Puente Alto
MUNICIPALIDAD DE PUENTE ALTO

ADMU / SEMU/ DICON/ DAJ/INF/ogz.

PUENTE ALTO, 31 DIC 2014

VISTOS: 1969

Las atribuciones que me confiere la Ley Nº18.695, Orgánica Constitucional de Municipalidades; Ley Nº18.575 Sobre Bases Generales de la Administración del Estado; Ley Nº19.880 Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado.

CONSIDERANDO:

1.- Que Contraloría General de la República, en su **Informe Final Nº2** de 2014, Sobre Auditoría Integral en la Municipalidad de Puente Alto, relacionada con los macroprocesos de finanzas, ingresos propios, recepción y/ o entrega de transferencias, adquisición y abastecimiento, concesiones, recursos humanos, entrega de beneficios, tecnologías de la información y comunicación, funciones institucionales y procedimientos , y auditorías a los contratos en etapa de ejecución, imputados bajo la **codificación contable 215 -31 .02 – 004 Obras Civiles**, formuló diversas observaciones a los mismos, los que ameritaban una determinada reacción de parte de esta Corporación Edilicia, a objeto de subsanar las mismas en tiempo y forma.

2.- Que en lo referente al macroproceso de tecnologías de la información y comunicación (TI), se observaba que no obstante que este Municipio cuenta con procedimientos informales de mantención preventiva de los servidores municipales, no existiría una política de adquisición y/o arrendamiento de sistemas informáticos, ni de licencias de software como tampoco de inversión en equipamiento.

3.- Que asimismo se observa que si bien el Municipio cuenta con un plan de contingencia, tal instrumento no se encuentra formalizado mediante decreto alcaldicio.

4.- Que no obstante que mediante **Decreto Exento Nº1626** de fecha 12 de Noviembre del 2013, este Municipio procedió a licitar el servicio que comprendía las materias antes mencionadas, dicho proceso por **Decreto Exento Nº213** de fecha 11 de Febrero del 2014, fue declarado sin adjudicar por cuanto ninguno de los oferentes participantes cumplía con los requerimientos mínimos exigidos en las Bases de Licitación.

5.- Que sin perjuicio de que se está trabajando institucionalmente en la elaboración de un Plan Integral Municipal, que abarcaría la totalidad de los macroprocesos relacionados con esta Corporación Edilicia, a objeto de dar debida respuesta a las aludidas observaciones de Contraloría General de la República, se ha estimado pertinente sancionar formalmente nuestro Plan de Contingencia, en el que se han incorporado las materias señaladas en el Considerando Segundo precedente de este Decreto.

APRUEBESE EL SIGUIENTE PLAN DE CONTINGENCIA Y POLITICAS DE SEGURIDAD TECNOLÓGICA DE LA MUNICIPALIDAD DE PUENTE ALTO.

PLAN DE CONTINGENCIA MUNICIPALIDAD DE PUENTE ALTO

Actualización diciembre de 2011

RESUMEN EJECUTIVO

El presente documento muestra el trabajo realizado en la Ilustre Municipalidad de Puente Alto, en materia de la continuidad del negocio, para lo cual se ha realizado un plan de contingencia en el departamento de informática, que permitirá a la institución estar preparada para las eventuales amenazas, ya sea de tipo criminales o no criminales.

Para la elaboración del plan de contingencia fue necesario estudiar el modelo a utilizar para llevar a cabo dicho plan. El modelo que se ha utilizado es el BS 7799 que es una norma que nos ayudara a identificar, administrar y minimizar la gama de amenazas a las cuales está expuesta regularmente la información. También fue necesario realizar un estudio detallado de la realidad actual de la municipalidad en ámbito informático, como por ejemplo ver si existían políticas de seguridad, áreas de seguridad, niveles de acreditamiento BS 7799, planes de contingencia.

Una vez realizado el diagnóstico de la actualidad de la municipalidad, fue necesario hacer una análisis de cuáles eran las amenazas a las cuales se ve expuestas la información y todos los recursos que están relacionados, para esto se definió un perímetro al cual se acotó el estudio. Otro punto visto fue la identificación de las soluciones para las posibles contingencias que puedan existir.

Para llevar a cabo el plan de contingencia, primero se hicieron políticas de seguridad, las cuales no existían en la institución. Después realizamos un estudio de lo que era un plan de contingencia, de la forma en que se aplicaría o cuales eran los pasos a seguir para realizarlo. Por último fue necesario realizar reuniones en las que se definieron los equipos de trabajo y la participación de cada trabajador del departamento de informática.

INDICE DE CONTENIDOS

INTRODUCCION

La información es la sangre de todas las organizaciones y puede existir de muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o electrónicamente, ilustrada en películas, o hablada en conversaciones. En el ambiente competitivo de hoy en los negocios, esa información está constantemente bajo la amenaza de muchas fuentes, que pueden ser internas, externas, accidentales o maliciosas. Con el incremento del uso de nueva tecnología para almacenar, transmitir y recobrar información, nos hemos abierto a un mayor número y tipos de amenazas.

