DOS, es un ataque a un sistema de computadoras o red que causa que el servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red.

Alcance

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

Meta

Potenciar el nivel informático de la Unidad de Desarrollo Tecnológico (UDT) de la MVES, y además las funciones cotidianas informáticas, haciéndolas seguras y consistentes, logrando con ello su buen desarrollo y la optimización de resultados.

SITUACIÓN ACTUAL

DIAGNOSTICO

Efectuada nuestra revisión de la administración de riesgos de la unidad de desarrollo tecnológico de la Municipalidad de Villa El Salvador consideramos que debe desarrollarse un Plan de Contingencias. Si bien hemos observado la existencia de normas, procedimientos y controles que cubren algunos aspectos de la seguridad de la información, que carece en general de una metodología, guía o marco de trabajo que ayude a la identificación de riesgos y determinación de controles para mitigar los mismos.

Dentro de los distintos aspectos a considerar en la seguridad, es necesario elaborar Políticas de Seguridad de la Información y una Clasificación de Seguridad de los Activos de Información de la Municipalidad. Cabe mencionar que se ha verificado la existencia de controles, en el caso de la seguridad lógica, sobre los accesos a los sistemas de información así como procedimientos técnicos establecidos para el otorgamiento de dichos accesos.

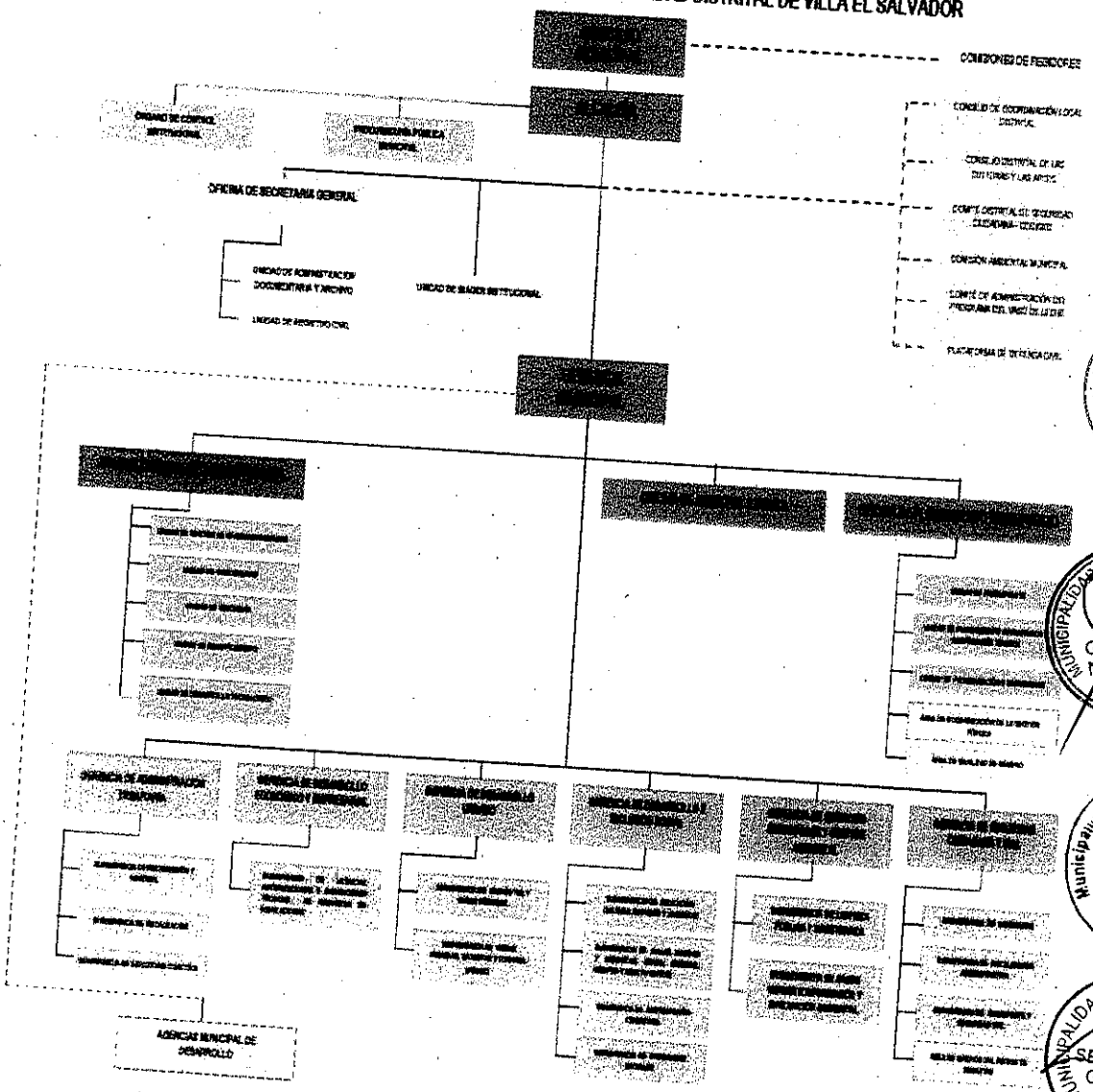
Sin embargo, estos controles no obedecen a una definición previa de una Política de Seguridad ni de una evaluación de riesgos de seguridad de la información a nivel de toda la Municipalidad. Los controles establecidos a la fecha son producto de evaluaciones particulares efectuadas por las áreas involucradas o bajo cuyo ámbito de responsabilidad recae cierto aspecto de la seguridad.

CAPITULO I: Planificación

1.1. ORGANIZACIÓN ESTRUCTURAL

ORGANIGRAMA

ORGANIGRAMA ESTRUCTURAL DE LA MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR



ESTRUCTURA Y FUNCIONES

CONCEJO MUNICIPAL

El Concejo Municipal es el órgano de gobierno de la Municipalidad distrital de Villa El Salvador. Está conformado por el/la Alcalde/sa y sus trece Regidores/as Sus atribuciones son normativas y fiscalizadoras su composición, competencias, organización interna y funcionamiento están normado por la ley orgánica de municipalidades, su respectivo Reglamento Interno de Concejo y otras que se le asignen por ley.

ALCALDIA

La Alcaldía es el órgano ejecutivo del gobierno local. El Alcalde es el representante legal de la Municipalidad, titular del pliego presupuestal y su máxima autoridad administrativa. Ejerce las funciones ejecutivas en la Municipalidad de Villa El Salvador de conformidad con lo dispuesto en la Ley N-27972, Ley Orgánica de Municipalidades, y otras normas conexas complementarias

GERENCIA MUNICIPAL

La Gerencia Municipal es un órgano de alta dirección, depende funcional y jerárquicamente de Alcaldía está a cargo de un/a funcionario/a con categoría de gerente Municipal quienes es designado por el/la Alcalde/sa mediante Resolución de Alcaldía, se encarga de planificar, normar, promocionar ejecutar y controlar el funcionamiento de los sistemas de administrativos y funcionales

ORGANO DE CONTROL INSTITUCIONAL

El órgano de control institucional es un órgano conformante del sistema nacional de control depende funcional y administrativamente de la Contraloría General de la República (CGR). Está a cargo de un/a funcionario/a con categoría de Gerente quien es designado por la Contraloría General de la Republica (CGR). Se encarga de planificar, normar, proporcionar, ejecutar y controlar el funcionamiento del sistema administrativo de Control

OFICINA DE ASESORIA JURIDICA

La Oficina de Asesoría Jurídica es un órgano de asesoramiento depende funcional y jerárquicamente de la Gerencia Municipal está a cargo de un/a Funcionario/a con categoría de Gerente, quien es designado por el/a Alcalde/a mediante resolución de alcaldía. Se encarga de planificar, normar, promocionar, ejecutar y controlar el funcionamiento del sistema administrativo sistema de defensa judicial del estado

OFICINA DE PLANEAMIENTO Y PRESUPUESTO

La Oficina de Planeamiento y Presupuesto es un órgano de asesoramiento, depende funcional y jerárquicamente de la Gerencia Municipal. Está a cargo de un/a funcionario/a con categoría de Gerente quien es designado por el/la Alcalde/sa mediante Resolución de alcaldía se encarga de planificar, normar promocionar, ejecutar y controlar el funcionamiento de los sistemas administrativos de público, planeamiento estratégico, Modernización de la Gestión Pública, y del sistema Funcional del Ministerio de la Mujer y poblaciones vulnerables

OFICINA DE SECRETARIA GENERAL

La Oficina de Secretaria General es un órgano de apoyo, depende Funcional y jerárquicamente de Alcaldía. Está a cargo de un/a Funcionario/a con categoría de Gerente quien es designado por el/la Alcalde/sa mediante resolución de Alcaldía. Se encarga de normar, promocionar, ejecutar y controlar el funcionamiento de los sistemas de trámite documentario y registro civil

OFICINA GENERAL DE ADMINISTRACION

La oficina General de Administración es un órgano de apoyo depende funcional y jerárquicamente de la Gerencia Municipal. Está a cargo de un/a funcionario/a con categoría de Gerente quien es designado por el/la Alcade/sa mediante resolución de Alcaldía. Se encarga de planificar, normar, promocionar y ejecutar el funcionamiento de los sistemas administrativos de Abastecimiento, Contabilidad, gestión de recursos humanos Tesorería y el sistema funcional de informática

UNIDAD DE DESARROLLO TECNOLOGICO

La Unidad de Desarrollo Tecnológico es un órgano de apoyo, depende funcional y jerárquicamente de la Oficina General de Administración está a cargo de un/a funcionario/a con categoría de Subgerente, quien es designado el/la Alcalde/sa mediante Resolución de Alcaldía. Se encarga de planificar, normar, promocionar, ejecutar y controlar el funcionamiento del sistema funcional de Informática

GERENCIA DE ADMINISTRACION TRIBUTARIA

La Gerencia de Administración Tributaria es un órgano de línea, depende Funcional y jerárquicamente de Gerencia Municipal. Está a cargo de un/a Funcionario con categoría de Gerente quien es designado por el/la Alcalde/sa Mediante Resolución de Alcaldía. Se encarga de planificar, normar, promocionar ejecutar y controlar el funcionamiento de los sistemas de tributación

GERENCIA DE DESARROLLO ECONOMICO Y EMPRESARIAL

La Gerencia de Desarrollo Económico y Empresariales es un órgano de línea, depende funcional y jerárquicamente de la Gerencia Municipal está a cargo de un/a funcionario/a con categoría de Gerente quien es designado por el/la Alcalde/sa mediante Resolución de Alcaldía. Se encarga de planificar, normar, promocionar, ejecutar y controlar el funcionamiento del sistema administrativo de producción

GERENCIA DE DESARROLLO URBANO

La Gerencia de Desarrollo Urbano es un órgano de línea, depende funcional y jerárquicamente de la Gerencia Municipal. Está a cargo de un/a funcionario/a con categoría de Gerente, quien es designado por el/la Alcalde/sa mediante Resolución de Alcaldía. Se encarga de planificar, normar, promocionar, ejecutar y controlar el funcionamiento de los Sistema Funcionales de Vivienda y Construcción, y Transporte y Comunicaciones en lo que le corresponde.

GERENCIA DE DESARROLLO E INCLUSION SOCIAL

La Gerencia de Desarrollo e inclusión Social es un órgano de línea, depende funcional y jerárquicamente de la Gerencia Municipal. Está a cargo de un/a funcionario/a con categoría de Gerente, quien es designado por el/la Alcalde/sa mediante Resolución de Alcaldía. Se encarga de planificar, normar, promocionar, ejecutar y controlar el funcionamiento de los Sistemas Funcionales de Desarrollo Social, Cultura, Deporte, Salud y Participación Ciudadana.

