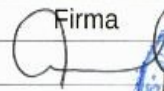




PLAN DE CONTINGENCIA INFORMÁTICO DE LA ALCALDÍA MUNICIPAL DE SOYAPANGO



Versión: 01	Código:	Fecha: Noviembre 2017	N.º Páginas:
Rubro	Nombre	Cargo	Firma
Revisado Por:	Ing. Ausel Garcia	Gerente General	
Aprobado Por:	Concejo Municipal		





INDICE

I. INTRODUCCIÓN.....	4
II. OBJETIVOS.....	5
III. ALCANCES.....	5
IV. MARCO LEGAL.....	6
V. RESPONSABILIDAD Y AUTORIDAD.....	6
CAPITULO I :.....	7
DEFINICIONES.....	7
1.1. Marco Teórico.....	7
CAPITULO II :.....	10
DISPOSICIONES GENERALES.....	10
2.1: Estructura Organizativa.....	10
2.2: Recursos Humanos.....	11
2.2.1: Recursos Informáticos y Tecnológicos Existentes.....	11
2.2.2. Hardware de Equipos Informáticos :.....	12
2.2.3. Aplicativos informáticos.....	14
2.2.4. Principales servicios que deberán ser restablecidos y/o recuperados.....	15
CAPITULO III.....	16
IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS.....	16
3.1: Identificación de Riesgos.....	16
3.2: Probabilidad de Ocurrencia de Riesgos.....	17
3.3: Riesgos en la Seguridad Informática (equipos y archivos).....	18
3.4: ESCENARIOS CONSIDERADOS PARA LA CONTINUIDAD DE LOS PROCESOS Y SERVICIOS.....	19
I. NO HAY COMUNICACIÓN ENTRE CLIENTE–SERVIDOR DENTRO DE LA INSTITUCIÓN MUNICIPAL.....	19
II. FALLA DE EQUIPOS INFORMÁTICOS.....	20
1. FALLA DE UN SERVIDOR.....	20
Detalle de las causas de Falla del Servidor.....	20
FALLA DE LOS EQUIPOS (PC,IMPRESORES,ETC.).....	22
APLICACIÓN DE CONTINGENCIA EN CASO DE SERVIDORES.....	23
III. AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE LA UNIDAD DE INFORMÁTICA.....	24
RECURSOS DE CONTINGENCIAS.....	24
IV. INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.....	27
V. PERDIDA DE SERVICIO INTERNET.....	28
RECURSOS DE CONTINGENCIAS.....	28
VI. INDISPONIBILIDAD DEL CENTRO DE CÓMPUTO (DESTRUCCIÓN DEL CUARTO DE SERVIDORES).....	28
CAPITULO IV:.....	30
IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA.....	30
4.1 Plan De Recuperación Y Respaldo De La Información.....	30



4.2 Plan de Verificación.....	32
4.3 Plan (Acciones Correctivas Y Preventivas).....	32
CAPITULO V.....	34
DISTRIBUCION DEL PLAN DE CONTINGENCIA.....	34
CAPITULO VI.....	34
MANTENIMIENTO DEL PLAN DE CONTINGENCIA.....	34



I. INTRODUCCIÓN

El presente documento es el Plan de contingencia informático de la Alcaldía Municipal de Soyapango, donde se tiene en cuenta la información como uno de los activos más importantes de la Municipalidad, además de la infraestructura informática y Telecomunicaciones de la cual está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos.

Este Plan implica realizar un análisis profundo de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos informáticos y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, backup, etc.).

Nuestro Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o humanos.



II. OBJETIVOS

Los objetivos principales del presente documento son los siguientes:

- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información y red de la institución ante la eventual presencia de cualquier tipo de siniestros que los paralicen parcial o totalmente.
- Garantizar la continuidad en los procesos de los elementos críticos necesarios para el funcionamiento de las aplicaciones de la institución e identificar las acciones que se deben llevar a cabo y los procedimientos a seguir en el caso de la presencia de un siniestro que restrinja el acceso a los sistemas de información y red interna.

III. ALCANCES

El alcance del plan de contingencia incluye los elementos básicos y esenciales, componentes y recursos informáticos que conforman los sistemas de información, equipos, infraestructura, personal, servicios y otros, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios de la Municipalidad.



IV. MARCO LEGAL

La norma técnica de Control Interno Específicas, de La Municipalidad de Soyapango en su Art. 20, Art 23, Art 25, Art. 27, Art. 95, Art. 99, Art. 101.

El Reglamento para el Uso y Control de las Tecnologías de Información y Comunicaciones en las Entidades del Sector Publico, Art 11, Art. 26, Art 27, Art. 39, Art. 40, Art. 41.

V. RESPONSABILIDAD Y AUTORIDAD

La Gerencia de Informática es la responsable de la Elaboración y actualización permanente del Plan de Contingencia; así mismo debe asesorar y apoyar a las diferentes unidades con responsabilidad administrativa a quienes tenga en su inventario equipo Informático y de Comunicaciones. La actualización será aprobada por el Honorable Concejo Municipal.

Cualquier incumplimiento de las normativas acá establecidas, serán sancionadas de acuerdo a la gravedad del hecho.

CAPITULO I:

DEFINICIONES

1.1. Marco Teórico

Acceso: Es la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una Base de Datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.

Amenaza: Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a un computador. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario

Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.

Base de Datos: Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran, brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.

