

**I. MUNICIPALIDAD DE TOME
SECRETARÍA MUNICIPAL**

MAT. : Aprueba "Plan de Contingencia para el Área Informática."

TOME, 22 MAR. 2018

ESTA ILUSTRE MUNICIPALIDAD DECRETO HOY LO SIGUIENTE:

2326

Nº _____/

VISTOS:

Estos Antecedentes:

- a) El Ord. N° 498 de fecha 07/11/2017, que informa cumplimiento de meta por PMG 2017.
- b) El documento que contiene el "Plan de Contingencia para el Área Informática".
- c) Las facultades que me otorga la Ley N° 18.695, Orgánica Constitucional de Municipalidades, cuyo Texto Refundido, Coordinado, Sistematizado y Actualizado fue fijado mediante el Decreto con Fuerza de Ley N° 1 de fecha 09 de Mayo de 2006, y sus modificaciones posteriores.

D E C R E T O:

- I. Apruébase el **Plan de Contingencia para el Área Informática**, el cual regula los distintos procedimientos ante eventos que alteren el normal funcionamiento de la red computacional, red telefónica, sistemas de respaldo de datos y seguridad e integridad de las bases de datos.
- II. El presente **Plan de Contingencia para el Área Informática**, tendrá vigencia de un año a contar de la fecha del presente decreto, debiendo este Plan ser actualizado al final de dicho año de vigencia.

**ANOTESE, COMUNIQUESE Y ARCHIVESE.
(FDO.) MARISSA MACCHIAVELLO GOLDBERG, ALCALDESA SUBROGANTE.
EDUARDO HENRIQUEZ SALINAS, ABOGADO, SECRETARIO MUNICIPAL.**

Lo que transcribo para su conocimiento y fines.



**EDUARDO HENRIQUEZ SALINAS
ABOGADO
SECRETARIO MUNICIPAL**

Distribución:

- Sr. Eduardo, Henriquez Salinas, Abogado, Secretario Municipal.
- cc. Manuel Quinteros Concha, Jefe de Planificación Presupuestaria e Informática, de SECPLA.
- cc. Sr. Francisco Lazcano Pizarro, Encargado de Sistemas e Informática, de SECPLA.
- cc. Sr. Patricio Parra Fuentealba, encargado de Soporte Computacional, Telecomunicaciones y Seguridad Informática, de SECPLA.
- cc. Archivo SECPLA:

MMG/EHS/WCR/MQC/FGLP/fglp.-



Secretaría Comunal de Planificación
Planificación Presupuestaria e Informática
Sistemas e Informática

ORD.: N° 498 /

ANT.: Programa de Mejoramiento de la Gestión
Municipal Período 2017.

MAT.: informa y remite lo que indica.

TOME, 07 Nov 2017

DE: WILLIAM CRUZ REYES
SECRETARIO COMUNAL DE PLANIFICACIÓN

A : SR. LUIS ASTUDILLO LIRA
DIRECTOR DE CONTROL

- I. Conforme a lo señalado en el antecedente, informo a Ud. que, como parte del cumplimiento de objetivo específico de gestión N° 2.8 **“Elaborar un Plan de Contingencia Informático Para el Nuevo Edificio Municipal”** y para el Programa de Mejoramiento de la Gestión 2017, ésta SECPLA coordinó y desarrollo, en conjunto con los profesionales de la oficina de informática, un Plan de Contingencia, el cual se encuentra materializado en documento adjunto.
- II. Lo anterior, para su conocimiento y fines.

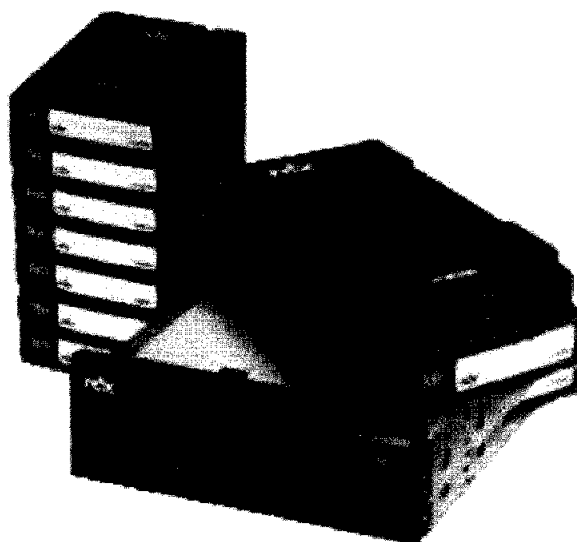
Cordial y atentamente saluda a Ud.