GERENCIA DE SERVICIOS MUNICIPALES Y GESTION AMBIENTAL

La Gerencia de Servicios Municipales y Gestión Ambiental es un órgano de línea, depende funcional y jerárquicamente de la Gerencia Municipal. Está a cargo de un/a funcionario/a con categoría de Gerente, quien es designado por el/la Alcalde/sa mediante Resolución de Alcaldía. Se encarga de planificar, normar, promocionar, ejecutar y controlar el funcionamiento del sistema funcional de Gestión Ambiental.

GERENCIA DE SEGURIDAD CIUDADANA Y VIAL

La Gerencia de Seguridad Ciudadana y Vial es un órgano de línea, depende funcional y jerárquicamente de la Gerencia Municipal. Está a cargo de un/a funcionario/a con categoría de Gerente, quien es designado por el/la Alcalde/sa mediante Resolución de Alcaldía. Se encarga de planificar, normar, promocionar, ejecutar y controlar el funcionamiento del sistema funcional de Seguridad Ciudadana y Vial

1.2. SERVICIOS Y/O BIENES PRODUCIDOS

La Municipalidad de Villa El Salvador es una institución que se encarga de brindar servicios a los vecinos de Villa El Salvador como:

1. Promover y realizar la inversión Pública en el ámbito Distrital.
2. Fortalecer la seguridad ciudadana.
3. Promover el desarrollo sostenible y mantener los parques y jardines.
4. Garantizar el control sanitario.
5. Conservar el medio ambiente.
6. Promover el fortalecimiento institucional de las organizaciones sociales de base de la jurisdicción
7. Fomentar la cultura, el deporte y el turismo.
8. La adecuada prestación de servicios públicos locales
9. Mantener la infraestructura vial.
10. Administrar el Registro Civil.

Entre otros, para cumplir con las disposiciones legales vigentes y poder brindar bienestar y desarrollo a la comunidad.

1.3. RECURSOS INSTITUCIONALES

El presente Plan de Contingencias requiere como respaldo contar con algunos requisitos para la puesta en marcha:

1. **Humanos**

Se refiere al personal que participa directa e indirectamente en el desarrollo del Plan, las cuales en un primer momento será el personal de la UDT con que cuenta la MVES, quienes definirán los procedimientos para poner en operación el Plan de Contingencias.
Tenemos luego a los Gerentes que al comprender la importancia y urgencia de la aplicación de este plan habrán de apoyar las propuestas que dan base a la ejecución del plan de contingencias, y han de hacer denominador común para su aplicación. Por último las personas de diferentes Subgerencias, Unidades, responsables de Funciones establecidas en el ROF de la MVES que servirán de nexo para la captura de información y definición de tareas del plan.

2. **Materiales**

Todas las herramientas de soporte, material de escritorio, computadores, equipos, insumos informáticos, útiles de escritorio, necesario para llevar a cabo el plan.

3. **Financieros**

Los recursos financieros con que se requiere contar para la aplicación del presente Plan de Contingencia, en acuerdo con la parte directiva de la UDT serían previstos al año siguiente después de aprobación del Plan de Contingencias de la Municipalidad de Villa El Salvador

4. **Entrenamiento**

El personal participante será entrenado para la aplicación correcta del Plan y para obtener el máximo provecho de acuerdo a la función que han de cumplir como parte conformante del plan.

5. **Responsabilidad**

La alta dirección habrá de ejercer la función de control y asegurará que las tareas desarrolladas, sean cumplidas de acuerdo a los planteamientos y objetivos del plan.

Los Planes de Contingencia se organizan para que las instituciones puedan prevenir fallas o accidentes en sus operaciones diarias y les permitan seguir activas, en la provisión de servicios o productos, en el caso de que algún componente sufra algún tipo de problema, que condicione el correcto

funcionamiento de sus equipos tecnológicos, aplicaciones informáticas y otros sistemas críticos.

1.4. INVENTARIO DE RECURSOS INFORMÁTICOS
(El inventario de hardware será mostrado en el anexo 4)

Software Utilizado.

El software utilizado en la MVES se muestra en el siguiente cuadro:

1. APLICATIVOS INFORMÁTICOS

Sistema	Nombre del Sistema	Descripción	Responsable Funcional
SISTRADOC	Sistema de Gestión de Expedientes	Permite la creación de expedientes y oficios presentados por los ciudadanos, los mismos que son enviadas a áreas determinadas según los asuntos.	Todas las áreas
SIGAVES	Sistema de Gestión Municipal	Administra los procesos requerimientos de órdenes de compra ordenes de servicios de todas las unidades orgánicas de la municipalidad (36)	Gerencia de Administración, S.G. Logística, S.G. Tesorería, G. Planeam. y Presupuesto, S.G. Contabilidad, Almacén
RUOS	Sistema de Registro Único de Organizaciones Sociales	Registra y controla las organizaciones sociales que están debidamente acreditadas con Resolución de Alcaldía	Subgerencia de Participación Vecinal
SIIR	Sistema de Emisión de Recibos	Emite los recibos por conceptos de procedimientos administrativos, referente al TUPA.	Áreas de Atención al Público
SIIR	Sistema Predial	Administra, evalúa y controla la información del contribuyente, del predio y de los tributos.	Gerencias de Rentas y sus Subgerencias
RDDSIIR	Resolución de Determinación de Deuda	Administra y controla la información de las diferencias de las declaraciones de los contribuyentes contra las fiscalizaciones.	Subgerencia de Fiscalización
VALSIIR	Sistema de Valores	Generar y efectúa el seguimiento de los documentos de cobranza que son notificados al contribuyente cuando incurren	Subgerencia de Recaudación, Subgerencia de Control Urbano, Subgerencia de

		en deudas con la Municipalidad.	Comercialización
SIIR	Sistema de Fraccionamiento de Deuda	Fracciona las deudas del pago de predial, arbitrios, multas y resoluciones de determinación de deuda.	Subgerencia de Recaudación
SAGU	Sistema de Control	Registra los exámenes especiales e intervenciones de control que realiza la oficina de control interno.	Oficina de Control Interno
VASO DE LECHE	Sistema del Vaso de Leche	Registra la cantidad de ayuda alimenticia que reciben todas las instituciones del distrito.	Unidad de Programas Sociales
SIAF	Sistema Integrado De Administración Financiera	.	Contabilidad
OMAPED	Sistema de Omaped	Registra la información de las personas con discapacidad del distrito	Unidad de Programas Sociales
TRIBU	Sistema de Licencias	Permite registrar las licencias de bodegas y establecimientos den el distrito	Alcaldía
COLASCLICK	Sistema de Difusión e imagen institucional	Brindar información consolidada y detallada de los procesos que se llevan a cabo en la Municipalidad, que son importantes para la toma de decisiones.	Unidad de imagen institucional
		Registrar las declaraciones juradas que existen en el Archivo Central.	Unidad de Trámite y Archivo
PORTAL WEB	PORTAL WEB	Publicación de la información general de la Municipalidad	Secretaría General, Subgerencia de Obras Públicas, Subgerencia de Recaudación, Imagen Institucional, Subgerencia de Contabilidad, Subgerencia de RRHH, Gerencia de Planeamiento y Presupuesto, Gerencia de Administración, Subgerencia de Logística
		Registra y administra, en forma digital, la información de las inscripciones de las partidas y certificados civiles de los	Unidad de Registros Civiles

		recurrentes y no recurrentes del distrito; así como controla las ceremonias civiles que se llevan a cabo dentro y fuera de la Municipalidad.	

CAPITULO II: Elaboración del Plan de contingencia

2.1. Análisis e identificación de Riesgos Informáticos

2.1.1. Identificación de Riesgos

Establecer los riesgos a los cuales está propensa la UDT, de igual manera determinar el nivel o factor de riesgo, que lo clasificaremos en los siguientes:

Identificación de Factor de Riesgo:

- Bajo
- Muy Bajo
- Alto
- Muy alto
- Medio

Ellos nos determinan nuestra tabla de riesgos y nivel de factores que a continuación detallamos:

RIESGO	Factor de Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Incendio					X
Inundación		x			
Robo Común					X
Vandalismo, daño de equipos y archivos.					X
Fallas en los equipos, daño de archivos.					X
Equivocaciones, daño de archivos.			x		
Virus, daño de equipos y archivo.					X
Terremotos, daño de equipos y archivos.				X	
Acceso no autorizado, filtración de info.					X
Robo de datos					X
Fraude, alteración de información.				X	

Desastre Total					X

En base a la tabla anteriormente presentada, concluimos que nuestro análisis de riesgo a modo general, nos hace ver que las posibles contingencias que pudieran presentarse en su mayoría van de un factor de ocurrencia medio y muy alto.

A continuación realizamos un deslinde de las causas por las cuales mayormente se presentan este tipo de contingencias, para ello realizamos la siguiente lista de preguntas:

1. Con respecto al ***fuego***, que puede destruir los equipos y los archivos

- ¿La Institución cuenta con protección contra incendios?
- ¿Se cuenta con sistemas de aspersión automática?
- ¿Cuenta con diversos extintores?
- ¿Detectores de humo?
- ¿Los empleados están preparados para enfrentar un posible incendio?

2. Con respecto al ***robo común***, llevándose los equipos y archivos

- ¿En qué tipo de vecindario se encuentra la Institución?
- ¿Hay venta de drogas?
- ¿Los equipos de cómputo se ven desde la calle?
- ¿Hay personal de seguridad en la Institución?
- ¿Cuántos vigilantes hay?
- ¿Los vigilantes, están ubicados en zonas estratégicas?
- ¿Existe un sistema de seguridad para prevenir el ingreso de personas no autorizadas?

3. Con respecto al ***vandalismo***, que dañen los equipos y archivos

- ¿Existe la posibilidad que un ladrón cause daños?
- ¿Hay la probabilidad que causen algún otro tipo de daño intencionado?

4. Con respecto a ***fallas en los equipos***, que dañen los archivos

- ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
- ¿Cuáles son las condiciones actuales del hardware?
- ¿Es posible predecir las fallas a que están expuestos los equipos?

5. A ***equivocaciones*** que dañen los archivos

- ¿Cuánto saben los empleados de computadoras o redes?
- Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?

- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

6. Con respecto a la acción de ***virus***, que dañen los archivos

- ¿Se prueba software en la oficina sin hacerle un examen previo?
- ¿Está permitido el uso de disquetes en la oficina?
- ¿Todas las máquinas tienen unidades de disquetes?
- ¿Se cuentan con procedimientos contra los virus?

7. Con respecto a ***terremotos***, que destruyen los equipos y archivos

- ¿La Institución se encuentra en una zona sísmica?
- ¿El edificio cumple con las normas antisísmicas?
- Un terremoto, ¿cuánto daño podría causar?

8. Con respecto a accesos ***no autorizados***, filtrándose datos importantes

- ¿Existe registro de personal autorizado en la Municipalidad?
- ¿Qué probabilidad hay que un colaborador intente hacer un acceso no autorizado?
- ¿Existe comunicación remota de la red? ¿Qué tipo de servicio se utiliza (Telnet, FTP, etc.)?
- ¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?

9. Con respecto al ***robo de datos***; y la posible difusión de estos.

- ¿Cuánto valor tienen actualmente las Bases de Datos?
- ¿Cuánta pérdida podría causar en caso de que se hicieran públicas?
- ¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?