Contingencia: Interrupción, no planificada, de la disponibilidad de recursos informáticos.

Datos: Los datos son hechos y/o valores que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos en el presente documento. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y Bases de Datos, textos (colección de



palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), videos

(secuencia de tramas), etc.

Golpe (Breach): Es la violación exitosa de las medidas de seguridad, como el robo de información, la eliminación de archivos de datos valiosos, el robo de equipos, PC, etc.

Incidente: Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.

Integridad: Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.

Plan De Contingencia: Conjunto de medidas (de DETECCIÓN y de REACCIÓN) a poner en marcha ante la presentación de una contingencia.

Plan de Prevención : Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan.

Plan de Ejecución : Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alternativo que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.



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

Privacidad: Se define como el derecho que tiene una institución para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros.

Seguridad: Se refiere a las medidas que toma la institución con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizada o intencional. En el caso de los datos e información contenidos en los sistemas de información de la institución, la privacidad y seguridad guardan estrecha relación entre sí, aunque la diferencia entre ellas radica en que la primera se refiere a la distribución autorizada de información y la segunda al acceso no autorizado.

Sistemas de Información: Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos.

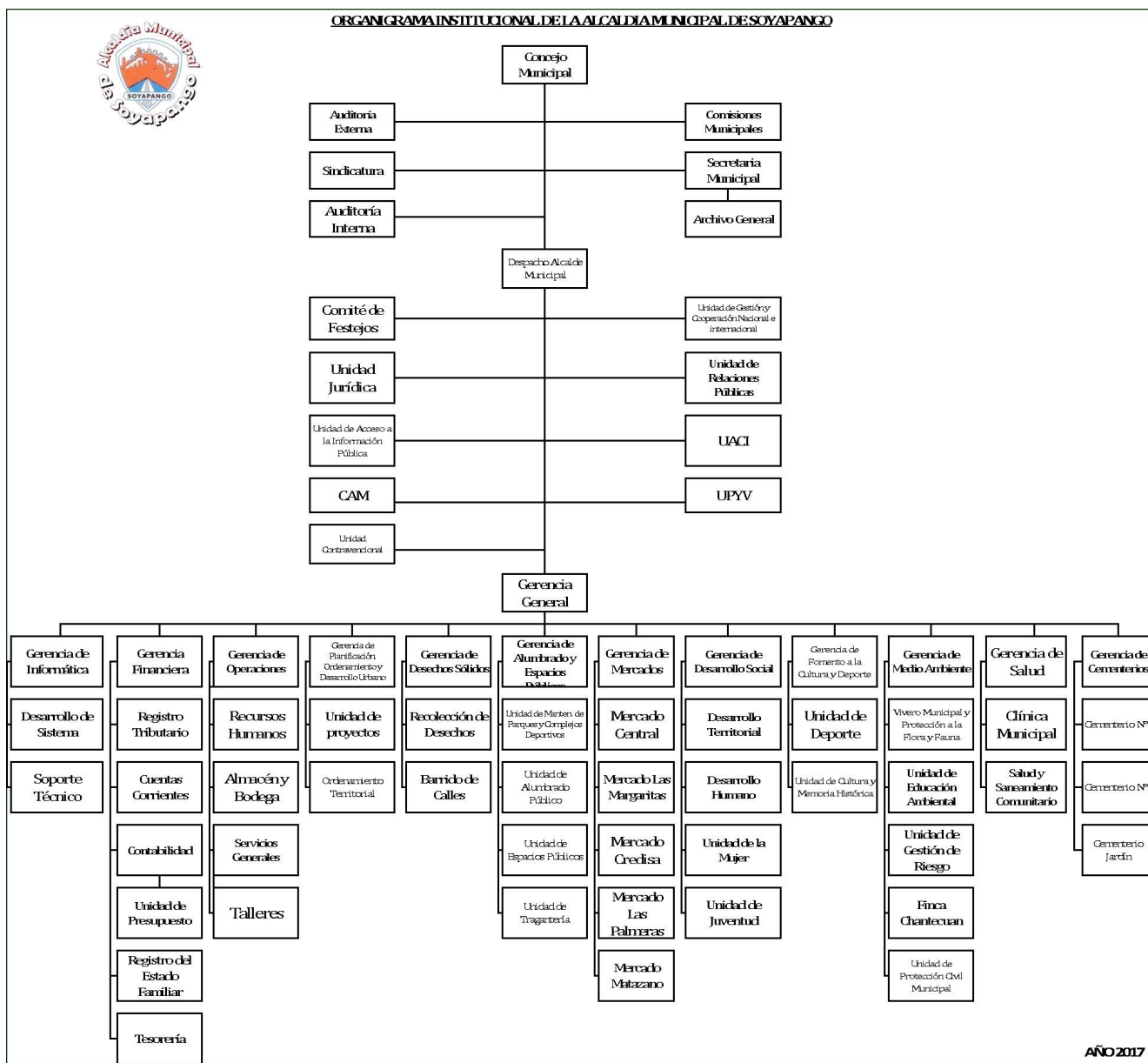
Cortafuegos (Firewall): Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

CAPITULO II:

DISPOSICIONES GENERALES

2.1: Estructura Organizativa

Localización y dependencia estructural de la Gerencia Informática: Bajo jerarquía de Gerencia General, dividida en dos unidades: Desarrollo de Sistemas y Soporte Técnico.