WILLIAM CRUZ REYES
SECRETARIO COMUNAL DE PLANIFICACIÓN

Distribución:

- Sr. Luis Astudillo Lira, Director de Control.
- cc. Sr. José Quinteros Concha, Director de Administración y Finanzas.
- cc. Sr. Ricardo Ulloa Mora, Jefe de Personal, de la Dirección de Administración y Finanzas.
- cc. Sr. Manuel Quinteros Concha, Jefe de Planificación Presupuestaria e Informática, de SECPLA ✓
- cc. Secretaría SECPLA.

WCR/MQC/FGLP/fglp.-



ILUSTRE MUNICIPALIDAD DE TOME PLAN DE CONTINGENCIA PARA EL ÁREA INFORMÁTICA

Tomé, Noviembre del 2017.-

Introducción.

Actualmente, la Ilustre municipalidad de Tomé cuenta con un nuevo edificio consistorial de cinco pisos y modernas oficinas equipadas con equipos computacionales acorde a las exigencia de un municipio que atiende alrededor de más de 52.000 habitantes, telefonía IP, red computacional de alta velocidad, un potente servidor de aplicaciones y base de datos, un servidor de respaldo de bases y servidores de respaldo base de datos municipal y respaldo de datos de usuario, un servidor de correos electrónicos, un servidor de página web, un cortafuegos y centros de comunicaciones de datos en cada piso del edificio consistorial y edificio fiscal .

Por otra parte, el edificio consistorial cuenta con oficinas cubiertas con los siguientes elementos contra riesgos:

- a) Sensores de humo
- b) Cámaras de vigilancia
- c) Extintores por cada piso
- d) Portones eléctricos
- e) Sistema de altoparlantes

Finalmente, el presente informe, basado en un exhaustivo diagnóstico de los riesgos presentes en la red computacional, establecerá los protocolos necesarios para actuar frente a contingencias tales como incendios, robos de la base de datos, sismos, etc.

Cinco grandes temas serán abordados en el presente documento, los que generarán los protocolos de seguridad y recuperación de software y datos:

- a) Riesgos de tipo eléctrico, cortes de energía.
- b) Riesgos por inundaciones
- c) Riesgos por incendios.
- d) Riesgos por robo o alteración de datos.
- e) Recurso humano disponible para el resguardo de la red computacional municipal y cumplimiento del plan de contingencia y protocolos.

I. Riesgos de tipo eléctrico, cortes de energía.

Para una organización de tipo municipal, los cortes de energía eléctricos ponen en alto riesgo la continuidad de los procesos de atención de público, sean estos generadores de ingresos o no para el municipio, como ser:

- Emisión de permisos de circulación vehicular, vía software interno y vía web.
- Emisión de licencias de conducir, vía software interno.
- Entrega de subsidios familiares y agua potable, vía web.
- Entrega de atenciones sociales, vía software interno.
- Recepción de pagos de parte de los contribuyentes, vía software interno.
- Derechos de feria, cementerios, extracción de residuos domiciliarios vía software interno y,
- Otros procesos generadores de información para distintos organismos como Intendencia, Contraloría General de la República, entre otras.

a) Protocolos a seguir para riesgos de tipo eléctrico, cortes de energía.

Este ítem menciona los protocolos necesarios a manejar en caso de que se produzca un corte de luz en edificio Consistorial o sector de edificio fiscal, con el objeto de mantener la mejor autonomía para funcionamiento o cierre de procesos en caso de corte prolongado; ya que se reconoce la importancia de poder privilegiar el funcionamiento de los equipos municipales, con especial énfasis en la atención de público y de servicios vía WEB.

La tabla de la página siguiente indica los actuales protocolos que se aplican en caso de que un proceso sea afectado por un corte de energía.