Hoy en día la tecnología con la que se cuenta, permite que las grandes y Pequeñas compañías manejen gran cantidad de información, la cual pasa a ser indispensable para su existencia, lo que lleva a convertir dicha información en algo muy preciado. Durante años, la función de la información dentro de la empresa se ha considerado por parte de las altas autoridades como una herramienta que brinda apoyo a las funciones operativas. Esta perspectiva tiende a cambiar radicalmente con el paso del tiempo, dándole otro enfoque. En la actualidad la información traspasa fronteras y pasa a ser como ·áreas de oportunidad para las empresas u organizaciones, para lograr ventajas en el ·ámbito de los negocios, ya que Éstos pueden representar un diferencial o un valor agregado con respecto a los competidores. Es por eso que la información es un bien que tiene una importancia incalculable para las empresas, esto ha llevado a que se trabaja cada día en buscar métodos, tecnología y herramientas que ayuden a mantenerla protegida de distintos ataques o danos a la que se ve sometida constantemente.

La información cuenta con tres pilares esenciales, que permiten que sea útil y trascendente para que las organizaciones logren sus objetivos. Estos son disponibilidad, confidencialidad e integridad. Es muy importante que toda información que se maneja este siempre disponible en el caso de ser requerida, por el contrario no estar- colaborando al cumplimiento de los objetivos organizacionales. Pero también a esto se agrega la confidencialidad que tiene que tener toda información, lo cual quiere decir que esta debe ser cuidada y no puede estar al alcance de cualquier persona, ya que puede ser mal utilizada. El último pilar nos indica que la información tiene que ser integra, es decir, que al momento de ser requerida tiene que estar en su totalidad para ser ocupada, porque si ha sido alterada ya no es información útil.

Los tres pilares presentado en el párrafo anterior, hoy en día se ven en constantes amenazas, lo que lleva a poner en peligro la información que administran las organizaciones y a su vez la continuidad del negocio, es por eso que los especialistas en el tema, han realizado estudios para lograr que estos pilares no sean afectados, es por eso que nace una idea que es llamada plan de contingencia.

Podríamos definir a un plan de contingencias como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

El plan de contingencia es una herramienta que ayudará a que los procesos críticos de la empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados o de otro tipo. Es decir, un plan que le permite a los negocios u organizaciones, seguir operando aunque sea al mínimo. Los objetivos de los planes de contingencia son:

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.

- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

En estos días existen muchas organizaciones que se ven afectada por la perdida de su información, muchas veces esto puede llevar a que tengan que dejar de operar sin tener la posibilidad de volver a restituirse, todo esto se debe por no poseer herramientas como planes de contingencias que ayuden a la continuidad del negocio en casos de catástrofe.

OBJETIVOS GENERALES

Construir un plan de contingencia para el departamento de informática de la Ilustre Municipalidad de Puente Alto, que ayude a la continuidad de sus labores en el caso que ocurran continencias por diferentes tipos de amenazas.

OBJETIVOS ESPECIFICOS

- Estudiar las tecnologas existentes y los métodos que ayuden a la Construcción y puesta en marcha de los planes de contingencia.

- Hacer un estudio detallado de la estructura y la actualidad con la que operan todos los sistemas y recursos informáticos de la municipalidad.

- Desarrollo de herramientas administrativas de seguridad Como políticas de Seguridad y plan de acción.

MARCO TEORICO

AMBITO DEL PROBLEMA

Para llevar a cabo de nuestro trabajo hemos realizado un estudio detallado sobre lo que son los planes de contingencia, como se pueden aplicar, cual es la norma que los regula y de qué forma nos ayudaran a dar solución a los problemas. También realizamos un estudio detallado de la actualidad de la municipalidad.
Al momento de comenzar con el estudio se ha podido percibir que el tema de plan de contingencia no existe y las medidas de seguridad son básicas. Por otro lado no existen políticas de seguridad y un á rea especializada en la seguridad informática.
Como se ha visto, en la Ilustre municipalidad de Puente Alto, en lo relacionado con la seguridad informática y especialmente con lo que es un plan de contingencia, es que estos temas aún no están implementados. Por lo tanto tendremos que realizar un estudio de la actualidad de la organización, ver cuál es el -rea en la que se centrara es estudio, de qué forma implementaremos el plan de contingencia y cuales serán las actividades para la implementación.

IDENTIFICACION DE LAS FASES DEL PLAN

FASE 1: FORMALIZAR EL PERÍMETRO

Definir el ámbito de aplicación del sistema de gestión de la seguridad de la información, esto quiere decir que tendremos que definir donde se aplicara este plan de contingencia y que es lo que queremos proteger.