2.2: Recursos Humanos

Personal del Área de Sistemas y Soporte Técnico Requerido:

SUB ÁREAS/ REQUERIDAS			SUB ÁREAS/ ACTUAL	
Gerencia Informática			1	
DESARROLLO DE SISTEMAS				
Nº	Cargos	Cantidad		
1	Coordinador de Sistemas	1	0	
2	Programadores-Desarrolladores WEB	4	3	
3	Administrador de Base de datos	1	0	
4	Depuradores de base	1	0	
SOPORTE TÉCNICO				
1	Coordinador de Redes	1	0	
2	Soporte Técnico/ Técnicos colaboradores	4	4	

2.2.1: Recursos Informáticos y Tecnológicos Existentes

El software Identificado en la institución es el siguiente:

Nº	SOFTWARE/LICENCIA	DESCRIPCIÓN	Total de Licencias
1	Sistemas Operativos de Estaciones de Trabajo	Microsoft Windows 7, 8, 10 Windows XP Linux Ubuntu vr 12- 16	40 1 230
2	Sistemas Operativos de Servidores	Linux Centos vr 7.0 Server Ubuntu Server Microsoft Windows Server 2003 Microsoft Windows Server 2012	1 9 1 1
3	Software de Oficina	Microsof Office Libre Office 3,5	10 250
4	Software de Base de Datos	Postgresql MySql	1 1

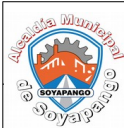


5	Software de Seguridad	Eset Nod 32 watchguard Control de Asistencia	40 1 2
6	Software de Diseño	Bricscad Escritorio AirGISd Escritorio AutoCAD Escritorio	10 1 1
7	Otros	Sistema de carnés	1

2.2.2. Hardware de Equipos Informáticos :

Los activos para el Sistema de Información con los que cuenta La Administración Municipal se detallan a continuación:

Nº	RECURSO	CANTIDAD	ESPECIFICACIONES / UBICACIONES
1	PCs	270	Clones, marcas DELL, Lenovo, HP, Toda la municipalidad y edificios anexos
2	SERVIDORES	11	Centro de Datos, DELL, HP
3	SWITCHES	17	Centro de datos, Edificios anexos, Interno, HP TP LINK
4	IMPRESORAS/ ESCANER Laser, Multifuncionales, Matriciales, etiqueteras, Carnetización		En toda la institución, HP, Canon, EPSON, Magic Card
5	TELÉFONOS IP/ANALOGOS	125	MITEL, GRANDSTREAM: en toda la institución
6	LAPTOPS	50	HP: en toda la Institución
7	ACCESOS POINT	5	Cuentas corrientes, Sala de concejo, Sala de despacho, Gerencia General, Comité de Festejos



8	PLOTTER	1	PDU
9	UPS	200	Centros de datos, Pcs de cada unidad
10	PLANTA TELEFÓNICA IP	1	Centro de datos
11	DISCOS EXTERNOS	3	Centro de Monitoreo, Cementerio, Comunicaciones
12	CÁMARAS IP	12	HikVision: Internas: Aseo, Despacho, Registro Familiar, Parqueo, Desarrollo Social
13	TORRES CDS/DISCOS COPIAS RESPALDOS	75	Informática, Tesorería
14	MARCADORES	5	Edificio central, Albert Eisnten, CAM, Aseo, informática
15	FIREWALL	2	Centro de datos: WacthGuard
16	Supresores	2	Centro de Datos
17	Antenas de Enlace de datos	20	Canopy, Ubiquiti: En toda la Institución
18	Pantallas TV	8	En toda la Municipalidad
19	Proyectores	6	En toda la municipalidad