10. Con respecto al ***fraude***, vía computadora.

- ¿Cuántas personas se ocupan de la contabilidad de la Institución?
- ¿Los sistemas son confiables? ¿Pueden copiar datos en archivos?
- Las personas que trabajan en las diferentes áreas, ¿qué tipo de antecedentes laborales tienen?
- ¿Existe acceso a los sistemas desde otros sistemas externos o por personas no autorizadas?

2.1.2. Identificación de bienes susceptibles a daños

a. Equipos Informáticos: Computadoras, impresoras, servidores.
b. Software: Sistemas operativos, sistemas de la MVES, base de datos.
c. Documentos: Manuales, informes.
d. Comunicaciones: Redes LAN, telefonía.

2.2. Impacto de los riesgos informáticos

Las operaciones de la Municipalidad de Villa el Salvador, pueden ser afectadas en menor o mayor medida por los distintos siniestros tanto naturales, accidentales o provocados. Se definen los anteriores eventos para ser considerados dentro de este plan de contingencia informático.

2.2.1. En caso de terremoto

SIN PERDIDA O DAÑOS MENORES DE LAS INSTALACIONES: El siniestro puede afectar únicamente parte de la estructura de las instituciones de la MVES, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de este; el impacto que provocaría en la MVES sería menor, puesto que las actividades se interrumpirían por unas horas o a hasta por un día completo.

CON PÉRDIDA DE LAS INSTALACIONES: La pérdida de las instalaciones afectadas gravemente a las operaciones de la MVES y los datos puede verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuadamente y oportunamente.

Riesgos asociados con el evento de un terremoto:

Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo	
					Total	Residuo
terremoto / Negación de servicio	Centro de computo	El centro de cómputo se encuentra en una región de alta actividad sísmica	Media	Alto	72	72
terremoto / Negación de servicio	Ruteadores, Switch y firewalls	Funcionan con energía eléctrica	Baja	Alto	36	27

2.2.2. En caso de incendio

AREA DE SISTEMAS (SITE DE COMPUTO): Se tiene gran impacto en la información ya que los sistemas utilizados residen en los Servidores y dispositivos de comunicación localizados en el SITE DE COMPUTO y en caso de sufrir algún daño, se requiera adquirir un nuevo equipo, así como de instalar nuevamente el sistema, configurar el servidor y restaurar los respaldos para continuar trabajando.

AREA DISTINTAS AL SITE DE CÓMPUTO: Un incendio dependiendo de su magnitud, puede afectar desde las estaciones de trabajo o periféricos y dispositivos de comunicación localizados en el centro de cómputo. En el caso de las primeras el impacto que tendría en la MVES es menor, puesto que la información o tiempo de operación que se pierde no tiene gran

repercusión en las operaciones generales, ya que puede restablecerse en un tiempo relativamente corto.

Los riesgos asociados con el evento de un incendio:

Pueden ser reinstalados casi de inmediato.

Los riesgos asociados con el evento de fallas de la red de voz y datos:

Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo	
					Total	Residuo
Personal técnico de mantenimiento / negación de servicio	Centro de computo	el cableado dentro del centro de cómputo no se encuentra debidamente ordenado	Media	Alto	54	18
Hacker / cambio en la configuración	Access Point	Cualquier computadora puede conectarse a la red Wireless	Alto	Alto	180	36
Código malicioso / negación de servicio	Windows 2000 server, Linux red hat y window 2000 server	Todos los usuarios del servidor están disponibles desde la red interna	Alta	Alto	180	45
Usuario del sistema/infección de la red	Equipo de Computo	Uso de las unidades USB	Media	Alto	180	38

2.2.2.1. Tipos de extinguidores

Muchas veces el contar con sistemas automáticos anti fuego (sprinklers de agua o sistemas de rociado de gas) no es debido a su alto costo, entonces se debe actuar con rapidez para poder sofocar el incendio. Para ello se debe tener en cuenta del material que se está siendo consumido por el fuego. Para cada tipo de situación hay un agente anti fuego ideal, así tenemos:

	Gas Carbónico (CO2)	Espuma	Agua
Papel, Madera Este tipo de material que deja brasa o ceniza requiere un agente que moje o enfrié	Apaga solamente en la superficie.	Sofoca	Excelente enfría y empapa apaga totalmente
Equipamiento Eléctrico	Excelente, no deja residuos, no daña el equipamiento y no es conductor de electricidad	Conduce la electricidad y además daña el equipo	Conductora de electricidad
Líquidos Inflamables (Aceites,gasolina,grasa,etc.) Requiere acción rápida de sofocar y enfriar	Bueno; no deja residuos y es inofensivo	Excelente, produce una sábana de espuma que sofoca y enfría	

Material	Modo de Operarlos
CO2	1.- Retirar la traba de seguridad 2.- Asegure firmemente el mango difusor. 3.- Apretar el gatillo. 4.- Oriente el chorro hacia la base del fuego haciendo un barrido. **Alcance:** 1 a 2 metros **Sustancia:** Bióxido de carbono. **Momento del Recargo:** Pérdida del más del 10% o más del peso.
Polvo Químico	1.- Abra la ampolla de gas. 2.- Asegure firmemente el mango difusor 3.- Apretar el gatillo 4.- Oriente el chorro de manera de crear una cortina de

	polvo sobre el fuego. Alcance: de 2 a 4 metros. Sustancia: Polvo Químico seco y CO_2 producido por el contacto del polvo con fuego. Momento de Recargo: Pérdida de peso de la ampolla superior al 10%
Espuma	1.- Inversión del aparato para abajo 2.- Oriente el chorro para la base del fuego. Alcance: de 9 a 18 metros Sustancia: Espuma formada por burbujas consistentes llenas de CO_2 Momento del Recargo: Anualmente.
Agua – Gas	Simple maniobra de apertura a la ampolla de CO_2 que sirve de propagador Alcance: de 9 a 20 metros Sustancia: Agua. Momento de recargo: Anualmente.

Instrucciones

Los colaboradores designados para usar extinguidores de fuego deben de ser entrenados en su uso. Ellos deben recibir algunas lecciones de instrucciones en el mecanismo de lucha contra el fuego y luego estar entrenados de cómo opera el extinguidor de mano.

Es muy importante que todos los colaboradores reciban la instrucción de no interferir con este proceso y evitar su actuación en el sistema de extinción.

Muchas veces la sensibilidad de comienzo de fuego en los ambientes laborales es muy alta. Esto genera falsas alarmas y los colaboradores se acostumbrar a fomentar el pánico, sin observar realmente si hay fuego.

Ello implica tener en cuenta algunos detalles más como son:

- Cuidado al seleccionar e implementar los sistemas de extinción y su conexión si es efectuada con fuerza eléctrica.

- Tener a mano el número telefónico de la Compañía de Bomberos y demás números de emergencia.
- Mantener procedimientos planificados para recibir y almacenar abastecimientos de papel.

2.2.3. En caso de inundación

a. Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.

b. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

c. Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.

d. Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

e. Proveer cubiertas protectoras para cuando el equipo esté apagado.

2.2.4. En caso de corte de energía eléctrica

Se puede presentar lo siguiente:

a. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.

b. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia (*), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.

c. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

(*) Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS.

Llámese corriente normal a la brindada por la compañía eléctrica.

Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador).

2.2.5. En caso de fallas en la red de voz y datos

1. Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

a. Caída del servidor de archivos por falla de software de red.

b. Falla en el suministro de energía eléctrica por mal funcionamiento de UPS.

c. Bajar incorrectamente el servidor de archivos.

d. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, cargar el sistema operativo de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz.

De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

2.2.6. En caso de fallas en el hardware y el software

Las alternativas que sufran los servidores tanto en Hardware y software pueden ser corregidas en la mayoría de los casos, sin embargo si las alternativas llegan a ser tan grandes que el tiempo requerido para el inicio de las operaciones normales puede extenderse hasta por días.

Los riesgos asociados con el evento de fallas en hardware o software son:

Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total	Riesgo residual
Personal técnico de mantenimiento / descarga o electroestática	Centro de computo	No se cuenta con piso antiestático	Media	Alto	36	12
Polvo / daño de equipo	Centro de computo	No está definido un periodo para realizar la limpieza del centro de computo	Alta	Alto	81	18
Bugs en el sistema/ negación de servicio	MySQL	No se ha actualizado la versión de la base de datos	Baja	Alto	36	27

2.2.7. En caso de hacking sabotaje o daño accidental

La alteración de la información requiere de la restauración de respaldo y de pruebas posteriores para contar con la integridad de los datos. Es posible que se requieran reproceso de captura de datos, dependiendo de las fechas de los respaldos que se tengan disponibles.

El paro total de las operaciones dentro de la Municipalidad de Villa el Salvador afectaría principalmente a los servicios que son proporcionados a la ciudadanía. Los principales conflictos que pudieran presentarse son:

En cuanto a la red, si el sistema llegara a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendría las operaciones a falta de monitoreo a los distintos sistemas.

Respecto a los dispositivos de almacenamiento, si se mantiene los respaldos únicamente dentro de la Municipalidad sería imposible reanudar las actividades que en un momento dado fuera críticas, como la nómina, contabilidad, etc. En un sitio alterno, ya que no contarían con copia de la información.

A continuación se menciona en forma enunciativa una serie de medidas preventivas en caso de presentarse un paro total de las operaciones.

- Determinar lugares especiales, fuera del centro de datos, para almacenar los respaldos y copia de la documentación de referencia.
- El personal clave del plan de contingencia informático, debe de dar la alerta del paro total y sacar los respaldos de información fuera del edificio dentro de un tiempo límite antes de ser declarada la huelga.
- Personal de la Sub Gerencia de Informática debe prever un sitio alterno para continuar con las operaciones críticas. Asimismo, se tendrá que establecer un tiempo de espera de solución de la huelga como por ejemplo 24 horas con el fin de que no afecte el servicio proporcionado al público en general, si después de este intervalo la huelga continuara, se determinara el lugar o lugares de reubicación alternos.
- Los riesgos asociados con el evento de vandalismo y manifestaciones son:

Amenaza	Activo	Vulnerabilidad	Probabilidad	Impacto	Riesgo total	Riesgo residual
Manifestaciones falla de personal	personal encargado de los sistemas	Ausentarse a laborar	Media	Alto	90	30

2.3.8 CONTINGENCIA SOBRE HOSTING E INTERNET

Afecta el clima a nuestras conexiones a internet, es una pregunta que nos tenemos que hacer, así como también si esto sucediera afectaría también nuestros servicios en línea, y si no fuera así y solamente caería nuestro hosting que contiene nuestro portal web y servicios en línea externos cual sería el tiempo de recuperación de nuestra información. Publicada y por ende cual sería el costo de recuperación.

En algunos puntos desconcentrados de nuestra institución que mantienen radio enlace para la conexión estos deberán estar en dirección vista a veces (lluvia o viento etc) podrían originar un corte en la conexión. Para esto se a previsto tener como contingencia de Brinkster (proveedor de hosting en la cual se publica nuestro portal)

Si este fallara se tiene previsto un Web Hosting adicional que prevea estos eventos es el superdomains donde se mantiene una copia actualizada de los contenidos web publicados a diario de tal manera que si Brinkster dejara de funcionar nuestro hosting de contingencia (superdomains) garantiza la continuidad del servicio

En caso de Internet si fuera el caso que el servicio contratado por nuestra institución se detuviera (AMERICATEL, servicio dedicado, 10 MB) los servicios prioritarios es decir los canales de atención al usuario caja, mesa de partes, las mesas de atención, siaf, finanzas etc se mantendrían conectados a un internet De TELEFONICA (servicio no dedicado) 8 MB

2.3. Medidas preventivas y dispositivos de seguridad frente a desastres naturales

2.3.1. Medidas de seguridad frente a terremotos

En la actualidad la mejor forma de contrarrestar los efectos producidos por terremoto y/o desastres son la programación de simulacros complementando con la debida señalización de las zonas seguras en las áreas adecuadas establecidas por un profesional competente en defensa civil de esta manera se minimizaran los daños considerablemente y el proceso de recuperación será en el menor tiempo posible.