DEFINICION DE PERIMETRO

En la cuadro 1 describimos cuales son las cosas que queremos proteger, la descripción y la importancia que tiene.

Nº	Nombre	Descripción	Importancia
1	Sala de Servidores	La sala de servidores, hace referencia a la parte física de los servidores, es decir el lugar donde están ubicados.	Alta
2	Servidores	Se cuenta con distintos tipos de servidores, los cuales dan servicio como: servidor de dominio, de prueba, de antivirus, bases de datos, de usuarios, de permiso de circulación.	Alta
3	Servicio Técnico	Lugar donde se hace la mantención a los equipos, como PCs e impresoras.	Alta
4	Sistemas de información	Existen distintos tipos de sistemas que se prestan servicio a los departamentos municipales como: sistema de tesorería, cobranza, remuneraciones, personal, adquisiciones, entre otros.	Alta
5	Bases de Datos	Para guardar la información de los sistemas de información se requieren distintas bases de datos.	Alta
6	Redes	La LAN de la municipalidad, que está compuesta por distintos dispositivos de red como es el caso de routers, switch, hub, Firewear, también tenemos el cableado de la red.	Alta
7	Departamento de Informática	El lugar físico donde está ubicado el departamento de informática.	Alta

Cuadro 1

DESCRIPCIÓN DEL PERÍMETRO

A continuación en el cuadro 2, se muestra porque queremos proteger el área, información o sistema señalado en el cuadro 1, como también la importancia que tiene dentro de la municipalidad.

Nº	Nombre	Amenazas	Detalle Importancia
1	Sala de Servidores	Proteger de ataques maliciosos de personas externas o internas a la municipalidad, también es necesario protegerla de desastre no intencionados como, incendios, inundaciones, derrumbes, etc.	Tiene una alta Importancia porque es el lugar físico en donde se encuentran los servidores de toda la LAN municipal.
2	Servidores	Protegerlos de robos, ataques de hacker y virus. También se tiene que proteger del fallo que pueda tener la parte física de los servidores, es decir el hardware, esto puede ser por recalentamiento de algún dispositivo, final de la vida útil de dichos dispositivos, etc. El otro fallo que pueden tener es la parte lógica, es decir el software, esto se puede deber al término de la licencia, falta de actualización, entre otros.	La importancia que tienen los servidores dentro de toda la organización es muy alta, ya que entregan servicio a todos los departamentos de la municipalidad. Sin el perfecto funcionamiento de estos servidores, los distintos departamentos no podrían realizar sus tareas.
3	Servicio Técnico	Puede sufrir perdida de equipos por robos, recalentamiento de algún equipo lo que puede provocar incendio, también en el lugar físico puede haber algún tipo de inundación.	A esta área se le ha catalogado con una importancia alta, porque los equipos (PC), que ahí se reparan pueden tener información muy importante, que si se llega a dañar puede ocasionar algunos problemas, como pérdida total de la información.
4	Sistemas de información	Las amenazas a las cuales se pueden ver afectados los sistemas	Dentro de la municipalidad existen muchos sistemas, que son ocupados por distintos

		Informáticos pueden ser por ingresos no autorizados, caída del sistema, errores en algún procedimiento, mal utilización por parte de los usuarios, caída del servidor de bases de datos, adulteración de alguna aplicación.	departamentos los cuales tiene una importancia muy alta, ya que son necesarios para el desarrollo de las tareas que realizan los departamentos. Al momento de que falle algún sistema se verá resentida una parte de la organización.
5	Bases de Datos	Una de las cosas más llamativas por los criminales informáticos son las bases de datos, ya que estas contiene información muy importante para las organizaciones y de las cuales pueden sacar mucho provecho, es por eso que esta es la amenaza más grande que pueden tener las bases de datos, los hacker.	Se le ha dado una importancia alta, ya que el funcionamiento de los sistemas depende en gran medida de las bases de datos, ya que es aquí donde se registran todos los datos que se ingresan en los sistemas. Si una base de dato es adulterada o robada esto provocara una gran pérdida en la organización.
6	Redes	Las redes pueden tener diferentes tipos de amenazas, como por ejemplo desperfecto o robo de un dispositivo de red, cortes en el cableado de la red, ya sea de forma intencional o casual.	Es necesario que la red funcione correctamente, es por eso que tiene una alta importancia, ya que si los equipos (PCs), están desconectados de la red, ya sea por cortes, no podrán tener acceso a los servicios que esta presta.
7	Departamento de Informática	En el departamento de informática se puede ver afectada por distintas amenazas, como incendios, inundaciones, derrumbes, robos externos e internos.	Tiene una importancia muy alta, ya que es aquí donde está ubicada la sala de servidores, servicio técnico y el área de soporte. Es importante tener protegidos el departamento de distintas amenazas a las cuales se puede ver expuesto.