2.2.3. Aplicativos informáticos

NOMBRE DEL SISTEMA	DESCRIPCION	RESPONSABLE	PLATAFORMA	BASE DE DATOS	AÑO DE CREACION	
SIMUS (Sistema Informático Municipal de Soyapango)	Ctas. Corrientes (CCT)	Permite la administración de todo lo relacionado al estado de la cuenta de los contribuyentes, y su respectivo cobro, sean éstos domiciliarios o empresariales.	Java	Postgresl	2009	Informática: Miguel Najarro
		Ctas. Corrientes : Víctor Ramos				Informática: Miguel Najarro
	Registro Trib. (CTO)	Consulta de estados de cuenta, calificaciones, mantenimiento de tasas e impuestos, colonias, etc				Reg. Tributario : Flor Saravia
		Reg. Familiar (REF)				Emisión y/o asentamiento de partidas de nacimiento, defunción, matrimonio y divorcio, además de carnés de minoridad
	Reg. Familiar : Beatriz Pérez					
	Tesorería (TES)	Manejo de ingresos monetarios en los diferentes departamentos de la municipalidad				Informática: Miguel Najarro
						Tesorería : José Gómez
	Recursos Humanos (RHM)	Control de datos de los empleados de la municipalidad así como elaboración de planillas				Informática: Miguel Najarro
						Recursos Humanos : Beatriz Leiva
	Inventarios y Bodegas (INV)	Manejo y Administración de diferentes tipos de inventarios, como bodega de materiales y existencia de repuestos en bodegas de Espacios Públicos y Aseo.				Informática: Jacqueline Flores y Miguel Najarro
Bodega papelería : Jorge Meléndez						
Aseo : Antonio Argueta						
Espacios Públicos : Salomon Lopez						
Mercados (MER)	Control de Ingresos de cuentas de Mercados, Registro de Propietarios, etc.	Informática: Miguel Najarro				
		Mercado Central : Rosalba Baires				
		Mercado Palmeras : Roxana Maldonado				
Equipo Informático (INF)	Control del inventario de equipos informáticos tales como monitores, CPUs, impresores, etc. Además de emisión de viñeta para colocar en cada equipo y tener su respectivo control	Informática: Douglas Servellón y Miguel Najarro				
Seguridad (SEG)	Administra los permisos que tendrán los usuarios a los diferentes módulos y opciones de todo el Sistema de Informático Municipal (SIMUS).	Informática: Douglas Servellón y Miguel Najarro				
SIAS (Sistema de Alcaldía de Soyapango)	Cheques	Elaboración, emisión y resguardo de cheques para el pago de empleados, proveedores de la municipalidad	Java	Postgresl	2012	Informática: Susana Cortéz
		Tesorería : Encarga de Emisión de Cheques				
ALISIA Y ALISON	Tickes de Turnos	Emisión de tickes de turnos para los contribuyentes, para las áreas de Cuentas Corrientes y Registro del Estado Familiar	PHP	MySql	2012	Informática: Susana Cortéz
		Ctas. Corrientes : Víctor Ramos				
		Reg. Familiar : Beatriz Pérez				
Sistema de Registro Familiar	Emisión de Partidas	Emisión de partidas de nacimiento, defunción, matrimonios, divorcios y reposiciones de éstas mismas (En la actualidad regularmente solo se ocupa de consulta)	Visual FoxPro 6.0	Tablas de Visual FoxPro 6.0	2001	Informática: Miguel Najarro
		Reg. Familiar : Beatriz Pérez				



2.2.4. Principales servicios que deberán ser restablecidos y/o recuperados

Nº	Plataformas	Servicios
1	Sistemas Operativos: Ubuntu Vr. 12-16 Windows 7-10	- Correo Electrónico - Servicio de Internet - Antivirus - Herramientas de Ofimática - Portales WEB Institucionales
2	Software Base de datos:	- Base de datos Postgre - Base de Mysql
3	Respaldo de la información	- Backup de la base de datos SIMUS - Backup de la plataforma de aplicaciones - Backup del servidor DHCP - Backup del servidor de Dominios - Backup de políticas de seguridad de internet(WhacthGuard) - Backup del servidor de aplicaciones 1.1 - Backup del servidor de archivos
4	PC	Backup de datos de Terminales

CAPITULO III.

IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

3.1: Identificación de Riesgos

Los desastres causados por un evento natural o humano, pueden ocurrir, en cualquier parte, hora, negocio e instituciones. En esta fase de análisis de riesgos se han considerado tres elementos que permitirán aproximar un valor objetivo de los riesgos principales:

- El Tipo,
- La Probabilidad,
- El grado de impacto



Por lo cual existen tres tipos de grupos de riesgos, como por ejemplo:

- **Riesgos Naturales:** tales como mal tiempo, terremotos, etc.
- **Riesgos Tecnológicos:** tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.
- **Riesgos Sociales:** como actos terroristas y desordenes.

Establecer los riesgos a los cuales está propensa la institución, de igual manera determinar el nivel o factor de riesgo, por lo que se muestra la clasificación de probabilidades de riesgos:

PROBABILIDAD DE OCURRENCIA	DESCRIPCIÓN
Bajo	Poco probable que suceda
Muy Bajo	Incidencias aisladas
Alto	Incidentes Repetidas
Muy Alto	Frecuente
Medio	Sucede alguna vez

3.2: Probabilidad de Ocurrencia de Riesgos

De acuerdo a la probabilidad de ocurrencia de Riesgos se determina la Tabla de clasificación de Factores de Riesgo, según su escenario:

RIESGO	Tipo de Riesgos	Factor de Riesgo				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
Incendios	Tecnológico					XX
Inundaciones	Sociales, Naturales		X			
Robo Común de equipos y	Sociales					X



Archivos						
Vandalismo, daño de equipos y archivos.	Sociales					X
Fallas en los equipos, daño de archivos.	Tecnológico					X
Equivocaciones, daño de archivos.	Tecnológico			X		
Virus, daño de equipos y archivo.	Sociales					X
Terremotos, daño de equipos y archivos.	Naturales				X	
Acceso no autorizado, filtración de info.	Sociales					X
Robo de datos	Sociales					X
Fraude, alteración de información.	Sociales				X	
Desastre Total	Natural					X

3.3: Riesgos en la Seguridad Informática (equipos y archivos).

Las causas más representativas que originarían cada uno de los escenarios propuestos en el Plan de Contingencias y Seguridad de la Información se presentan en el siguiente cuadro.

Causas	Escenarios
<ul style="list-style-type: none"> • Fallas Corte de Cable UTP. • Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Punto de Swicht • Fallas Punto Pacht Panel. • Fallas Punto de Red. 	I. NO HAY COMUNICACIÓN ENTRE CLIENTE y SERVIDOR
<ul style="list-style-type: none"> • Fallas de Componentes de Hardware del Servidor. • Falla del UPS (Falta de Suministro eléctrico). • Virus. • Sobrepasar el límite de almacenamiento del Disco 	II. FALLA DE UN SERVIDOR.