Acciones a realizar antes del terremoto

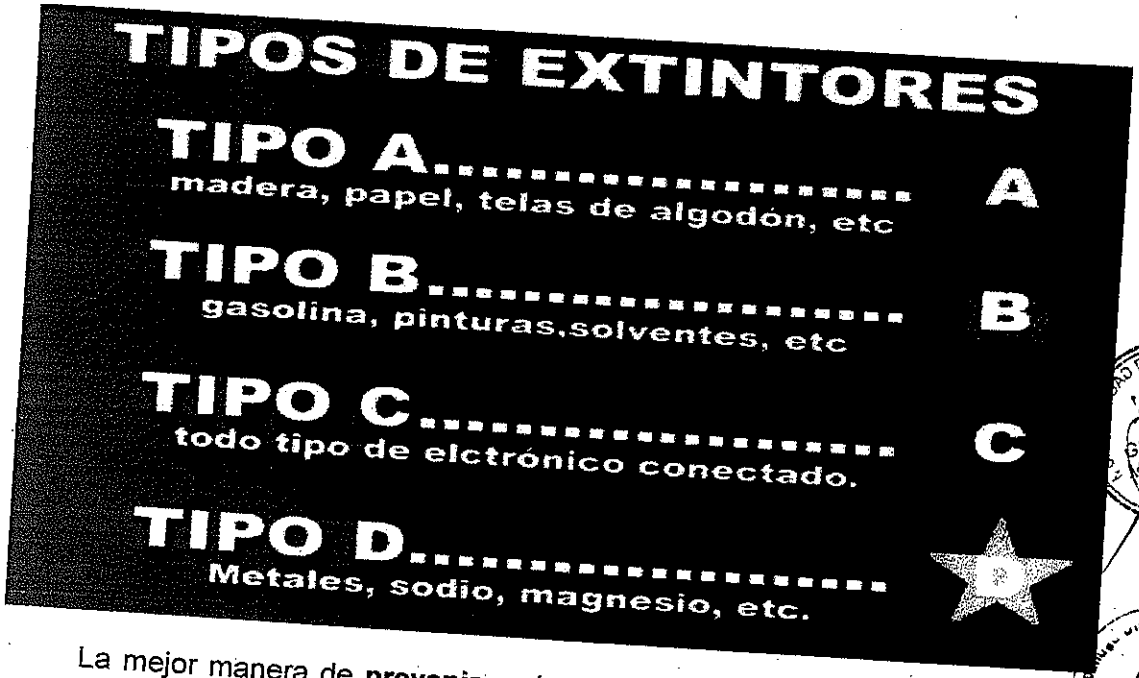
- Identificar los lugares más seguros en los que el personal pueda protegerse.
- Revisar periódicamente y reparara, si es el caso, las instalaciones de electricidad para que siempre se encuentren en buen estado.

2.3.2. Medidas de seguridad frente a incendios

Dentro de los dispositivos que existen en el mercado sobre la detección automática de incendio para centros de cómputo. Se encuentran los siguientes:

- Detector de humo direccionable Ionico.
- Detector de humo direccionable fotoeléctrico.

Conocer los tipos de extintores, para que según sea el caso en el cual suceda el incendio se use correctamente.



La mejor manera de **prevenir** un incendio es no provocarlo. Observe las prohibiciones de no fumar y las normas de prevención propias del local en que se encuentre, y con mayor razón en un centro de cómputo.

<u>En presencia del fuego tenga en cuenta que:</u>

- Puede tratar de apagar un fuego en una oficina siempre que tenga detrás una puerta que le permita salida.
- Si el fuego prende en sus ropas, no corra, tírese al suelo y ruede. Si el hecho ocurre otra persona cúbrala con alguna prenda o con una toalla humedecida, si se encuentra próximo a un aseo. No se quite la ropa si tiene quemaduras.
- En presencia de aparatos eléctricos, no eche agua al fuego. Tampoco debe hacerlo ante líquidos inflamables (alcohol, aceite, gasolina, etc.).
- Si hay mucho humo póngase un pañuelo en la boca y nariz, a ser posible mojado, y salga agachado o gateando. Respire profundamente para evitar desvanecimientos.
- Al salir de una dependencia, procure cerrar las ventanas y las puertas, pues las corrientes avivan el fuego.
- Si se encuentra aislado y no puede ponerse a salvo, diríjase a la habitación más alejada del fuego (pero no a un nivel superior a menos

que esté seguro de que los equipos de rescate se encuentran muy cerca y provistos de escaleras largas u otro equipo.

- Si se ve obligado a huir a través de las llamas para ponerse a salvo, no se entretenga en recoger nada, cúbrase (incluyendo la cabeza) con una manta, una toalla, una cortina o un abrigo mojados si es posible, luego aguante la respiración y corra.
- Si tiene que desalojar el edificio siga las normas de "Evacuación deLa MVES".

Con respecto a los equipo de computo

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en cintas magnéticas.

a. Ante todo, se debe conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, se debe tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

b. En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).

c. Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.

d. Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

2.3.3. Medidas de seguridad frente a inundaciones

a. Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.

b. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

c. Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.

d. Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

e. Proveer cubiertas protectoras para cuando el equipo esté apagado.

2.3.4. Procedimientos de respaldo

PHVA
Planeación: Garantizar la realización de respaldo.
Hacer: Desarrollar cada una de las actividades contempladas en el proceso de Backup. Realizar recuperación de información cuando sea necesario.
Verificación: Registrar en la bitácora de control de Backup's.
Actuar: Hacer seguimiento proceso de Backup`s.

CONTENIDO: Se describe la actividad y se establecen los link con formatos, documentos, instructivos, protocolos, normas, actas.

ACTIVIDAD ESENCIAL	DESCRIPCIÓN.
Proceso de Backup	Descripción de actividades: 1. Determinar o identificar el número de aplicativos y/o bases de datos para respaldo. 2. Determinar los mecanismos de copias de respaldo según la base de datos a respaldar: manual o automático. 3. Verificar si el Backup es automático el sistema asigna fecha de creación de la base de datos, si no se debe cambiar la fecha de creación de la misma. 4. Verificar los archivos log del servidor. 5. Comprimir los archivos en formato .zip o .rar si la copia se realiza correctamente. 6. Verificar las copias comprimidas, para verificar que se pueden descomprimir cuando se necesiten. 7. Volver a realizar copia por segunda vez, si el archivo log del servidor indica un error. 8. Grabar diaria, semanal y anualmente, en un dispositivo de almacenamiento (CD) todas las copias y guardar en la Oficina de Informática. 9. Grabar mensualmente en un dispositivo de almacenamiento (CD) todas las copias se guarda una en la oficina de Informática y se envía otra a un ente externo con sus respectivas bases de datos y fecha de creación. Nota: Las copias de Backup de las Bases de Datos realizadas en el Centro de Cómputo se generan de dos formas: manual y automática ejecutando Scripts de Backup's. Responsable: Coordinador Centro de Cómputo, Profesional Universitario, Analista de Sistema y Técnico. Conocimiento: Aplicaciones y Bases de Datos.

Recursos esenciales: Sistema de información, instructivos y equipos.
Normatividad:
- NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información.
- Frecuencia: Diaria, semanal y/o mensual
- Decretos y normatividad aplicable a la SNR.

RESPECTO A LA ADMINISTRACIÓN DE LOS BACKUPS

a. Se administrará bajo la lógica de un almacén, esto implica ingreso y salida de medios magnéticos (cintas, disquetes, casettes, cartuchos, discos removibles, CD's, etc.) obviamente teniendo más cuidado con las salidas y cuidando que el grado de temperatura y humedad sean los adecuados.

b. Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.

c. El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

d. Para los Backup's sólo se deben utilizar Tape Backup nuevos o en buen estado.

e. El proceso de etiquetado tiene que quedar registrado.

2.3.5. Mantenimiento y limpieza de los dispositivos

PARA EL MANTENIMIENTO DE DISCOS MAGNÉTICOS

a. En general los discos magnéticos son medios de almacenamiento "delicados", pues si sufren un pequeño golpe puede ocasionar que la información se dañe o producir un CRASH al sistema.

b. El cabezal lectura – escritura debe estar lubricado para evitar daños al entrar en contacto con la superficie del disco.

c. Evitar que el equipo sea colocado en una zona donde se acumule calor, ya que el calor puede dilatar algunas piezas más que otras, o secar los lubricantes. Con ello se modifican la alineación entre el disco y los cabezales de lectura-escritura, pudiéndose destruir la información.

d. Las ranuras de los ventiladores de refrigeración deben estar libres.

e. Evitar, en lo posible, la introducción de partículas de polvo que pueden originar serios problemas.

PARA EL MANTENIMIENTO DE LOS DISCOS DUROS

a. Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.

b. El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.

c. Evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.

d. No mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

e. para mantener la velocidad en el equipo, se debe realizar una vez al mes el proceso de desfragmentación para conservar en óptimo estado la respuesta del equipo; Windows incluye un desfragmentado de disco fácilmente localizable en el menú Inicio/Todos los programas/Accesorios/Herramientas del Sistema/Desfragmentado de disco.

CAPITULO III: Desarrollo e Implementación del Plan de Contingencia

3.1. Emergencia Físicas (casos)

3.1.1. Error Físico de Disco de un Servidor (Sin RAID)

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

a. Ubicar el disco malogrado.
b. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
c. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
d. Bajar el sistema y apagar el equipo.
e. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
f. Restaurar el último Backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
g. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
h. Habilitar las entradas al sistema para los usuarios.

3.1.2. Error de Memoria RAM

En este caso se dan los siguientes síntomas:

a. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
b. Ante procesos mayores se congela el proceso.
c. Arroja errores con mapas de direcciones hexadecimales.
d. El servidor deberá contar con ECC (error correctchecking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.
e. Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo
f. inmediatamente.
g. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias malogradas.
- Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Probar los sistemas que están en red en diferentes estaciones.

- Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

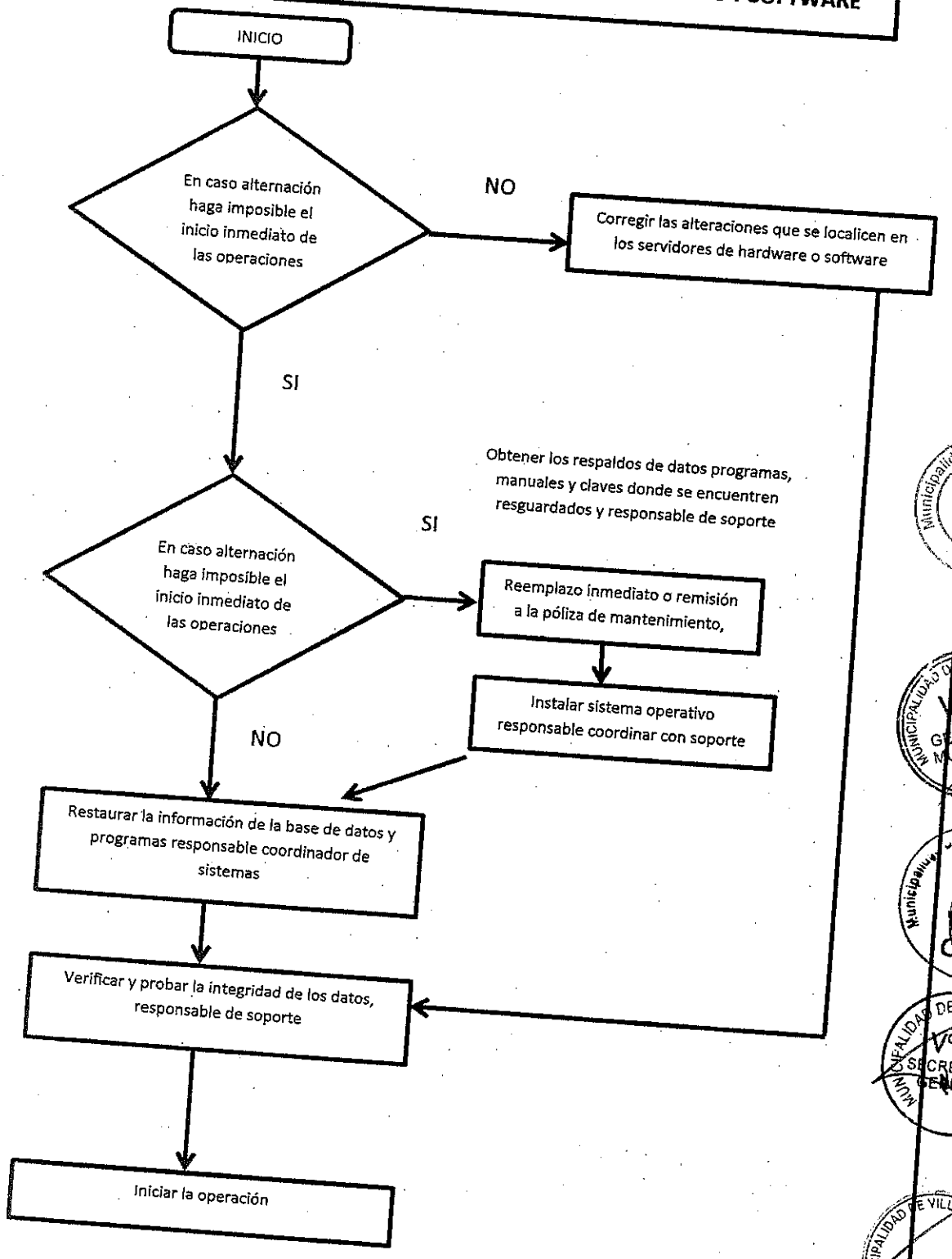
3.1.3. Error de Tarjeta(s) Controladora(s) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

a. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
b. El servidor debe estar apagado, dando un correcto apagado del sistema.
c. Ubicar la posición de la tarjeta controladora.
d. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
e. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
f. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
g. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

Diagrama del procedimiento de respuesta en caso de fallas en hardware y Software

DIAGRAMA PROCEDIMIENTOS DE FALLAS EN HARDWARE Y SOFTWARE



La mejor manera de **prevenir** un incendio es no provocarlo. Observe las prohibiciones de no fumar y las normas de prevención propias del local en que se encuentre, y con mayor razón en un centro de cómputo.

En presencia del fuego tenga en cuenta que:

- Puede tratar de apagar un fuego en una oficina siempre que tenga detrás una puerta que le permita salida.
- Si el fuego prende en sus ropas, no corra, tírese al suelo y ruede. Si el hecho ocurre a otra persona cúbrala con alguna prenda o con una toalla humedecida, si se encuentra próximo a un aseo. No se quite la ropa si tiene quemaduras.
- En presencia de aparatos eléctricos, no eche agua al fuego. Tampoco debe hacerlo ante líquidos inflamables (alcohol, aceite, gasolina, etc.).
- Si hay mucho humo póngase un pañuelo en la boca y nariz, a ser posible mojado, y salga agachado o gateando. Respire profundamente para evitar desvanecimientos.
- Al salir de una dependencia, procure cerrar las ventanas y las puertas, pues las corrientes avivan el fuego.
- Si se encuentra aislado y no puede ponerse a salvo, diríjase a la habitación más alejada del fuego (pero no a un nivel superior a menos que esté seguro de que los equipos de rescate se encuentran muy cerca y provistos de escaleras largas u otro equipo.
- Si se ve obligado a huir a través de las llamas para ponerse a salvo, no se entretenga en recoger nada, cúbrase (incluyendo la cabeza) con una manta, una toalla, una cortina o un abrigo mojados si es posible, luego aguante la respiración y corra.
- Si tiene que desalojar el edificio siga las normas de "Evacuación de La MVES".

Con respecto a los equipo de computo

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en cintas magnéticas.

a. Ante todo, se debe conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, se debe tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.

b. En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).

c. Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.

d. Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

3.1.4. Caso de Inundación.

a. Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.

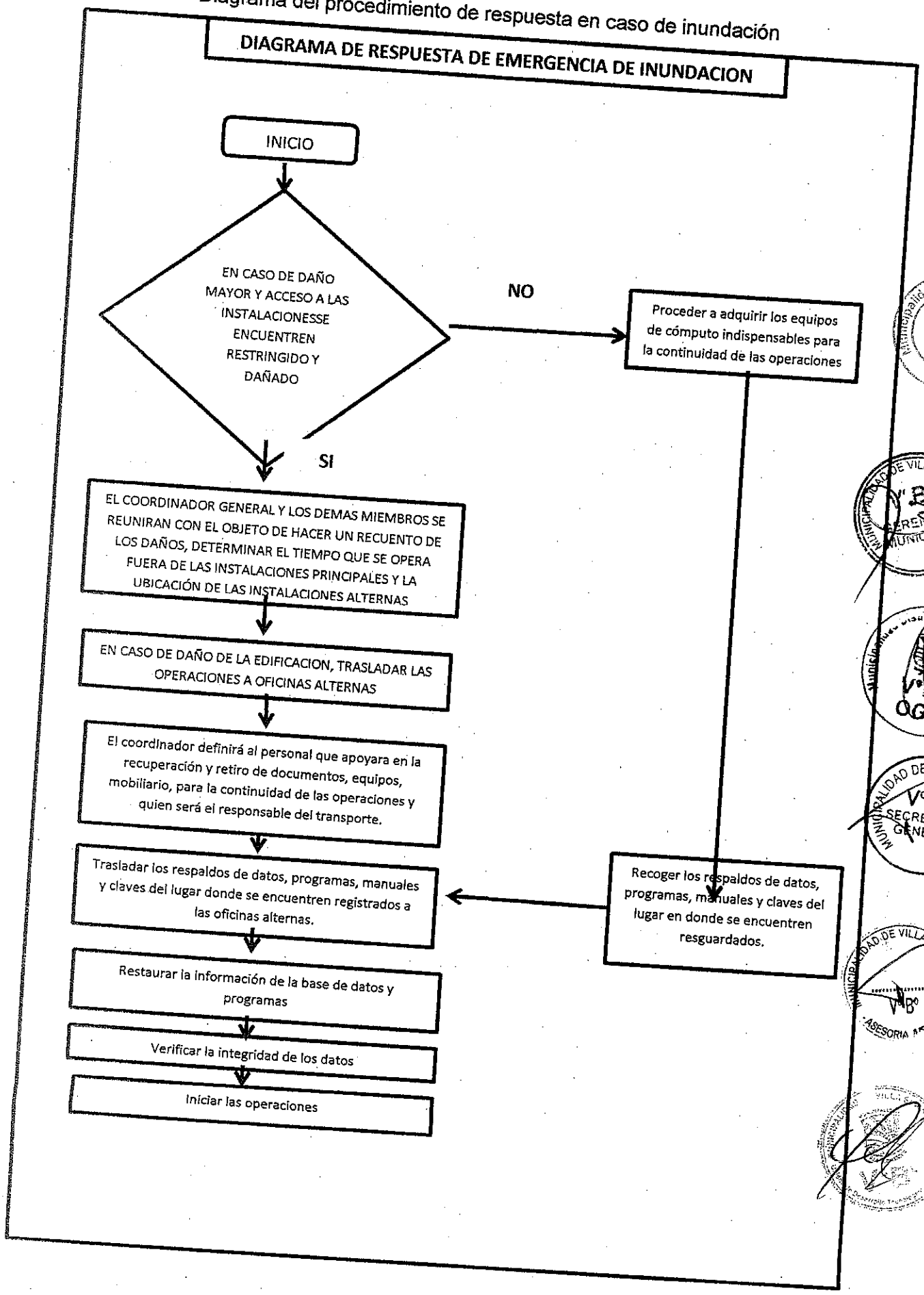
b. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

c. Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.

d. Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

e. Proveer cubiertas protectoras para cuando el equipo esté apagado.

Diagrama del procedimiento de respuesta en caso de inundación



3.1.5. Caso de Fallas de Fluido Eléctrico.

Se puede presentar lo siguiente:

A. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.

B. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia (*)), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.

C. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (

(*) Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS.

Llámese corriente normal a la brindada por la compañía eléctrica.

Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador).

3.2. PLAN DE RECUPERACIÓN DE DESASTRES

En esta parte nos enfocaremos en el tema del desastre en concreto y que acciones debemos tomar con las etapas siguiente (3):

3.2.1. ACTIVIDADES PREVIAS AL DESASTRE

Como actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información que nos asegure un proceso de recuperación con el menor costo posible a nuestra institución, tenemos

que señalar las siguientes acciones que son precisas de realizar en la ejecución del presente plan.

a. Definición y Establecimiento de un Plan de Acción

Establecer los procedimientos relativos a:

(1). Sistemas de Información.- La UDT tendrá una relación de los Sistemas de Información con los que cuenta. Debiendo identificar toda información sistematizada o manual, que sea necesaria para la buena marcha Institucional.

La relación de *Sistemas de Información* detallará los siguientes datos:

- ***Nombre del Sistema***, es determinado por el analista-desarrollador asignado por la UDT.
- ***Lenguaje o Paquete*** con el que fue creado el Sistema, programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- ***La Dirección,*** (Gerencia, Subgerencia, área, etc.) que genera la información base (el <<dueño>> del sistema).
- Las ***unidades o departamentos*** (internos/ externos) que usan la información del Sistema.
- El ***volumen de los archivos*** que trabaja el Sistema.
- El ***volumen de transacciones*** diarias, semanales y mensuales que maneja el sistema.
- El ***equipamiento necesario*** para un manejo óptimo del Sistema.
- La(s) ***fecha***(s) en las que la información es necesitada con carácter de urgencia.
- El ***nivel de importancia*** estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).
- ***Actividades*** a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Con toda esta información se realizará una lista priorizada (Ranking) de los Sistemas de Información necesarios para que la MVES recupere su operatividad perdida en el desastre (Contingencia).

(2). Equipos de Cómputo: Se tendrá en cuenta lo siguiente:

- ***Inventario actualizado*** de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que

usa, principales archivos que contiene), su ubicación y nivel de uso institucional.

- ***Pólizas de Seguros Comerciales***. Como parte de la protección de los activos institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del computador siniestrado se hará por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

- ***Señalización*** o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con información importante o estratégica y color verde a las PC's de contenidos normales.