Cuadro 2

Nota: en la columna amenazas del cuadro 2 aparecen descritas las posibles amenazas que pueden tener las áreas, información, equipos, sistemas o servicios, en forma superficial, es decir a grandes rasgos, ya que, en la Tarea 2 de la Fase 3 se describen con mayor detalle.

FASE 2: POLITICAS DE SEGURIDAD

GENERALIDADES:

1. Los activos de información y los equipos informáticos son recursos importantes y vitales para la institución. Sin ellos no se podrían lograr los objetivos institucionales y por tal razón el alcalde y los directores o jefes de departamentos tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información esté libre de amenazas y riesgos tales como fraude, sabotaje, espionaje, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

2. La información perteneciente a la municipalidad debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar como la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o como se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

3. A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos inform·ticos de la Municipalidad. Debe hacerse hincaplé en que la seguridad informática es una actividad tan vital para la institución como lo son las otras areas

4. Los usuarios que no cumplan alguna de las políticas deben pasar al comité de seguridad que analizara su situación.

SOBRE LOS USUARIOS:

5. Los usuarios son responsables de cumplir con todas las políticas de la institución relativas a la seguridad informática y en particular:
a. Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
b. No divulgar información confidencial de la municipalidad a personas no autorizadas.
c. No permitir y no facilitar el uso de los sistemas informáticos de la Municipalidad a personas no autorizadas.
d. No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la municipalidad.
e. Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
f. Seleccionar una contraseña robusta que no tenga relación obvia con

el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
g. Reportar inmediatamente a su jefe directo o a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la municipalidad y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

SOBRE LOS EQUIPOS (PCS):

6. Los computadores de la municipalidad solo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
7. Los equipos de la municipalidad solo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
8. Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática.
9. No se permite fumar, comer o beber mientras se está- usando un PC.
10. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
11. Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
12. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la municipalidad se requiere una autorización escrita.
13. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
14. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto.

SOBRE LA INFORMACION:

15. Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.
16. Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario. Los privilegios que se darán serán para los sistemas computacionales de los distintos departamentos.
17. No está- permitido llevar al sitio de trabajo computadores portátiles y en caso de ser necesario se requiere solicitar la autorización correspondiente.

18. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la municipalidad está- protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

19. Los usuarios no deben copiar a un medio removible (como un diskette, pendriver, CDs, etc.), el software o los datos residentes en las computadoras de la municipalidad, sin la aprobación previa de los jefes.

20. No pueden extraerse datos fuera de la sede de la municipalidad sin la aprobación previa de los directores. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o est·n conectados a redes como Internet.

21. Debe instalarse y activarse una herramienta de antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

22. Solo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la municipalidad.
23. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.
24. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el Departamento de Informática.
25. No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la municipalidad a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
26. Los respaldos de la información de los equipos de los usuarios, debe hacerse en un período de tiempo definido por el jefe de cada departamento y el jefe de informática. Este respaldo tiene que tener dos copias, una para el jefe del departamento y la otra para el departamento de informática.

Ley N^ 17.336 sobre Propiedad Intelectual. Artículo 3^, inciso 16.

27. Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los Directores de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal).
28. Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad.
29. El personal que utiliza un computador portátil que contenga información confidencial de la municipalidad, no debe dejarla abandonada.

SOBRE LA COMUNICACION:

30. Con el fin de mejorar la productividad, la municipalidad promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la municipalidad y no propiedad de los usuarios de los servicios de comunicación.
31. Los sistemas de comunicación de la municipalidad generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la municipalidad.
32. Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
33. La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la municipalidad y en tal sentido deben usarse las horas no laborables.
34. Los empleados y funcionarios de la municipalidad no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La municipalidad se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario intercetar ciertas comunicaciones.

Ley N° 19.628 sobre la Protección de la Privacidad o de Datos de Carácter Personal

35. Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifradas. Para tal fin debe utilizarse Outlook, Outlook Express u otros productos previamente aprobados por el Departamento de Informática.
36. Tomando en cuenta que cierta información está- dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la municipalidad, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la municipalidad sin la debida aprobación.
37. Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su -rea de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

SOBRE LAS CUENTAS DE USUARIOS:

38. Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
39. La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
40. Toda cuenta queda automáticamente suspendida despuÈs de un cierto
Periodo de inactividad. El periodo recomendado es de 30 días.
41. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.
42. Cuando un empleado es despedido o renuncia a la municipalidad, debe desactivarse su cuenta antes de que deje el cargo.
43. El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
44. Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
45 Está- prohibido el uso de contraseñas de grupo para facilitar el acceso a
archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos. Esto se aplica en particular a la contraseña del administrador.

46. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

47. Los usuarios no deben intentar violar los sistemas de seguridad y de control de accesos. Acciones de esta naturaleza se consideran violatorias de las políticas de la institución, pudiendo ser causal de despido o sumario administrativo.

48. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

E Ley N^ 19.223 sobre Delitos Informáticos

FASE 3: ESTUDIO DEL PLAN DE CONTINGENCIA

SALA DE SERVIDORES

DIAGNOSTICO

Análisis del Perímetro

Temas a tratar	Diagnostico
Servicio y/o Bienes Producidos	El servicio que presta la sala de servidores, es mantener en un lugar adecuado y bajo condiciones óptimas los servidores de la municipalidad, para que ellos brinden el mejor servicio.
Servicios y/o Materiales Utilizados.	La sala de servidores utiliza los siguientes servicios: energía eléctrica y sistema de climatización.
Inventario de Recursos Informáticos	En la sala de servidores se encuentran los siguientes recursos informáticos: servidores con sus respectivos periféricos (monitor, teclado, Mouse), dispositivos de red como switch y hub, cables de red.

IDENTIFICACION DE RIESGOS Y AMENAZAS

Amenazas Criminales	Amenazas no Criminales	Servicio o areas afectadas	Importância
▯▯ Robos de equipos hechos por personas internas o externas a la municipalidad. ▯▯ Destrozo intencionado realizado por personas internas o externas. ▯▯ Corte intencionado del suministro eléctrico. ▯▯ Ataque terrorista.	▯▯ Incendio. ▯▯ Inundaciones. ▯▯ Terremotos. ▯▯ Corte de suministro eléctrico no intencionado.	▯▯ Servidores ▯▯ Sistemasinformáticos que ocupan los servidores de sistema y de bases de datos. ▯▯ Departamentos y/o usuarios que tienen acceso a los servidores, ya sea por las distintas aplicaciones que realizan.	**Alta**

SERVIDORES

DIAGNOSTICO

Análisis del Perímetro

Temas a tratar	Diagnostico
Servicio y/o Bienes Producidos	Prestan servicio a los sistemas computacionales de los distintos departamentos municipales, a las bases de datos de los sistemas, servicio de dominio, de correo, de pruebas, de antivirus, entre otros.
Servicios y/o Materiales Utilizados.	Utilizan la sala de servidores, servicio de climatización y energía eléctrica. También utiliza los dispositivos de red como switch, hub y todo el cableado.
Inventario de Recursos Informáticos	Dentro del inventario tenemos: servidores, PC que cumplen la tarea de servidor, monitores, teclados, Mouse, switch, hub, cables.

Descripción de Servidores

Nombre del Servidor	Descripción
Servidor Puente Alto (puentealto)	▯▯ Controlador de Dominio ▯▯ Servidor de archivos
Servidor Impaproxy	▯▯ Equipo Disponible (Sin uso Actualmente)
Servidor WebDatos	▯▯ Servidor de Prueba de Base de Datos Municipales ▯▯ Servidor FTP
Servidor Antivirus (kavserver)	▯▯ Presta servicio de Antivirus
Servidor Proxy (Pro)	▯▯ Servidor de servicios de Internet ▯▯ Servidor WINS
Servidor Impadatos	▯▯ Servidor Base de Datos
Servidor Licencias	▯▯ Presta servicio al departamento de transito

IDENTIFICACI''N DE RIESGOS Y AMENAZAS

Amenazas Criminales	Amenazas no Criminales	Servicio o areas afectadas	Importancia
▯▯ Robos por parte de personas internas o externas. ▯▯ Intrusión, sabotaje y robo por parte de hackers o criminales informáticos de la información que ahí	▯▯ Mal uso de los usuarios de forma casual. ▯▯ Corte del suministro eléctrico que dejan inactivos los servidores. ▯▯ Depreciación de los	▯▯ Los distintos sistemas que tiene acceso a los servidores, ya sea de bases de datos, servidor de sistema, etc. ▯▯ Usuario de los departamentos municipales que ocupan	**Alta**

se registra. Daño físico y lógico hecho por criminales o usuarios.	dispositivos que componen elaplicaciones que están estre-servidor, como disco duro,chamente relacionados con placa madre, fuente de po- los servi-der, etc, dores. Desperfecto del hardware. Fallas en el software, estas pueden ser por errores en la compilación o por término de la licencia del software. Virus.	

SERVICIO TECNICO

DIAGNOSTICO

Análisis del Perímetro

Temas a tratar	Diagnostico
Servicio y/o Bienes Producidos	Reparación y mantención de todos los equipos informáticos como PC e impresoras. También se da respaldo de la información de PC.
Servicios y/o Materiales Utilizados.	Para el servicio que presta esta área se requiere de energía eléctrica y una sala en donde trabajar. Se ocupa también software con sus respectivas licencias para ser instalados en los PC. Otro servicio que utilizan es conexión a Internet.
Inventario de Recursos Informáticos	En el servicio técnico se cuenta con los siguientes recursos informáticos: PC con sus periféricos y software con sus licencias.