TABLA DE PROCESOS V/S PROTOCOLOS

PRINCIPALES PROCESOS DEPENDIENTES DEL SUMINISTRO ELECTRICO				
PROCESO	IMPORTANCIA	EQUIPAMIENTO QUE REQUIERE ENERGIA ELECTRICA CONSTANTE	PROTECCION ACTUAL	PROTOCOLO QUE ACTUA EN CASO EN CASO DE CORTE DE ENERGIA ELECTRICA
SISTEMAS MUNICIPALES	Programas que proporciona los sistemas arrendados a la empresa SMC, mediante la red, hacia los computadores personales municipales para atención de público en los diversos procesos administrativos y de atención de público, tal como: Sistema de Contabilidad, Remuneraciones, Patentes, Adquisiciones, Licencias, Personal, entre otros.	Servidor de aplicaciones Red municipal Computadores personales Rack por piso	Generador de energía eléctrica Ups en centros de comunicación Ups en equipos de atención de público	Actúa generador luego de 15 segundos Ups protege apagado Autonomía – ver tiempo y apagar equipos
PROCESOS DE ENTREGA DE SERVICIOS VIA WEB	Algunas unidades entregan sus servicios a través de páginas web de diversos organismos públicos y privados, tal como: registro social de hogares, sernac, mercado público, banco de proyectos, cotizaciones, correos electrónicos, búsquedas web, entre otros	Servidor de aplicación Red municipal Computadores personales Línea internet de Entel (externo) Equipos de Entel Rack por piso	Generador de energía eléctrica Internet respaldada, con velocidad baja, que provee Entel Ups en servidores Ups en centros de comunicación	Actúa generador luego de 15 segundos
USOS DE EQUIPOS PARA EFECTOS ADMINISTRATIVOS	Los computadores personales municipales contienen los software y datos municipales para soportar los sistemas municipales, internet, datos, programas de diseño, programas de bases de datos, correos electrónicos, entre otros	Servidores aplicación Red municipal Computadores personales. Servicio internet de entel (externo) Equipos de entel Rack por piso	Generador de energía eléctrica Ups en centros de comunicación Actúa ups en algunos equipos de atención de público Sistema de respaldo de internet	Actúa generador luego de 15 segundos Actúa ups de algunos computadores personales.

SERVIDORES DE SISTEMAS MUNICIPALES Y RED, SERVIDORES WEB Y CORREO ELECTRONICO	Los servidores son los equipos fuentes que administran y soportan la administración de los sistemas municipales, el correo electrónico y página web, sin los cuales no se podrían ejecutar los servicios de atención de público y de uso administrativo.	Servidor de aplicación Red municipal Computadores personales Servicio internet de entel (externo) Equipos de entel Rack por piso	Generador de electricidad Ups por centro de comunicación Ups en servidores web y correo Sistema de respaldo de internet Soporte externo	Actua generador luego de 15 segundos Actua ups de algunos computadores personales Actua ups de servidores web y correo Actua ups de centros de comunicación
UNIDADES DE RESPALDO DE SERVIDORES Y UNIDADES DE RESPALDO DE COMPUTADORES PERSONALES	Los servidores de respaldo es un equipamiento que tiene como función tener una copia de los datos y software municipales; además de los respaldos locales que contienen los principales datos alojados y respaldados por los usuarios, tal como documentos word, excel, jpg, autocad, entre otros, en caso de pérdida de información	Servidor de aplicación Red municipal Servidores de respaldo y computadores personales. Servicio internet de entel (externo) Equipos de entel Rack por piso	Generador de electricidad Ups	Actua generador luego de 15 segundos
CIRCUITO DE REDES E INTERNET	Para el traslado de los servicios de propiedades de red, de internet, y usos de sistemas, este municipio tiene una red administrada por piso y guiada desde el data center, hacia los rack por piso y estos distribuidos a cada computador; los cuales requieren contar con electricidad para su funcionamiento.	Rack por piso Servicio internet de entel (externo) Equipos de entel	Generador de electricidad Ups por centro de comunicación	actua generador luego de 15 segundos ups, funcionan 20 min promedio

b) Medidas a considerar.

Dado lo anterior, considerar que existe, como parte del protocolo, un circuito de protección eléctrico, que comprende un generador o equipo electrógeno, el cual funciona levantando el suministro eléctrico, incluyendo el de la red computacional, luego de 10 segundos, en edificio consistorial, que protegerá el equipamiento computacional que esté conectado en sistema de conexión enchufes MAGIC, por lo cual las medidas consideradas, luego de expuesta esta matriz, son:

- b.1 Verificar regularmente que las UPS de soporte de equipos están conectadas al servicio de alimentación eléctrica respaldada por el generador.
- b.2 Los computadores que son alimentados con UPS, tienen la capacidad de funcionar hasta 20 minutos aproximadamente, lo que dará tiempo a que el generador inicie su funcionamiento y levante el suministro eléctrico.
- b.3 Los usuarios cuyos equipos estén respaldados por UPS y, que no están conectadas al servicio de alimentación eléctrica del generador, tendrán 20 minutos para apagar los equipos.
- b.4 Realizar un catastro de todos los equipos municipales del edificio consistorial que requieran ser cambiados a la red MAGIC que está conectada al sistema de respaldo del generador.

c) Funcionamiento y Contingencia en Data Center Municipal

El Centro de Datos (Data Center) es un espacio físico que alberga el centro de comunicaciones y datos de todos los sistemas municipales y, está específicamente acondicionado para albergar equipamiento informático como ordenadores, equipos de red, sistema de almacenamiento, etc.