<ul style="list-style-type: none"> • Computador del Escritorio funciona como Servidor. 	
<ul style="list-style-type: none"> • Accidente • Renuncia Intempestiva 	III. AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE INFORMATICA.
<ul style="list-style-type: none"> • Corte General del Fluido eléctrico 	IV. INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.
<ul style="list-style-type: none"> • Falla de equipos de comunicación: SWITCH, Antenas, Fibra Óptica. • Fallas en software de Acceso a Internet. • Perdida de comunicación con proveedores de Internet. 	V. PERDIDA DEL SERVICIO DE INTERNET
<ul style="list-style-type: none"> • Incendio • Sabotaje • Corto Circuito • Terremoto • Tsunami 	VI. INDISPONIBILIDAD DEL CENTRO DE COMPUTO (DESTRUCCIÓN DE LA SALA DE SERVIDORES)

3.4: ESCENARIOS CONSIDERADOS PARA LA CONTINUIDAD DE LOS PROCESOS Y SERVICIOS

Las personas que interviene en la ejecución del plan de contingencia, es el personal de informática, quienes son los responsables de emitir la alarma de la falla e iniciar las actividades para la ejecución de la contingencia.

A continuación se detallas los posibles escenarios que interrumpirían el normal desarrollo del funcionamiento de las operaciones y/o prestación de servicios específicos:

I. NO HAY COMUNICACIÓN ENTRE CLIENTE–SERVIDOR DENTRO DE LA INSTITUCIÓN MUNICIPAL.

IMPACTO DE ÁREA	AFECTA
No se puede trabajar con los recursos de la	Área en que labora



red de la institución (Información)	
Interrupción de sus actividades	Área en que labora

Tiempos Aceptables de Caídas:

RECURSO	PRIORIDAD DE RECUPERACIÓN
Sistemas: SIMUS,	ALTO
Servidor: Controlador de Dominio Primario, Base de Datos, Web, Aplicaciones	ALTO
Servidor correo y sistema documental(compartida)	ALTO
Servidor de Internet, SAFIM, COMPRASAL	ALTO

RECURSOS DE CONTINGENCIAS

Componentes de Reemplazo.-
Tarjeta de Red, Conector RJ-45, Jack RJ-45, Testeador, herramientas de Cableado estructurado, etc.

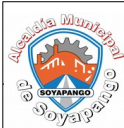
II. FALLA DE EQUIPOS INFORMÁTICOS

1. FALLA DE UN SERVIDOR.

IMPACTO DE ÁREA	AFECTA
Paralización de los sistemas o aplicaciones que se encuentran en los servidores que presentan fallas	Todas las áreas de atención de usuarios y proveedores
Posible Pérdida de Hardware y software	Unidad de Informática
Perdida del proceso automático de Backup y restore	Unidad de Informática

Prioridad De Recuperación De Servicios

RECURSO	PRIORIDAD DE RECUPERACIÓN
Servidor: Controlador de Dominio Primario, Base de Datos, Web, Aplicaciones	ALTO



Servidor de compartida	ALTO
Servidor de DNS y Firewall	ALTO
Servidor Backup	ALTO
Servidor Web	MEDIO
Servidor DHCP	ALTO

Detalle de las causas de Falla del Servidor.

CAUSA DE FALLAS	DESCRIPCIÓN DE ACCIONES
<p>CASO A: Error Físico de Disco de un Servidor (Sin RAID).</p> <p>Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:</p>	<ol style="list-style-type: none">1. Ubicar el disco malogrado.2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red o teléfono a jefes de área.3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.4. Bajar el sistema y apagar el equipo.5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.7. Revisar los sistemas que se encuentran en dicho disco y verificar su buen estado.8. Habilitar las entradas al sistema para los usuarios.
<p>CASO B: Error de Memoria RAM</p> <p>En este caso se dan los siguientes síntomas:</p> <ol style="list-style-type: none">1. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.2. Ante procesos mayores se congela el proceso.3. Arroja errores con mapas de direcciones hexadecimales.4. Es recomendable que el servidor cuente con ECC (error correctchecking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.	<p>Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por informática.</p> <p>Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:</p> <ol style="list-style-type: none">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 las memorias malogradas.d) Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.e) Realizar pruebas locales, deshabilitar las



	<p>entradas, luego conectar el cable, habilitar entradas para estaciones en las cuales se realizarán las pruebas.</p> <p>f) Probar los sistemas que están en red en diferentes estaciones.</p> <p>g) Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios.</p>
<p>CASO C: Error de Tarjeta(s) Controladora(s) de Disco</p> <p>Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:</p>	<ol style="list-style-type: none">1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.2. El servidor debe estar apagado, dando un correcto apagado del sistema.3. Ubicar la posición de la tarjeta controladora.4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.
<p>CASO D: Error Lógico de Datos</p> <p>La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:</p> <ul style="list-style-type: none">• Caída del servidor de archivos por falla de software de red.• Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.• Bajar incorrectamente el servidor de archivos.• Fallas causadas usualmente por un error de chequeo de inconsistencia física.	<ol style="list-style-type: none">1. Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos.2. Deshabilitar el ingreso de usuarios al sistema.3. Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.4. Cargar un utilitario que nos permita verificar en forma global el contenido



<p>En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:</p>	<p>del(os) disco(s) duro(s) del servidor. 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.</p>
<p>CASO E: Caso de Virus Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:</p>	<ol style="list-style-type: none"> 1. Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación 2. El antivirus muestra el nombre del archivo infectado y quién lo usó. 3. Estos archivos (exe, com, etc.) serán reemplazados del CD/DVD original de instalación o del backup. 4. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión y desinfección.