IDENTIFICACION DE RIESGOS Y AMENAZAS

Amenazas Criminales	Amenazas no Criminales	Servicio o areas Afectadas	Importancia
Robos de los equipos que ahí se reparan o repuestos de los equipos, estos robos pueden ser de personal externo o interno.	Corte del suministro eléctrico que les impide realizar el trabajo de reparación de algún equipo. Extravío de repuestos. Incendio.	Los equipos que se repararan. Usuarios que ocupan los equipos que ahí se reparan. La información contenida en los discos	

▯▯ Robo de información que manejan, como por ejemplo inventario de piezas o repuestos.	▯▯ Inundación. ▯▯ Terremotos. ▯▯ Negligencia por parte del personal técnico en la reparación de algún equipo.	duros de los equipos en reparación.	**Alta**

SISTEMAS DE INFORMACION

DIAGNOSTICO

Análisis del Perímetro

Temas a tratar	Diagnostico
Servicio y/o Bienes Producidos	Ayuda a los distintos departamentos municipales a manejar de la mejor forma posible la información que ahí se procesa. Existen distintos tipos de sistemas para los departamentos, como se muestra en el cuadro siguiente.
Servicios y/o Materiales Utilizados.	Para dar su servicio, los sistemas de información utilizan el servidor de sistemas, el servidor de bases de datos, la red LAN, conexión a Internet (en algunos casos). También es necesaria una estación de trabajo para que los usuarios puedan acceder a ellos.
Inventario de Recursos Informáticos	En el inventario tenemos los siguientes recursos informáticos: PC o estaciones de trabajo equipadas, servidor de bases de datos, servidor de sistemas, servidor Web.

Sistemas de información de la municipalidad

Nombre del Sistema	Departamentos afectados
Sistema de Contabilidad Gubernamental	▯▯ Departamento de Contabilidad ▯▯ Departamento de Adquisiciones ▯▯ Departamento de Tesorería
Sistema de Tesorería	▯▯ Departamento de Tesorería
Sistemas de Cobranzas	▯▯ Cobranza, Unidad del Departamento de Finanzas
Sistema de Remuneraciones	▯▯ Departamento de Personal ▯▯ Departamento de Contabilidad
Sistema de Personal	▯▯ Departamento de Personal
Sistema de Inventario	
Sistema de Derechos de	▯▯ Derecho de Aseo, Unidad del Departamento de Rentas

Aseo	
Sistema de Adquisiciones	▯▯ Departamento de Adquisiciones
Sistema de Bodega	▯▯ Inter dirección de Bodega
Sistema de Inspección	▯▯ Dirección de Inspección General ▯▯ Juzgado de Policía Local
Sistema de Portal de Pagos	▯▯ Dirección de Inspección General (pago de patentes comerciales) ▯▯ Departamento de Transito (pago de permiso de circulación) ▯▯ Dirección de Aseo, Ornato y áreas Verdes (pago derecho se aseo)
Sistema de Juzgado de Policía Local	▯▯ Departamento de Tesorería ▯▯ Dirección de Inspección General
Permiso de Circulación de Circulación	▯▯ Departamento de Transito ▯▯ Departamento de Tesorería
Convenios	▯▯ Departamento de Tesorería
Patentes Comerciales	▯▯ Patentes Comerciales, Unidad del Departamento de Rentas
Sistema de Social	▯▯ DIDESO, Departamento de subsidios fiscales, Aseo

IDENTIFICACION DE RIESGOS Y AMENAZAS

Amenazas Criminales	Amenazas no Criminales	Servicio o areas Afectadas	Importancia
▯▯ Ataques a la información de hacker o piratas informáticos. ▯▯ Ingreso de persona no autorizada. ▯▯ Robo de claves de ingreso a los sistemas ▯▯▯ Robo de las bases de datos de los sistemas.	▯▯ Desperfecto en el servidor de sistemas y de bases de datos. ▯▯ Mal uso por parte de los usuarios. ▯▯ Falla en el diseño y la programación de funciones o procedimientos. ▯▯ Inconsistencia de los datos. ▯▯ Fallo en los software relacionados con el sistema. ▯▯ Fallas en el equipo en el cual se está ejecutando el sistema.	▯▯ Los usuarios que trabajan directamente con los sistemas. ▯▯ Los departamentos que su trabajo se basa en el uso de algún sistema, para mayor detalle haga clic aquí. ▯▯ Información que es procesada en los sistemas.	**Alta**

BASES DE DATOS

DIAGNOSTICO

Análisis del Perímetro

Temas a tratar	Diagnostico
Servicio y/o Bienes Producidos	En las bases de datos se registra y guarda toda la información que es procesada en los distintos sistemas de información, como también entrega la información requerida por dichos sistemas, es decir, permite el acceso a la información que necesita el usuario (esto es según los permisos o privilegios que tenga el usuario).
Servicios y/o Materiales Utilizados.	Ocupa un servidor de base de datos, la LAN junto con todos sus dispositivos y el servidor de sistemas.
Inventario de Recursos Informáticos	El inventario de recursos informáticos está compuesto por: un servidor de bases de datos, software necesario con sus respectivas licencias.