Dentro de las posibles eventualidades de catástrofe que perjudiquen este centro de datos se pretende describir el mejor plan de contingencia para que el sistema siempre este en óptimas condiciones y no sufra una pérdida para el usuario final quien utiliza el servicio día a día.

A continuación y, a través de la siguiente tabla comparativa Funcionamiento v/s Contingencia, se señalan los protocolos respectivos para cada caso.

Tabla Comparativa Funcionamiento v/s Contingencia en Data Center

Dependencia	Actualidad	Problema	Contingencia (protocolo)	Estado
Data Center	Servidor SMC Municipal	Corte de Corriente	UPS	Funcionando
		Respaldo de Datos	Servidor de Respaldo	Funcionando
Data Center	Servidor Municipal	Corte de Corriente	UPS	Funcionando
		Respaldo de Datos	Respaldo NAS	Implementando
Data Center	Central Telefonía IP	Corte de Corriente	UPS	Funcionando
		Respaldo de Datos	ENTEL	Funcionando
Data Center	Servidor WEB	Corte de Corriente	UPS	Funcionando
		Respaldo de Datos	Respaldo NAS	Implementando
Data Center	Servidor Correo	Corte de Corriente	UPS	Funcionando
		Respaldo de Datos	Respaldo NAS	Implementando
Data Center	Servidores NAS	Corte de Corriente	UPS	Funcionando
		Respaldo de Datos	Respaldo HDD	Funcionando
Data Center	Router	Corte de Corriente	UPS	Funcionando
		Respaldo de Datos	ENTEL	Funcionando
Data Center	Centro de Datos	Corte de Corriente	UPS	Funcionando
		Seguridad Acceso	Llaves	Funcionando
		Incendio	Extintor y Detector de Humo	Implementando
		Vigilancia	Cámaras	Implementando

d) **Funcionamiento y Contingencia en la Red Municipal**

La red está conformada con un enlace de Fibra Óptica Mono-modo 9um de 6 Hilos repartida en 6 Racks distribuidos en los pisos del edificio, conectándose con el Data Center quien posee los Servidores y el servicio de Internet. La Conexión de Fibra será directamente en los Switches a través de los puertos SFP con el Adaptador Transceiver la cual estará configurada de manera Troncal.

Se segmentó la red en Vlan correspondientes para Administrar de manera más segura el ancho de banda, configurada en cada Switch, en Forma de Acceso con su respectiva Puerta de Enlace, así se optimizan los recursos de la Red.

En la siguiente tabla se muestra el estado de la contingencia para optimizar y atenuar el margen de error mejorando el servicio de conectividad en el municipio.

Tabla Comparativa Funcionamiento y Contingencia en la Red Municipal

Dependencia	Actualidad	Problema	Contingencia (protocolo)	Estado
Municipalidad	Firewall	Corte de Corriente	UPS	Funcionando
		Falla Hardware	Equipo de Respaldo	Implementando
Municipalidad	Switch CORE	Corte de Corriente	UPS	Funcionando
		Falla Hardware	Equipo de Respaldo	Funcionando
Municipalidad	Switch PoE	Corte de Corriente	UPS	Funcionando
		Falla Hardware	Equipo de Respaldo	Funcionando
Municipalidad	Transceiver SFP	Corte de Corriente	UPS	Funcionando
		Falla Hardware	Equipo de Respaldo	Implementando

e) Funcionamiento y Contingencia en la Telefonía IP Municipal

En servicio de Telefonía IP que está implementado en la ilustre Municipalidad de Tomé utiliza los recursos de la Red Municipal para optimizar el servicio hacia todos los usuarios brindando varias facilidades en tecnología moderna como lo es en la actualidad.

Consta con diversos modelos de teléfonos que destacan en su diversa administración y servicio para el usuario, esta tecnología simplifica la gestión centralizada en equipamiento unificando todo en el Centro de Datos para un mejor desempeño. Estos teléfonos constan con una conexión a la red el cual se interconectan hacia una central administrada por el proveedor del servicio.

En el siguiente cuadro describe la actualidad y la contingencia para un mejor y seguro servicio.