- **Respaldo de PC´s**, tener siempre una relación actualizada de PC´s requeridas como mínimo para cada sistema permanente de la institución (que por sus funciones constituye el eje central de los servicios informáticos), para cubrir las funciones básicas y prioritarias de cada uno de estos sistemas cuando se requiera.

(3). **Obtención y Almacenamiento de los Respaldos de Información (BACKUPS):** Establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas o aplicativos de la MVES, contando con:

- ***Backups del Sistema Operativo.*** En caso de tener varios sistemas operativos o versiones se contará con una copia de cada uno de ellos.
- ***Backups del Software Base.*** Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales.
- ***Backups del Software Aplicativo.*** Considerando tanto los programas fuentes como los programas objeto correspondiente, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final. Considerando las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- ***Backups de los Datos.*** Base de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del software aplicativo de la MVES ***Backups del Hardware***. Implementar mediante dos modalidades:

Modalidad Externa. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

Modalidad Interna. Teniendo locales en diferente lugar geográfico, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se probará y asegurará que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

(4). Políticas (Normas y Procedimientos de Backups): Establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto 3). Incluyéndose:

- Periodicidad de cada tipo de Backups.
- Respaldo de Información de movimiento entre los períodos que no se cuenta con Backups (backups incrementales).
- Uso obligatorio de un formulario estándar para el registro y control de backups.
- Correspondencia entre la relación de sistemas e informaciones necesarias para la buena marcha de la institución (mencionado en el punto a) y los backups efectuados.

- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

b. **Formación de Equipos Operativos para el Plan de Acción**

Todas las áreas u oficinas de la MVES, que almacenen Información y que sirva para la operatividad institucional, designará un responsable de la seguridad de dicha información. Pudiendo ser el jefe del área o el colaborador que maneje directamente la información.

Entre las acciones a tomar por la UDT conjuntamente con las oficinas serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas, subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, modem, otros aditamentos para comunicaciones.
- Establecer procedimiento de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad de almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

3.2.2. ACTIVIDADES DURANTE EL DESASTRE

3.2.2.1. Determinación de los tiempos de recuperación y especificaciones

3.2.2.1.1. En situaciones criticas

En situaciones críticas cuya afectación inutilice el centro de cómputo y las instalaciones dela sede central de la Municipalidad de Villa el salvador, se establecerá un centro de cómputo alterno de acuerdo a la siguiente tabla.

Orden	Área	Local	Dirección
1	Gerencia Desarrollo Social	Sala de Computo	Av. Los Álamos s/n Sector 3

Tabla de orden de establecimiento de centro de cómputo alterno

El centro de cómputo alterno se deberá establecer en 48 hrs. Como plazo máximo, con el equipo que se muestra a continuación:

Las PC's para los usuarios y para el personal de la Sub Gerencia de informática que opera en las instalaciones alternas deberá contar con las siguiente configuración.

- Windows XP o Superior
- Office 2007 0 Superior
- Antivirus SOPHOS
- Explorador de internet 8.0
- Impresora
- Salida a internet por medio de la red

Fallas de internet.- Cuando se trate de fallas de acceso en internet causados por el proveedor de servicio, se deberá tener comunicación con el ejecutivo de cuenta para realizar el reporte del año y para establecer el tiempo en el que estará sin servicio.

En caso de fallas graves o por un tiempo prolongado se recomienda que para los usuarios operativos y Gerentes que lo requieran, se reconfigurara el servicio mediante un enlace Dial-Up o mediante internet inalámbrica móvil.

3.2.2.2. Sitios alternos y almacenajes off-site

3.2.2.2.1. Sitios alternativos

Dependiendo de la gravedad de la contingencia, se destinaran los siguientes sitios alternos.

Orden	Área	Local	Dirección
1	Gerencia Desarrollo Social	Sala de Computo	Av. Los Álamos s/n Sector 3

En caso de contingencia catastrófica que dejara inhabilitado para funcionar las instalaciones de la Municipalidad de Villa el Salvador, se optara por

instalar el Site de computo alterno provisional en la Gerencia Desarrollo Social en Av. Los Álamos s/n sector 3.

Iniciar las operaciones	Coordinador de sistemas y Coordinador de Redes y Comunicaciones

3.2.3. ACTIVIDADES DESPUÉS DEL DESASTRE

Durante la contingencia, se tomará en cuenta lo planificado en el plan de Emergencia.

a. Evaluación de Daños.

Inmediatamente después que la contingencia ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se lanzará un pre-aviso a la institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha institución.

b. Priorización de actividades del Plan de Acción

Toda vez que el Plan de acción contemple una pérdida total, la evaluación de daños reales y su comparación con el Plan, nos dará la lista de actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para su asignamiento temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

c. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción.

Cada uno de estos equipos contará con un coordinador que reportará diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, informará de inmediato a la jefatura a cargo del Plan de Contingencias (UDT).

Los colaboradores de recuperación tendrán dos etapas:

- **La primera**, la restauración de los servicios usando los recursos de la MVES o local de respaldo.
- **La segunda**, es volver a contar con los recursos en las cantidades y lugares propios de los sistemas de información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro sistema e imagen institucional, como para no perjudicar la operatividad de la MVES o local de respaldo.

d. Evaluación de Resultados.

Una vez concluidas las labores de recuperación del (los) sistema(s) que fueron afectados por la contingencia, se evaluará objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro, saldrán dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

e. Retroalimentación del Plan de Acción.

Con la evaluación de resultados, se optimizará el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

3.2.3.1. Disposiciones Complementarias

3.2.3.1.1 Conformación de los comité del Plan de contingencia informático

COMITÉ DEL PLAN DE CONTINGENCIA INFORMATICO

Rol en el CPCI	Cargo Actual
Presidente del CPCI	Gerente Municipal
Coordinador General	Sub Gerente de Informática
Coordinador de Redes y Comunicaciones	Administrador de Red
Coordinador de Soporte Técnico	Encargado de Soporte Técnico
Coordinador de Sistemas	Administrador de Base de datos/Web máster
Personal Clave	Sub Gerente de Administración Tributaria Sub Gerente de Tesorería Sub Gerente de Licencias Sub Gerente de Tramite Documentario

3.2.3.1.2 Integrantes del Comité del Plan de Contingencia Informático

Los integrantes del comité del plan de contingencia informática (CPCI), son trabajadores de la Municipalidad de Villa el Salvador (MVES) que tienen un Y conformado por miembros de la Unidad de Desarrollo tecnológico (UDT) y el resto por personal clave de las otras gerencias Sub Gerencias de la MVES, los cuales son personas que tienen una trascendencia importante en temas de pro actividad y experiencia en sus respectivas áreas además de tener una aptitud cooperativa frente a casos de emergencia.

El hecho concreto de que CPCI este conformado por personas de diferentes áreas de la MVES es debido principalmente a que las tecnologías de información y comunicación (TICs) se encuentran dispersa e integradas por todas las áreas de la MVES y en caso de la caída de estas TICs el personal de informática requiere apoyo y la cooperación de estas personas claves para restaurar la tecnología e información que usan estas misma manera más rápida y sin complicaciones posteriores. A continuación se muestra la tabla que define formalmente al CPCI.

3.2.3.1.3. Definición de roles de los integrantes del comité del PCI

Presidente del Comité.- Es el responsable de aprobar la realización del Plan de Contingencia Informático, dirigir las comunicaciones de concientización y solicitud de apoyo a los Gerentes de las diferentes áreas involucradas y aprobar su terminación.

Una vez concluida la realización del Plan de Contingencia, el presidente tendrá como función principal, verificar que se realicen reuniones periódicas, cuando menos casa seis meses en donde se informe de los posibles cambios que se deban efectuar al plan original y de que se efectúen pruebas del correo funcionamiento del Plan de Contingencia

Informático, cuando menos dos veces al año o antes si se presentan circunstancias de cambio que así lo ameriten.

Al declararse una contingencia, deberá tomar las decisiones correspondientes a la definición de las ubicaciones para instalar el centro de cómputo alterno y autorizara las inversiones a realizar así como el fondo de efectivo a asignarse para los gastos necesarios iniciales.

El directorio de proveedores de equipos, garantías, servicio de mantenimiento y reparaciones, suministros, refacciones y desarrollo de software, en su caso, e incluirlo dentro del Plan de Contingencia Informático.

En caso de que se declare alguna contingencia que afecte a los equipos y al software, sea cual fuera su grado de afectación, es el responsable de establecer el servicio a la brevedad, con el objeto de que no se agrave el daño o se llegara a tener consecuencias mayores.

Por tal efecto debe participar en pruebas del Plan de Contingencia en conjunto con los demás miembros del comité, con el objeto de estar permanentemente preparado para actuar en caso de contingencia.

Coordinador de Sistemas.- es el responsable de determinar los sistemas Críticos de la Municipalidad de Villa el Salvador, que en caso de presentarse alguna contingencia como corte de energía eléctrica prolongada, temblor, incendio, falla del sistema de cómputo, perdida de documentación, o alguna otra causa determinada, se llegara a afectar sensiblemente la continuidad de las operaciones en las áreas que utilicen dichos sistemas críticos. En caso de cambiar a otras instalaciones alternas, el Coordinar de Sistemas deberá definir cuáles serían las actividades que se deberán seguir para la configuración o instalación de los sistemas desarrollados, optimizando los recursos con los que se cuente, realizando las pruebas necesarias hasta su correcto funcionamiento en las terminales destinadas para su operación. Deberá mantener actualizados los manuales y utilización al momento de requerirse.

Personal Clave.- es el responsable de la aplicación de los procedimientos que describa el plan de contingencia para cada una de las diferentes circunstancias o contingencias previstas y de reportar con la periodicidad que se indique en el plan, al Coordinador de su área y al Coordinar General, los resultados de la aplicación de alguna de las fases del plan. Coordinaran con el personal de la Municipalidad de Villa el Salvador involucrado, la realización de las actividades contenidas en el plan de contingencia para la situación que se hubiera presentado y tratar por todos los medios que les sea posible el logro de los objetivos y asegurar la continuidad de las operaciones de la MVES, disminuyendo el impacto de la contingencia al mínimo.

Darán aviso al coordinador de su área, cuando a su juicio, las circunstancias que provocaron la activación del plan hubieran desaparecido y se estuviera en condiciones de continuar normalmente con las actividades. En caso de requerir de actividades complementarias para regresar a las actividades normales, especialmente cuando se trate de los sistemas informáticos de MVES, deberán incluir el plan de actividades que se deberá seguir para retomar a la situación normal.

Personal de la Municipalidad de Villa el Salvador (usuarios).- El personal usuario en general, al verse afectado por una situación de contingencia, deberá en primera instancia apoyar para salvaguardar las vidas propias y de sus compañeros de trabajo, cuando la situación que se tuviera presentado sea grave (incendio, terremoto, etc.); posteriormente, y en la medida en que la situación lo permita, deberá coadyuvar a salvaguardar los bienes de la MVES (el propio inmueble, equipos computacionales, documentación, etc.).

3.2.3.1.4. CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

ANTECEDENTES

La elaboración de un Plan de Contingencias implica disponer de personal con responsabilidades y recursos definidos que ayuden a suplir los sistemas de información afectados.