IDENTIFICACION DE RIESGOS Y AMENAZAS

Amenazas Criminales	Amenazas nó Criminales	Servicio o areas afectadas	importancia
Robos por parte de piratas informáticos. Adulteración de algún dato almacenado, este robo puede ser provocado por usuarios o hacker. Robo del servidor de bases de datos. Daños intencionados al servidor de bases de datos.	Mala manipulación por parte de los usuarios. Mal diseños de las bases de datos. Desperfecto en el servidor de bases de datos. Virus que afecte al servidor de bases de datos. Falla en algún software que tenga relación con la base de datos. Inconsistencia entre el sistema y la base de datos.	Sistemas informáticos que almacenan datos en las bases de datos. Usuarios quetiene acceso a las bases de datos por intermedio de los sistemas informáticos.	**Alta**

RED LAN

DIAGNOSTICO

Análisis del Perímetro

Temas a tratar	Diagnostico
Servicio y/o Bienes Producidos	La LAN municipal tiene por finalidad entregar el servicio de conectividad entre las estaciones de trabajo (con su dirección IP), de los distintos departamentos municipales y a los servicios y recursos informáticos que se requieran, como los servidores.
Servicios y/o Materiales Utilizados.	Utiliza el cableado, dispositivos de red como switch, hub, router, Firewall. También los equipos (PC) que se conectan a ella.
Inventario de Recursos Informáticos	Dentro del inventario encontramos: PC, switch, hub, router, Firewall, cableado.

Arquitectura LAN

La figura 3 y la figura 4 muestran la arquitectura de la red municipal, con todas sus dependencias.

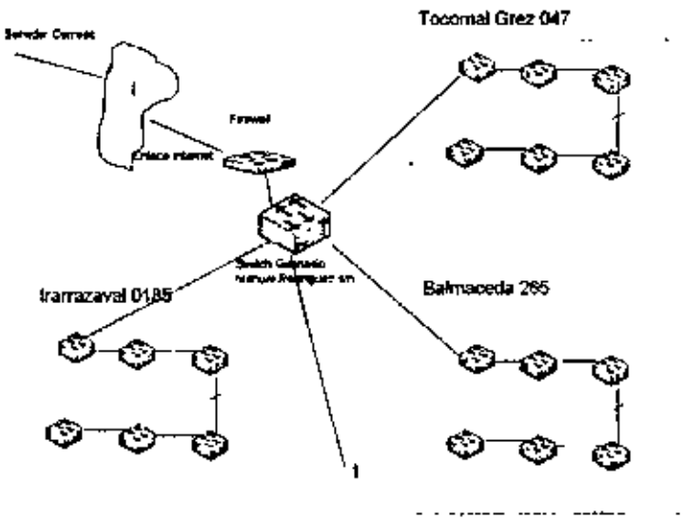

Figura 3: muestra la arquitectura de red en su primera parte

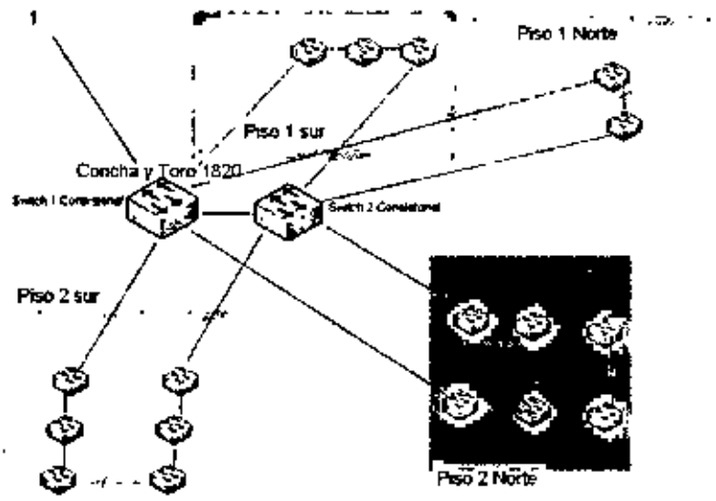

Figura 4: muestra la arquitectura de red en su segunda parte

IDENTIFICACION DE RIESGOS Y AMENAZAS

Amenazas Criminales	Amenazas no Criminales	Servicio o áreas Afectadas	Importancia
Robo en el cableado o de algún dispositivo de la red, como switch, hub, router, etc. Daños intencionados de los dispositivos de la red. Cortes intencionados del cableado de la red.	Desperfecto de los dispositivos de red. Corte casual del cableado. Mal diseño de la red. Corte del suministro eléctrico.	Servidores. Estaciones de trabajos. Sistemas informáticos. Conectividad. Usuarios. Servicio informáticos, como Internet, correo electrónico, acceso a los sistemas, etc.	**Alta**