Tabla Comparativa Funcionamiento y Contingencia Telefonía IP Municipal

Dependencia	Actualidad	Problema	Contingencia (protocolo)	Estado
Municipalidad	Requerimientos de Telefonía	Gestión y Administración	Supervisión de Informática	Funcionando
		Reconfiguración	Informática y ENTEL	Funcionando
Municipalidad	Teléfonos IP	Problema del Equipo	Informática y ENTEL	Funcionando
		Falla Configuración	Informática y ENTEL	Funcionando
Municipalidad	MPLS	Problema Hardware	ENTEL	Funcionando
		Falla Configuración	ENTEL	Funcionando

II. Riesgos por Inundaciones

Si bien el municipio no cuenta con equipamiento delicado susceptible de recibir agua producto de una salida moderada del mar, este estudio considera también como inundación aquella causada por la rotura de cañerías cercanas al equipamiento computacional, las que se indican en las siguientes ubicaciones:

1. Sala de Data Center – Edificio Consistorial
2. Sala de Data Center, servidor de respaldo de base de datos – Edificio fiscal
3. Centros Eléctricos del 1ro al 5to piso – Edificio Consistorial
4. Equipos Computacionales del 1ro al 5to piso – Edificio Consistorial
5. Equipos Computacionales de edificio Fiscal – 1ro y 2do piso

Como medida primordial para establecer un protocolo de seguridad en este aspecto, es necesario señalar que se cuenta con los planos de tipo “As Built” (o de cómo realmente se ejecutó la construcción del edificio consistorial) de las redes de aguas y con la ubicación de las llaves principales de paso de agua potable.

Por lo anterior, el protocolo de seguridad a ejecutar, en el caso de inundaciones, será el siguiente:

1. Producido el flujo de agua que de origen a una inundación y que afecte los equipos computacionales y centros de comunicaciones, se debe dar aviso inmediatamente al Encargado del Edificio Consistorial, quien ejecutará las acciones necesarias tanto para cortar el suministro de agua como de electricidad en el sector afectado.
2. Posteriormente, se dará aviso a los usuarios de la red del sector afectado que, durante el tiempo que sea necesario, no funcionará la red computacional hasta que sea controlado el evento. Una vez controlado y reparados los daños que se hayan producido, se pondrá en funcionamiento la red.

III. Riesgos por incendios

Frecuentemente, el origen de este tipo de riesgo se origina por las siguientes causas:

- a) Sobrecalentamiento de circuitos y equipos eléctricos
- b) Presencia de elementos combustibles indebidamente aislados o cerca de equipamientos eléctricos
- c) Equipos eléctricos a los que no se les ha realizado regularmente mantención o limpieza.

Por otra parte y, antes de establecer un protocolo de carácter preventivo y correctivo, se mostrará en la página siguiente una matriz de puntos críticos afectados a riesgos por incendios.

Matriz de estado y seguridad de puntos críticos de la red computacional.

Para este caso, nos referiremos a los puntos críticos como aquellos sujetos a riesgos por incendios. La matriz siguiente revelará que en dichos puntos críticos existe mayormente tecnología, de naturaleza eléctrica e informática, que debería quedar protegida. Para cada caso se indicará si existe algún elemento de tipo preventivo o no.

Dependencia	Respaldo Eléctrico	Respaldo Base de Datos	Seguridad Contra Incendios	Cámara de Vigilancia	Aire acondicionado	Cantidad de equipos eléctrico
Sala Servidor Base de Datos 4º Piso Edificio Consistorial	UPS autonomía hasta 3 horas	Respaldo: Sí Documentado: No Cortafuegos: Sí	Extintor: Sí (vigente), falta asegurar en pared. Puerta Sala: No permite visibilidad Detector Humo: No	No	Sí	06
Sala Servidor de Respaldo de Base de Datos Edificio Fiscal Sector Correos de Chile	UPS autonomía hasta 1 hora	Respaldo: Sí Documentado: No	Extintor: Sí (vigente) Puerta Sala: No permite visibilidad Detector Humo: No	No	Sí	03
Centro de Comunicaciones 1º Piso Edificio Consistorial	UPS autonomía hasta 1 hora	No Aplica	Extintor: Sí (vigente) Puerta Sala: No permite visibilidad Detector Humo: No	No	No	02
Centro de Comunicaciones 2º Piso Edificio Consistorial	UPS autonomía hasta 1 hora	No Aplica	Extintor: Sí (vigente) Puerta Sala: No permite visibilidad Detector Humo: No	No	No	04
Centro de Comunicaciones 3º Piso Edificio Consistorial	UPS autonomía hasta 1 hora	No Aplica	Extintor: Sí (vigente) Puerta Sala: No permite visibilidad Detector Humo: No	No	No	04
Centro de Comunicaciones 4º Piso Edificio Consistorial	UPS autonomía hasta 1 hora	No Aplica	Extintor: Sí (vigente) Puerta Sala: No permite visibilidad Detector Humo: No	No	No	04
Centro de Comunicaciones 5º Piso Edificio Consistorial	UPS autonomía hasta 1 hora	No Aplica	Extintor: Sí (vigente) Puerta Sala: No permite visibilidad Detector Humo: No	No	No	04

Protocolo de cómo actuar en caso de incendio en los sectores señalados en matriz anterior.