FALLA DE LOS EQUIPOS (PC,IMPRESORES,ETC.)

IMPACTO DE ÁREA	ACCIÓN CORRECTIVA
<p>La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.</p>	<p>Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.</p>
<p>La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.</p>	<p>Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de equipos que están para dar de baja.</p>
<p>Cada área funcional se une a la Red a</p>	<p>Se cumple. Los gabinetes se encuentran</p>



través Gabinetes, la falta de energía en éstos, origina la ausencia de uso de los servicios de red.	protegidos en un lugar de acceso restringido y son manipulados solo por personal técnico de Informática.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo	Los equipos de escritorio cuentan con ups de 600va/750VA, el centro de datos esta protegido con UPS de 1,5KVA y supresores.
Perdida de Hardware y Software	Unidad de Informática

APLICACIÓN DE CONTINGENCIA EN CASO DE SERVIDORES

Equipo Server	RECURSOS DE CONTINGENCIAS
Servidores (hardware)	<ol style="list-style-type: none">1. Se verifica la falla de los componentes del servidor2. Se realizan pruebas de funcionamiento3. Se reemplaza el componente malo (Memoria, Disco Duro, etc.).4. En caso que es el disco se tiene que instalar y configurar el sistema operativo para server.5. Se restablecen las copias de configuración almacenadas en el servidor de Repositorio Backup diario de la Información de los servidores, en otro equipo o servidor en paralelo.6. Se reinician los servicios Tiempo aproximado: 2 horas7. Si el daño es el server completo, se monta un nuevo server, con sus configuraciones, tiempo aproximado: 4 horas
Servidores (software)	Para restablecer los servicios de aplicaciones, se deben seguir los siguientes pasos: <ol style="list-style-type: none">1. Se reinicia el servicio de TOMCAT2. Se restaura la última copia realizada a la base de datos almacenada en el disco de copias de BACKUP. También existe un consolidado mensual en el servicio FTP alojado en el servidor3. Se reinstala la base de datos de Posgresql del repositorio 10.10 1.8 la instalación se encuentran



en la oficina de informática.

4. Se reinstala la consola administrativa del antivirus, el usuario y la contraseña se encuentra en la oficina de sistemas

5. Se reinstala el openfire, la copia con los usuarios se encuentra en el servicio FTP en el servidor

6. Se reinician todos los PC que acceden al sistema integral de información o algún otro servicio alojado en este servidor. Tiempo aproximado: De 2 a 4 horas

Recursos: Personal Humano de la oficina de sistemas

III. AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE LA UNIDAD DE INFORMÁTICA.

IMPACTO DE ÁREA	AFECTA
Interrupción de funciones de la persona ausente	Todas las Áreas
Administración de bases de datos Control y monitoreo de servidores. Soporte a los usuarios. Ajustes a programas críticos en producción	Las Áreas de atención a contribuyentes y usuarios.

RECURSOS DE CONTINGENCIAS

Se presentan las funciones actuales que tienen a su cargo el personal de la Unidad de Informática:

DESARROLLO DE SISTEMAS/

Técnico Programador

- Contribuir con la Jefatura del departamento en cuanto al análisis de nuevos sistemas informáticos a implementar.
- Desarrollar los programas necesarios para la operacionalización de los procesos.
- Actualizar los sistemas de computación en las opciones y reportes que sean requeridos por la Jefatura.

- Elaboración de diferentes reportes de información almacenados en la base de datos de la Municipalidad.
- Brindar asesoría informática a las diferentes dependencias, a efecto de lograr implantar diferentes tipos de sistemas para las actividades que se realizan.
- Contribuir al mejoramiento continuo de procesos y programas.
- Brindar soporte técnico a los departamentos de la municipalidad, en cuanto al uso del equipo informático.
- Mantener actualizada la mecanización posterior de cada uno de los sistemas.
- Capacitación en software y hardware que la institución posee.
- Instalación de Software de configuración en servidores de producción.
- Subir a la página WEB Institucional información proporcionada por el Oficial de Acceso a la Información.

SOPORTE TÉCNICO/

Técnicos Colaboradores

- Mantenimiento preventivo y correctivo a equipos de informática, telecomunicaciones e infraestructura de red.
- Instalación de software y registro de licencias
- Creación de programas/scripts para automatizar, estandarizar tareas de computadoras de usuario final de servidores
- Brindar asistencia técnica para solventar fallas y necesidades de informática
- Instalación y mantenimiento de infraestructura de red de datos.
- Realizar y administrar respaldos de información de forma permanente en los programas y bases de datos de uso operacional
- Investigar especificaciones técnicas, costos y proveedores de equipos de informática, telecomunicaciones.
- Establecer enlaces de datos en edificios municipales
- Instalación y configuración de equipos de Seguridad Institucional.