MIEMBROS

El Comité de Seguridad de la Informacion acompaña y hace seguimiento a la marcha del Plan en función de los objetivos planteados. Los representantes de este Comité son:

Área	Encargado
Gerencia Municipal	Sr. Edgar Hinojosa Alarcon
Unidad de Desarrollo Tecnológico	Sr. Luis Alberto Álvarez Flores
Gerencia de Administración	Ing. Luz Zanabria Limaco
Unidad de Logística Servicios Generales y control patrimonial	Abog. Eileen Laos Moscoso
Gerente de Planeamiento y Presupuesto	Sr. José Arturo Robles Villafuerte

3.2.3.1.5. Las funciones del Comité de Seguridad de la Informacion serán:

a. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
b. Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
c. Aprobar las principales iniciativas para incrementar la seguridad de la información.
d. Evaluar y coordinar la implementación de controles específicos de seguridad de información para nuevos sistemas o servicios.
e. Promover la difusión y apoyo a la seguridad dentro de La Municipalidad.
f. Coordinar el proceso de administración de la continuidad de los sistemas de información municipales frente a interrupciones imprevistas.
g. Realizar las actividades que sean necesarias para el cumplimiento de su objetivo.
h. Efectuar el monitoreo y la evaluación periódica de los resultados;
i. Gestionar recursos financieros para la ejecución del Plan de Contingencias.

REUNIONES

a. El Comité se reunirá ordinariamente por lo menos dos veces al año. La asistencia a esta reunión es de carácter obligatorio. En el caso que algún miembro no pueda asistir, deberá nombrar a un representante o suplente de su Gerencia o Subgerencia.

b. En el curso de la reunión el Comité puede establecer los equipos de trabajo que considere necesario para facilitar las labores del Comité, designando un responsable por cada equipo de trabajo.

c. El quórum para las reuniones del Comité estará constituido por la mitad más uno de los representantes designados o de sus suplentes (en caso de ausencia de los respectivos titulares).

d. Si se presenta a consideración un asunto no incluido en la orden del día de cualquiera de las reuniones, se decidirá de inmediato, mediante el voto de la mayoría, si procede o no su deliberación sobre el nuevo asunto.

e. Las decisiones del Comité se tomarán por voto de la mayoría simple de los representantes presentes del Comité.

f. A las reuniones del Comité de Seguridad de la Informacion podrán asistir en calidad de observadores, representantes de las diferentes áreas relacionadas con el tema de la reunión y que hayan sido invitados a través del Coordinador del Comité.

g. Se elaborarán informes finales de cada reunión, los cuales serán comunicados a los integrantes del Comité. Cuando se solicite o el caso lo requiera, los documentos se publicarán en otros medios de información.

1. El Plan de Contingencias contará con el apoyo correspondiente por parte de la Alta Dirección, para suministrar de recursos financieros, humanos y materiales a fin de su implementación y ejecución.

2. Los Gerentes, Subgerente, Jefes, y colaboradores que laboren en la Municipalidad de Villa El Salvador, deben tomar parte de las actividades y están obligados a participar en la implementación y ejecución del Plan de Contingencias.

1. Contar con la colaboración de los organismos como: Policía Nacional del Perú, Defensa Civil, Cruz Roja, ESSALUD, Organizaciones Vecinales, e instituciones, como apoyo externo.

2. Definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento del Plan de Contingencias.

3. Implementar un Plan de Capacitación y Entrenamiento a todos los colaboradores de la Municipalidad de Villa El Salvador, con la finalidad de mantener al personal debidamente entrenado para prevenir y enfrentar cualquier emergencia, así como, disponer de un plan de entrenamiento de todos los colaboradores en la solución de situaciones de emergencia a través de charlas periódicas en los que se describan los riesgos existentes.

4. Las medidas que debemos adoptar para protegernos son tantas como amenazas existen, es por ello que se debe difundir a todas las áreas de la Municipalidad copias del Plan, documentos resumen, carteles, afiches u otro tipo de documento para su información.

5. Realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Plan de Contingencias, y así cumplir con las disposiciones legales vigentes dispuestas por la ONGEI.

6. Implementar un servidor de respaldo que haga de Backup a todos los servidores, reemplazando a uno u otro según se necesite, para ello se realizará las acciones necesarias para que la MVES/UDTE cuente con dicho servidor que cumpla a su vez con una gama de funciones como por ejemplo: Servidor de Archivo, Servidor de Respaldo, Almacenamiento masivo, Servidor de usuarios y/o Workgroups, etc.

Bibliografía

1. Gobierno Electrónico Peruano.
   Metodologías Informática del INEI N° 10. Plan de Contingencias y Seguridad de la Información.
2. Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información.
3. Tesis sobre Políticas de Seguridad de la Universidad Mayor de San Marcos.

4. Páginas visitadas en Internet.

ANEXOS

IMPLEMENTACION DEL PLAN DE CONTINGENCIAS

REQUERIMIENTOS MINIMOS A CONSIDERAR PARA LA IMPLEMENTACION DEL PLAN DE CONTINGENCIAS DE LA MVES

El área usuaria es la responsable de definir con precisión las características, condiciones, cantidad y calidad de los bienes, servicios u obras que requiera para el cumplimiento de sus funciones

Servidores
02 servidores de alto desempeño

Computadoras
10 computadoras que sirvan de respaldo a ser instaladas en cualquier punto

Pozo a tierra
Habilitación de los 3 pozos a tierra para Data Center y Plataformas de Atención al Contribuyente

Deshumecedores
Para equipos informáticos

Discos alternos NASS
Permitiendo salvaguardar información de respaldo para garantizar la continuidad de las labores

Los respaldos se realizarán en medios magnéticos removibles (01 TERABYTE), y serán etiquetados inmediatamente después de acabada la operación de backup. La terminología que se utilice para identificación de los cartuchos, estará basada principalmente en la fecha de realización del mismo, y también en la naturaleza de la data archivada.

Los cartuchos serán almacenados en las instalaciones la MUNICIPALIDAD. Como medida de contingencia, se sugiere que se implemente una rutina de rotación de cartuchos mediante el cual al menos una vez a la semana se almacene una copia de los sistemas desarrollados en las instalaciones de la MUNICIPALIDAD Y AGENCIAS DESCONCENTRADAS

Sistema Anti-Intrusión

Se deberá instalar sensores de movimiento marca (que indique LOGISTICA), cuya finalidad es detectar el ingreso de personas al edificio. Este sistema ante la presencia de cualquier individuo o fuente de calor, hace sonar la alarma ubicado en el patio de ingreso. La señal también debería se registrada los bomberos mediante sistema de control remoto. En base a estas señales se toman las decisiones pertinentes. Del mismo modo urge la instalación de este sistema para la sala de servidores.

Sistema de Circuito Cerrado
Se recomienda un sistema de circuito cerrado compuesto por cámaras de vigilancia por video con grabadora digital que permita almacenar registros durante 30 días. Este sistema nos permitirá obtener registro e imagen del área donde se encuentre para detectar intrusiones, eventos no deseados, sabotajes, entre otros.

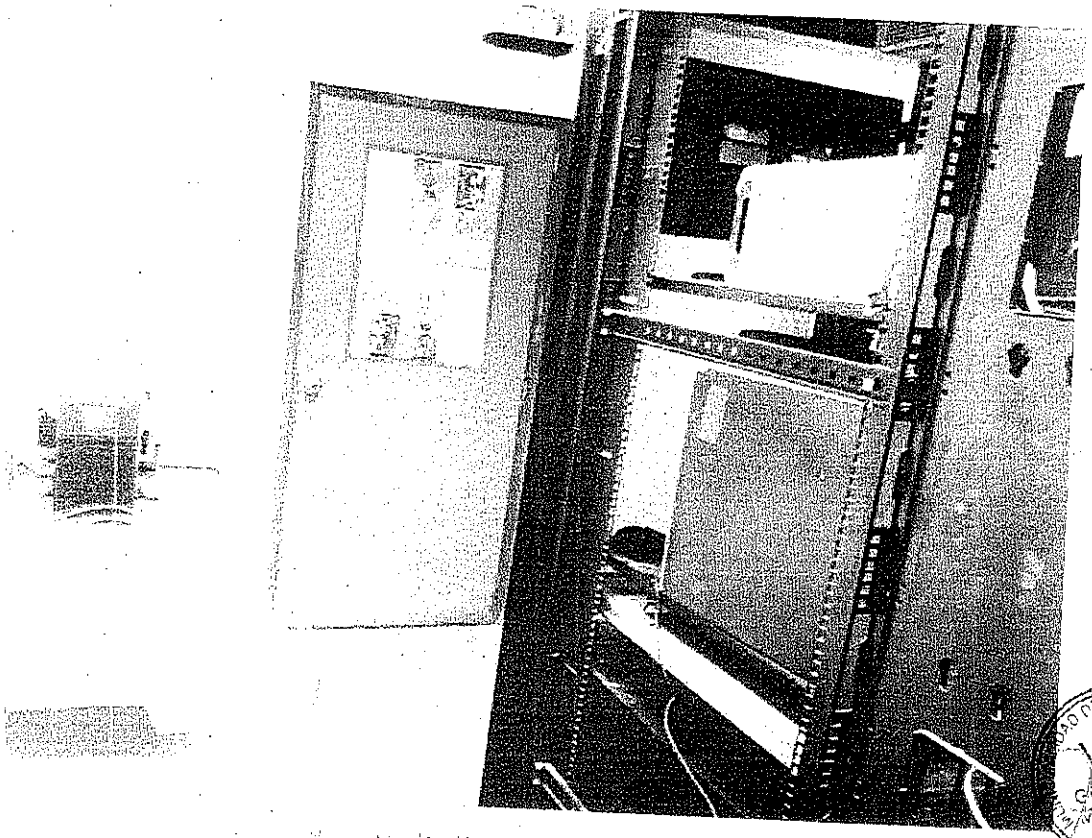
Sistema Anti-Inundación
Se recomienda reparación completa en el sistema de drenaje y la instalación de sensores de aniego.