Dar aviso inmediato al encargado del edificio, quien tomará las acciones que correspondan, como ser:

- Corte del suministro de energía del sector comprometido por el incendio.
- Evacuación del personal cercano al sector comprometido por el incendio.
- Aviso al cuerpo de bomberos.

IV. Riesgos por robo o alteración de datos.

Se entenderá por robo o alteración de datos a aquel que signifique la sustracción mediante copia ilegal, hackeo u otro tipo de intrusión que afecten tanto los datos contenidos en los computadores personales, medios de respaldo de propiedad del municipio como a la base de datos municipal. Lo anterior de acuerdo a lo especificado en el texto de la ley N° 19.223 publicada con fecha 07 de Junio del 1993, la cual tipifica en sus artículos las figuras penales relativas a la informática.

Ahora, independiente al carácter legal del presente capítulo, se establecerán los protocolos para cada caso.

a) Protección de datos y protocolos de recuperación en general.

Actualmente se cuenta con una amplia gama de datos contenidos en los discos de los equipos computacionales y, estos, dependiendo del tipo de equipamiento, se indican en la siguiente tabla, la cual contiene a su vez el protocolo de recuperación:

Equipamiento	Ubicación	Datos contenidos	Protocolo de recuperación de datos y configuraciones
Servidor de base de datos y softwares de aplicación municipal	Sala Servidor Central 4° piso edificio consistorial	Base de datos, softwares de aplicación municipal, Sistema Operativo y configuraciones, respaldos diarios de la base de datos municipal.	<p>Base de Datos: Se recupera desde disco portátil desconectado de la red computacional (en primera instancia), de disco de equipo computacional que almacena los últimos cinco respaldos (en segunda instancia).</p> <p>Sistema Operativo, software de aplicaciones y configuraciones: Se ejecuta por parte de la oficina de informática (en primera instancia) Se ejecuta por parte del proveedor (en segunda instancia)</p>

Servidor de respaldo de la base de datos municipal.	Sala Servidor de respaldo 1° piso Sector edificio fiscal (costado oficinas URBEP)	Respaldo diarios Base de datos, Sistema Operativo y configuraciones	<p>Respaldo Base de Datos: Se recupera desde disco de respaldo del servidor central (en primera instancia), de disco portátil desconectado de la red computacional. (en segunda instancia), de disco de equipo computacional que almacena los últimos cinco respaldos (en tercera instancia) y de discos portátiles almacenados en caja fuerte, (en última instancia).</p> <p>Sistema Operativo y configuraciones: Se ejecuta por parte de la oficina de informática (en primera instancia). Se ejecuta por parte de servicio técnico especializado (en segunda instancia)</p>
Unidades de respaldo de datos de usuarios	Sala Servidor de respaldo 1° piso Sector edificio fiscal (costado oficinas URBEP)	Respaldo de datos de usuarios (Word, Excel, power point, autocad y otros archivos generados por software autorizado (licenciado)	<p>Datos de usuario: Se ejecuta por parte de la oficina de informática (en primera instancia).</p> <p>Sistema Operativo y configuraciones: Se ejecuta por parte de la oficina de informática (en primera instancia). Se ejecuta por parte de servicio técnico especializado (en segunda instancia).</p>
Firewall (cortafuegos)	Sala Servidor Central 4° piso edificio consistorial	Configuraciones de: Permisos de acceso a páginas web, Denegaciones	<p>Configuraciones: Se ejecuta por parte de la oficina de informática (en primera instancia). Se ejecuta por parte de servicio técnico especializado (en segunda instancia)</p>
Equipos computacionales	<ul style="list-style-type: none"> • Edificio consistorial • Sector Bodega Municipal • Sector Edificio Fiscal (Costado Correos de Chile) 	<p>Datos de equipos computacionales y configuraciones.</p> <ul style="list-style-type: none"> • Datos y configuraciones del servidor central • Datos y configuraciones del servidor de respaldo de base de datos municipal • Datos y configuraciones de unidades de respaldo • Configuraciones de Firewall • Datos y configuraciones de equipos computacionales 	<p>Configuraciones y datos: Se ejecuta por parte de la oficina de informática (en primera instancia). Se ejecuta por parte de servicio técnico especializado (en segunda instancia)</p>