IV. INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.

IMPACTO DE ÁREA	AFECTA
Interrupción de funciones de la persona ausente	Todas las áreas
Posible Pérdida de Hardware y software, Administración de bases de datos Control y monitoreo de servidores. Soporte a los usuarios. Ajustes a programas críticos en producción	Todas las áreas

RECURSOS DE CONTINGENCIAS

Se puede presentar lo siguiente:

1. Si fuera corto circuito o una interrupción de hasta 10 minutos, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda, hasta que los usuarios completen sus operaciones y apaguen los equipos. Posteriormente se apagará manualmente los servidores y UPS.
3. Cuando el fluido eléctrico de la calle se ha restablecido se procederá a encender de forma manual el UPS y servidores.
4. Si se produjera en horas no laborables una interrupción del fluido eléctrico, se podrían paralizar los procesos de cierre y backup de los servidores con motores de base de datos.
5. Por tal motivo es necesario revisar continuamente el estado de las baterías del UPS. Dichas baterías deben garantizar una autonomía de aproximadamente media hora.
6. Es necesario que el CAM este pendiente de la alarma que emita el Centro de Datos y de aviso al personal de Informática, esto se da cuando la temperatura se eleva a más 28°, es donde falla uno de los aires o en caso de corte de energía.



V. PERDIDA DE SERVICIO INTERNET.

IMPACTO DE ÁREA	ACCIÓN CORRECTIVA
Interrupción de la recepción y envío de información, mensajes y datos a nivel nacional e internacional, falla interna de red.	Revisar los servicios del servidor de dominios que estén levantados y el router este dando las señales respectivas
Si la falla del servicio de Internet es causado por el proveedor de servicios.	Mantener comunicación con el ejecutivo, para reporte de daño y establecer el tiempo de recuperación del servicio. Si el tiempo es prolongado, mantener un servicio alterno para cubrir falla en donde sea requerido, además de activar una red inalámbrica móvil.

RECURSOS DE CONTINGENCIAS

Hardware 1 entrada LAN
Software
Herramientas de Internet.
Backup de las reglas del servidor Firewall.

VI. INDISPONIBILIDAD DEL CENTRO DE CÓMPUTO (DESTRUCCIÓN DEL CUARTO DE SERVIDORES)

IMPACTO DE ÁREA	AFECTA
Caída de la Red LAN: Servidores Windows y Linux, equipos de comunicación	Todas las áreas
Interrupción de las comunicaciones Internas y Externas	Todas las áreas
Paralización de los sistemas que soportan las funciones de la Institución	Todas las áreas
Paralización de operaciones de Informática	Todas las áreas
Perdida de Hardware y Software	Unidad de Informática



RECURSOS DE CONTINGENCIAS GENERALES

Router (Proveído por el proveedor de Internet).

Servidores y Equipos de Comunicación (Switchs, Antenas, Fibra, etc.).

Gabinete de Comunicaciones y Servidores.

Materiales y herramientas para cableado estructurado cat 6. UPS Backup de los Sistemas.

Instaladores de las aplicaciones, de Software Base, Sistema Operativo, Utilitarios, etc.

RECURSOS DE CONTINGENCIAS ESPECÍFICOS

a. Hardware:

- 3 Servidores Intel® Xeon® E5-2600 mínimo, con 2 discos de 2TB, 16 GB RAM, con unidad de dvd, mouse, teclado, monitor.
- 3 switch de 48 puertos 10/1000 POE
- 3 caja de cable UTP cat 5e
- 500 conectores RJ45,hembras-machos
- 1 UPS de 1,5KV
- 1 Router
- Cajas y Canaletas

b. Software y Data:

- Server Ubuntu 16
- Posgret 9
- Apache tomcat 7
- Windows server Std 2012 R2 x64
- Backup de las Bases de Datos.
- Backup de las fuentes de la Aplicación.

RECURSOS DE INFRAESTRUCTURA ALTERNA

Espacio Físico:

Para este escenario, se requiere acondicionar un ambiente alterno que pueda ser utilizado como sala de servidores en el momento de la contingencia. Con un espacio mínimo de 5.5 m2 que tiene forma rectangular para facilitar la ubicación de los equipos y mobiliario.

CAPITULO IV:

IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA

Las personas que intervienen en la ejecución del plan de contingencia, es el personal de Informática, en Coordinación con Gerencia General, el personal Técnico de Informática es el responsable de emitir la alarma de la falla e iniciar las actividades para la ejecución de la contingencia, con apoyo del equipo en su totalidad.

4.1 Plan De Recuperación Y Respaldo De La Información

Actividades previas al desastre, se consideran las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Municipalidad. Se establecen los procedimientos relativos a:

a. Sistemas de Información

La Municipalidad cuenta con una relación de los Sistemas de Información de software de datos, para backups y de documentos importantes.

b. Equipos de Cómputo

Se debe tener en cuenta el esquema de red dentro los edificios donde se encuentra el equipo PC, impresoras, scanner, modems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- **Pólizas de seguros comerciales**, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- **Señalización o etiquetamiento de las computadoras** de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante.

- **Mantenimiento actualizado del inventario** de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la entidad.

c. Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

Almacenamiento de Backups de los Datos y de estructura de datos (Bases de Datos, Índices, tablas de validación, contraseñas, usuarios, roles y todo archivo necesario para el funcionamiento del Sistema SIMUS y la pronta recuperación de los mismos en caso de fallas).

4.2. Plan de Verificación

Para el Plan de Contingencia es muy importante y es conveniente que una autoridad independiente aplique las pruebas de verificación. Para sistemas de menor importancia, la verificación puede realizarse internamente.