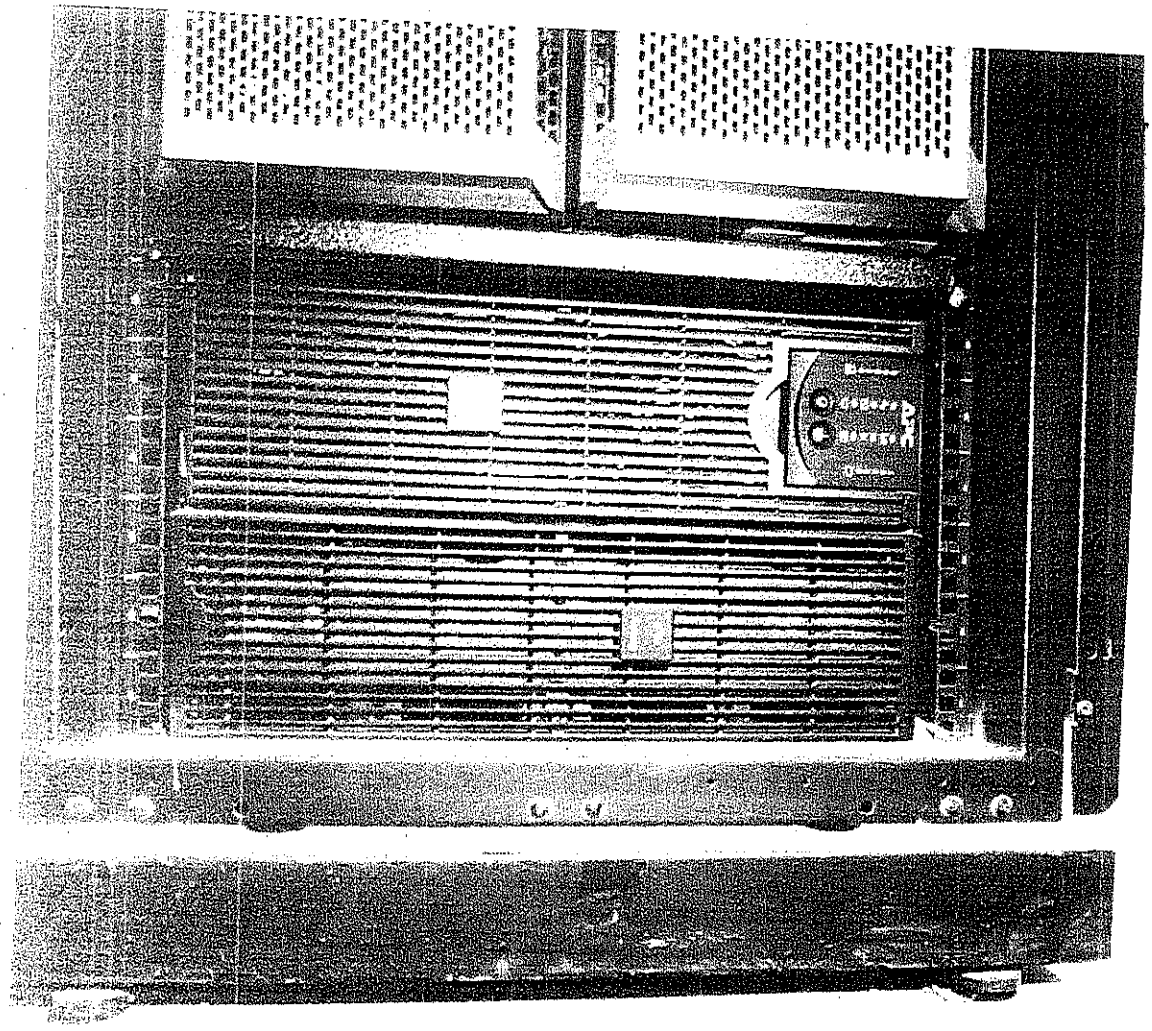
Sistema Contra Incendio (Extintores)
La institución en la sede central deberá de contar con un sistema de protección contra incendios, el cual se basa en extintores de polvo químico seco (PQS) y gas carbónico (Co2) distribuidos en todos los pisos de la institución desde el sótano hasta la azotea (cuarto piso). Así también en la explanada, Agencias desconcentradas y Gerencias desconcentradas. LA MUNICIPALIDAD también deberá de contar con los siguientes tipos de extintores para las diversas clases de incendios:
Incendios Clase B y C: Todo lo referente a Líquidos Inflamables y/o Equipos Eléctricos (Gasolina, Pinturas, Solventes, Equipos eléctricos conectados).
Sistema Contra Incendio (Agente Limpio)
En el gabinete de lucha contra incendios deberá de constar de una manguera de 50 metros de largo dos pulgadas de diámetro, un hacha y un extintor PQS de 6 kilos adicional.
Así también tenemos en todas las oficinas y pasadizos extintores de gas carbónico y de polvo químico seco de conformidad a la norma correspondiente.

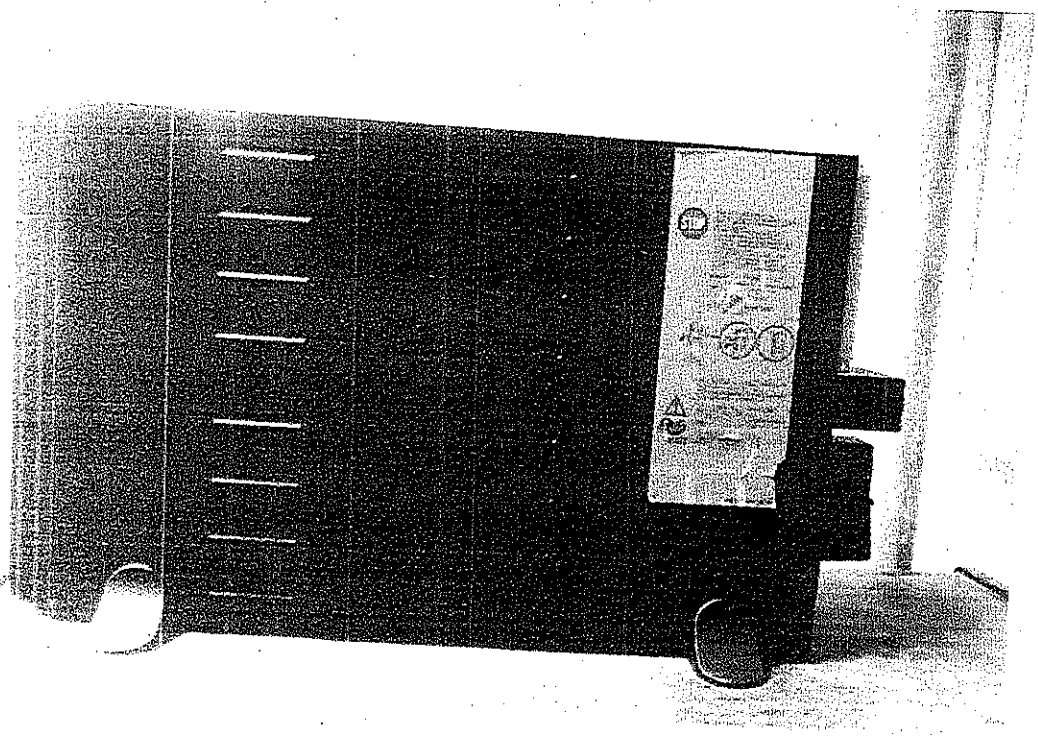
Luces de Emergencia
Se deberá instalar sistema de luces de emergencia, las cuales tiene una batería interna que se activan ante un corte de fluido eléctrico con una autonomía de 02 horas y están distribuidos en todas las áreas los pasadizos de cada piso en la sede central. Se recomienda la activación de estas luces por encontrarse actualmente ninguna Grupo Electrógeno operativo 100% con sistema llave en mano
Es recomendable la adquisición de un GRUPO ELECTROGENO de mayor potencia en proporción a la demanda de usuarios y equipos de investigación de última tecnología.

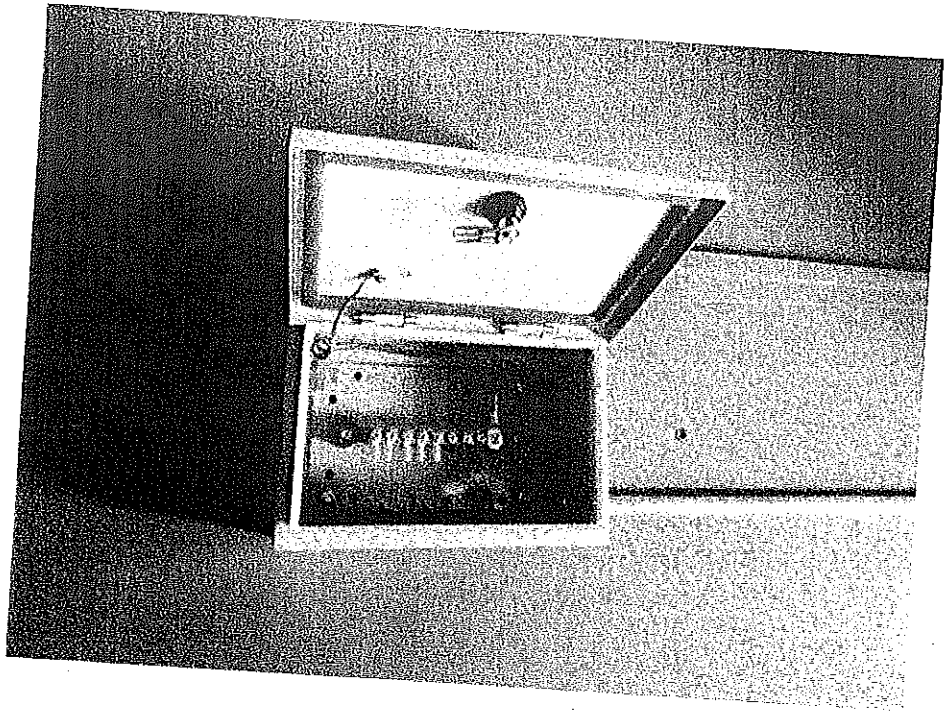
EJECUCION DE LA IMPLEMENTACION DEL PLAN DE CONTINGENCIAS : 2015 - 2016

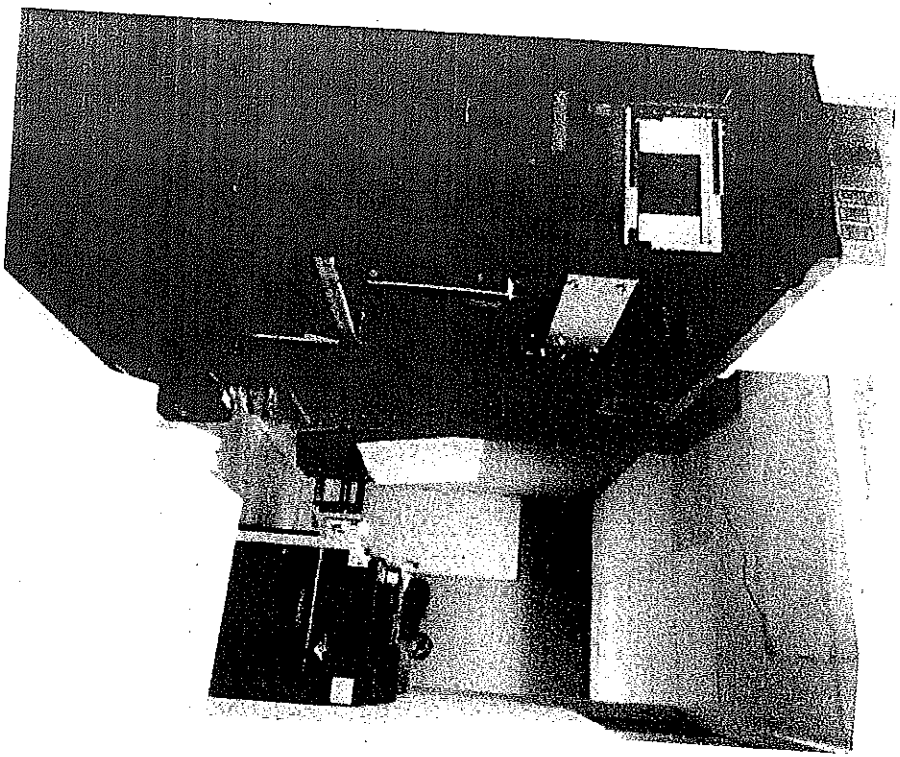
- Reestructuración de la Sala de Servidores, habilitación del RAC de Servidores
- Ampliación de ambientes para la Sala de Servidores
- Implementación de nuevos elementos de seguridad de software FORTINET,
- Implementación de Antivirus – GDATA
- Adquisición de UPS .- 2 UPS y un transformador
- Implementación del Pozo a Tierra
- Reestructuración de la RED
- Implementación de Servidor HP Proliant – habilitación de RAID de discos duros
- Adquisición de discos NASS
- Programación de ejecución de Backups de los Sistemas











MUNICIPALIDAD DE VILLA EL CHACAY
V°B°
GERENCIA MUNICIPAL

MUNICIPALIDAD DE VILLA EL CHACAY
V°B°
SECRETARIA GENERAL