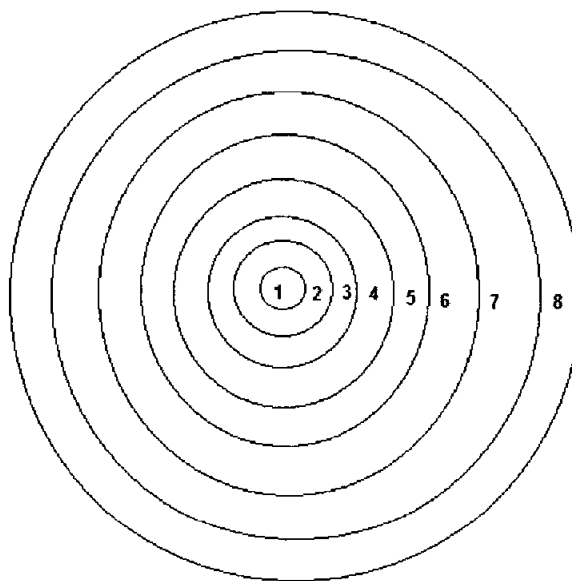
b) Base de datos municipal.

A modo ilustrativo, la siguiente tabla muestra los datos generados y contenidos en la base de datos desde Mayo del 2005, por los sistemas de aplicación municipal que se enuncian en un orden no relevante:

Sec.	Sistema	Datos Contenidos
01	Contabilidad Gubernamental	Todas las contabilidades anuales desde el 05/2005
02	Conciliación Bancaria	Todas las Conciliaciones Bancarias desde el 05/2005
03	Tesorería	Todos los giros e ingresos desde el 05/2005
04	Remuneraciones	Todas las remuneraciones desde el 05/2005
05	Adquisiciones, Bodega y Bienes	Todas las compras, por órdenes de compra interna desde mayo del 2005, se comienzan a incluir las órdenes de portal mercado público, desde el 2011 en adelante.
06	Rentas y Patentes Comerciales	Todos los registros de contribuyentes, registros de las diferentes entidades comerciales de la comuna y que generan ingresos para las arcas municipales, desde el 05/2005 en adelante.
07	Licencias de Conducir	Todas las Licencias de conducir y licencias históricas (renovaciones y primeras licencias entregadas) desde el 05/2005.
08	Permisos de Circulación Vehicular	Todos los permisos de circulación vehicular entregados desde el 05/2005
09	Personal y Licencias Médicas	Todas las licencias médicas y datos de personal ingresados desde el 05/2005, incluyendo la asistencia y otros antecedentes.
10	Organizaciones Comunitarias	Todos los registros históricos desde antes del 05/2005.
11	Atención Social	Todos los registros de atenciones sociales desde el año 2008.
12	Juzgado de Policía Local	Todas las causas desde el 05/2005

Niveles de seguridad de respaldo de la base de datos municipal.

El diagrama siguiente permite mostrar los niveles, de carácter ascendente, de los respaldos de la base de datos municipal. A continuación de dicho diagrama, se detallarán los distintos niveles y se indicará en qué punto se produce la desconexión (en términos físicos) del respaldo de la base de datos, de la red física de comunicaciones.



Descripción de los niveles de seguridad y protocolo de recuperación de la base de datos

- Nivel 1: Respaldo histórico de la base de datos dentro de sí misma: la base de datos municipal contiene el registro de todos los datos desde el mes de mayo de año 2005. Lo anterior significa y, a modo de ejemplo, que un usuario puede consultar sus liquidaciones de sueldo o las contabilidad gubernamental de cualquier época, desde la fecha antes indicada. La base de datos se aloja en el disco principal del servidor junto al sistema operativo.
- Nivel 2: Copia de la base de datos en el disco de tipo "espejo" (reflejo del disco principal) del servidor computacional central. Este disco, aunque físicamente visible, no lo es a nivel de sistema operativo. Sin embargo, la copia de la base de datos ubicada en el disco "espejo" se actualiza simultáneamente con la base de datos original. Un daño de tipo físico o eléctrico del uno de los discos, dará la posibilidad de retirar el disco dañado sin provocar la detención del servidor computacional central y, por ende, de los procesos críticos del municipio, como lo son los de atención de público.
- Nivel 3: Respaldo semanal (siete copias diarias) de la base de datos comprimida en formato RAR, en un segundo disco del servidor computacional central.
- Nivel 4: Copia del respaldo semanal de la base de datos en otro disco de tipo "espejo" (reflejo automático del segundo disco) del servidor computacional central.
- Nivel 5: Respaldo de la base de datos comprimida en formato RAR, en un quinto disco del servidor computacional central. Los respaldos se van acumulando de modo que siempre se eliminará el respaldo más antiguo para no copar la capacidad del quinto disco.
- Nivel 6: Respaldo de la base de datos comprimida en formato RAR, en un servidor destinado exclusivamente para ello. Dicho servidor tiene conectado un disco portátil, el cual al completarse, es enviado a resguardo en una caja fuerte ubicada fuera del edificio consistorial.
- Nivel 7: Respaldo de la base de datos comprimida en formato RAR, de los últimos cinco días, en el disco duro de uno de los equipos computacionales de la oficina de informática.
- Nivel 8: Respaldo descrito en nivel 7 se copia manualmente en disco portátil y que posteriormente es resguardado en una caja fuerte ubicada fuera del edificio consistorial. Es en este nivel en donde se produce la desconexión en términos físicos, del respaldo de la base de datos. Se agrega a este nivel, una copia del respaldo realizada manualmente por el Encargado de Sistemas e Informática.