Las pruebas de verificación (también conocidas como pruebas de calidad) pueden incluir:

- Probar los equipos bajo condiciones que simulen las de operación real.
- Probar los programas para asegurar que se siguen los estándares apropiados y que desempeñan las funciones esperadas.
- Asegurar que la documentación sea la adecuada y esté completa.
- Asegurar que los sistemas de comunicación se adecuen a los estándares establecidos y funcionen de manera efectiva.
- Verificar que los sistemas sean capaces de operar bajo condiciones normales, pero también bajo potenciales condiciones inesperadas.
- Asegurar que se cuente con las debidas medidas de seguridad.

4.3. Plan (Acciones Correctivas Y Preventivas)

→ Los que afectan a la seguridad del edificio.

Preparar extinguidores, organizar las señales de evacuación, preparar bombas de extracción de agua, generadores eléctricos, etc.

→ Los que afectan la integridad de los datos. Instalar: firewalls, antivirus, sistemas de monitoreo de entrada y salida de archivos, implantar seguridad de ingreso a los centros de manejo de información, etc.

→ Topología de Red. Preparar planos de la topología, tener equipos de repuestos de la red, herramientas necesarias todo esto en lugar de fácil acceso.

→ Copias de Seguridad: se realizarán de la siguiente manera: Al final de cada día la información, es decir la base de datos Municipal, es copia en un disco extraíble y en servidor de backup interno. Esto permite salvar la información, en caso de ruptura parcial o total, de uno o ambos servidores, o de la propia base de datos. Además, existe una copia que es enviada a un servidor externo ubicado en oficinas Externas de la municipalidad preparada especialmente para dicho fin, esta operación se realiza cada fin de semana, y también se realiza una copia en un disco extraíble a CD-ROM, para archivar definitivamente. Esta ultima copia, que se realiza en forma mensual, podría ser emitida por duplicado, para que de esta manera, se pueda archivar una dentro de la Municipalidad y otra fuera de la misma. De este modo la Institución se asegura de que en caso de robo dentro de los edificios, se cuente con otra copia de la información de la Municipalidad. La restauración de la información, disminuye los tiempos de inactividad, en caso de rupturas parciales o totales de uno o ambos servidores o de las bases de datos, dado a que se



cargaría el CD-ROM con el backup del día, o del mes (según corresponda) y se instalarían nuevamente los sistemas operativos en los terminales y de red, para levantar la contingencia.

- ➔ Extinguidores: Mantenerlos cerca de los edificios y uno cercano al centro de datos

CAPITULO V.

DISTRIBUCIÓN DEL PLAN DE CONTINGENCIA

Distribuir el plan de contingencia a todos los empleados de la Municipalidad. Además, realizar una lista con los nombres, teléfonos y direcciones, de las personas encargadas de llevar adelante dicho plan. En caso de modificarse el plan de contingencia, actualizar todas las copias de cada uno de los empleados, con la posterior destrucción de la copia anterior, para unificar la información.

CAPITULO VI.

MANTENIMIENTO DEL PLAN DE CONTINGENCIA

Realizar periódicamente un informe sobre el plan de contingencia, teniendo en cuenta las posibles modificaciones que se pudieran hacer. Se recomienda también lo siguiente:

- a.** Verificar los procedimientos que se emplearan para almacenar y recuperar los datos (backup).
- b.** Comprobar el correcto funcionamiento del disco extraíble, y del software encargado de realizar dicho backup.
- c.** Realizar simulacros de incendio, capacitando al personal en el uso de los extinguidores;



caída de sistemas o fallas de servidores, para la medición de la efectividad del plan de contingencia.

EL INFRASCRITO SECRETARIO MUNICIPAL,-----

CERTIFICA: Que en el Acta Número **CUATRO**, Sesión Ordinaria, celebrada por el Concejo Municipal de esta ciudad, el día veintitrés de enero de 2018, se encuentra el **ACUERDO** que literalmente dice: "-----"**ACUERDO NÚMERO DOS:** Presentados que han sido por el Gerente General y la Gerente de Informática de esta Institución, el Manual de Procedimientos de Informática, Plan de Contingencia de Informática y el Manual de Política de Seguridad de Informática, a efecto de generar la normativa que permita proteger los equipos informáticos, las Tecnologías de Información y los Sistemas Informáticos, que a su vez dichos Manuales serán un mecanismo, para establecer los casos de responsabilidad administrativa, en cuanto a los servidores públicos que tengan a su cargo, cuidado y custodia los equipos en referencia, según lo establecen las Normas Técnicas de Control Interno Específicas, el Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación, de las Entidades del Sector Público; en tal sentido solicitan aprobación y autorización de los manuales y Plan según detalle:

1. Manual de Procedimientos de Informática.
2. Plan de Contingencia de Informática.
3. Manual de Política de Seguridad de Informática.

Este Concejo **ACUERDA:** Tener por recibida la presentación de los Manuales y Plan antes detallados, presentados por los Funcionarios en referencia, en consecuencia se aprueban en todas y cada una de sus partes, para su respectiva aplicación Institucional, instruyendo a la Gerencia de Informática, para dar cumplimiento y seguimiento a la presente resolución. La votación del presente acuerdo queda unánime. **COMUNIQUESE.**

ES CONFORME A SU ORIGINAL, CON EL CUAL SE CONFRONTÓ.

Alcaldía Municipal de Soyapango, a los veintiséis días del mes de enero del año dos mil dieciocho.



Licdo. Santos Vidal Ascencio Bautista.
Secretario Municipal.