Dependiendo de cada caso enunciado anteriormente y, como parte del protocolo a seguir, se ejecutará el siguiente paso previo:

- Aviso mediante informe escrito, a la Jefatura de Informática. En dicho informe se deberá:
 - Relatar lo ocurrido.
 - Solicitar se haga la denuncia que corresponda al caso y,
 - Incluir la firma y el nombre del responsable del informe.

V. Funcionamiento y contingencia de Cortafuegos (Firewall).

Se define a este dispositivo como un equipo computacional que permite realizar las siguientes funciones:

1. Preservar nuestra seguridad y privacidad.
2. Para proteger la red computacional municipal.
3. Para tener a salvo la información almacenada en nuestra red, servidores y computadores.
4. Para evitar intrusiones de usuarios no deseados en nuestra red y ordenador. Los usuarios no deseados tanto pueden ser hackers como usuarios pertenecientes a nuestra misma red.
5. Para evitar posibles ataques de denegación de servicio.

Ante una contingencia por posible falla del actual cortafuegos instalado y funcionando en la red computacional del Municipio, se ha definido el siguiente plan de acción, a ejecutar por la oficina de informática.

1. Adquisición de un cortafuegos de respaldo para, en caso de falla del cortafuegos original, sea reemplazado por el equipo de respaldo.
2. Traslado o copia de las reglas de denegación y permisos del cortafuegos y puesta en marcha del equipo de respaldo.

VI. Recurso Humano disponible para el resguardo de la Red Computacional Municipal y cumplimiento de los planes de contingencia y/o protocolos.

Los siguientes funcionarios de la Ilustre Municipalidad de Tomé estarán a cargo del cumplimiento de los planes de contingencia y protocolos:

Nombre funcionario	Profesión	Cargo
Manuel Quinteros Concha	Ingeniero Civil Químico	Jefe de Planificación Presupuestaria e Informática.
Francisco Lazcano Pizarro	Ingeniero (E) En Gestión Industrial	Encargado de Sistemas e Informática
Patricio Parra Fuentealba	Técnico Programador	Encargado de Soporte
Gregory Alarcón Reyes	Ingeniero en Conectividad y Redes	Apoyo Informático

VII. Consideraciones Finales.

Se establece que el presente documento deberá ser actualizado cada un año, a contar del mes de Diciembre del año en curso. Ello considerando que:

- Se debe documentar, durante el plazo de menos de un año, el proceso de respaldo de la Base de Datos Municipal.
- Posibles actualizaciones a la red computacional y los equipos que la componen.
- Procesos de especialización que pueda afectar al recurso humano a cargo de la ejecución del presente plan.
- Posible desarrollo de un plan informático para la Ilustre Municipalidad de Tomé.

<u>Índice</u>	Pág.
Introducción	02
I. Riesgos de tipo eléctrico, cortes de energía	03
Protocolos a seguir para riesgos de tipo eléctrico, cortes de energía	03
Medidas a considerar	06
Funcionamiento y Contingencia en Data Center Municipal	06
Funcionamiento y Contingencia en la Red Municipal	08
Funcionamiento y Contingencia en la Telefonía IP Municipal	09
II. Riesgos por Inundaciones	10
III. Riesgos por Incendios	11
IV. Riesgos por robo o alteración de datos	13
Protección de datos y protocolos de recuperación en general	13
Base de datos municipal	15
V. Funcionamiento y contingencia de Cortafuegos (Firewall)	17
VI. Recurso Humano disponible para el resguardo de la Red Computacional	
Municipal y cumplimiento de los planes de contingencia y/o protocolos	18
VII Consideraciones Finales	18