DEPARTAMENTO DE INFORMATICA

DIAGNOSTICO

Análisis del Perímetro

Temas a tratar	Diagnostico
Servicio y/o Bienes Producidos	Entrega servicio a todos los departamentos de la municipalidad, ya sea en servicio técnico de los recursos computacionales, soporte de conectividad, desarrollo de aplicaciones computacionales, mantención y monitoreo de sistemas informáticos. También es el lugar físico donde se encuentran dispositivos de la LAN, que son importantes para la municipalidad, como servidores.
Servicios y/o Materiales Utilizados.	Utiliza un lugar físico, energía eléctrica para el funcionamiento de los equipos, conexión a Internet, equipos.
Inventario de Recursos Informáticos	En el inventario del departamento de informática tenemos: PC, servidores, software con sus licencias, conectividad.

IDENTIFICACI""N DE RIESGOS Y AMENAZAS

Amenazas Criminales	Amenazas no Criminales	Servicio o áreas Afectadas	Importancia
⊠ Daños físicos al departamento por parte de personas internas o externas. ⊠ Robo de información, equipos, etc. ⊠ Ataques terroristas.	⊠ Corte del suministro eléctrico. ⊠ Incendio. ⊠ Terremotos. ⊠ Inundaciones.	⊠ Los distintos departamentos a los cuales se les da servicio ⊠ Aplicaciones en las cuales se trabaja.	**Alta**

FASE 4: CONSTRUCCION DEL PLAN DE CONTINGENCIA

SALA DE SERVIDORES

ESTRATEGIAS

Tipo:	Amenazas:	Solución para controlar amenazas:
C	Robos de equipos hecho por personas internas o externas a la municipalidad	▯▯ Control restringido a la sala de servidores. ▯▯ Sistema de identificación y seguridad para el ingreso. ▯▯ Inventario de los equipos de la sala. ▯▯ Registro del personal que ingresa a la sala.
C	Destrozo intencionado realizado por personas internas o externas	▯▯ Cámaras de vigilancia dentro de la sala.
C	Corte intencionado del suministro eléctrico	▯▯ Usar protectores contra temporales cortes de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).
C	Ataques terroristas	▯▯ Contar con sistema de vigilancia y con cámaras de seguridad.
NC	Incendio.	▯▯ Tener en la sala un sistema contra incendio. ▯▯ Contar con extintores de incendio, los cuales deben tener una mantención adecuada para que cumplan la norma.
NC	Inundaciones.	▯▯ La sala de servidores debe estar ubicada en un lugar en el cual este fuera del alcance de las posibles inundaciones. Se recomienda que esta sala no esté en subterráneos.
NC	Terremotos.	▯▯ El lugar donde esté ubicada la sala de servidores tiene que ser una construcción sólida, si es posible construcción antisísmica.
NC	Corte de suministro eléctrico no intencionado	▯▯ Usar protectores contra temporales cortes de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).

IDENTIFICACION DE LAS SOLUCIONES

Tipo:	Amenazas o Contingencias:	Solución para el Desastre:
C	Robos de equipos hecho por personas internas o externas a la municipalidad	▯▯ Evaluar cuáles son los equipos que han sido robados y los servicios que han sido afectados. ▯▯ Remplazar rápidamente el equipo que ha sido robado. ▯▯ Ver el sistema de registro de ingresos a la sala. ▯▯ Ver la cinta de video de vigilancia para

		identificar la persona que ha robado el equipo.
C	Destrozo intencionado realizado por personas internas o externas	Realizar una evaluación de cuáles son los equipos que han sido dañados y los servicios que han sido afectados. Remplazar rápidamente el equipo que ha sido dañado si es que el daño ha dejado inhabilitado el equipo.
C y NC	Corte intencionado y no intencionado del suministro eléctrico	Revisar los tableros eléctricos. Avisar a la empresa que presta este servicio en el caso que interrupción sea por un periodo de tiempo prolongado.
C	Ataques terroristas	Hacer una evaluación rápida de los servidores afectados, para ponerlos en funcionamiento en el menor tiempo posible. Ver las cámaras de seguridad para identificar de qué lugar provinieron los ataques.
NC	Incendio.	Activar el sistema contra incendio, en el caso que Éste no sea automático. Evaluar el daño ocasionado por el incendio y ver cuales son los servidores dañados y servicios afectados, para remplazarlos en el menor tiempo posible y activar el servicio. Hacer una investigación de las causas del incendio.
NC	Inundaciones.	Activar la alarma de emergencia, para que el personal actúe con la debida rapidez. Sacar y proteger los equipos que están siendo afectado por la inundación. Evaluar rápidamente que servicios fueron afectados y que están caídos, para ponerlos en funcionamiento en el menor tiempo posible. Hacer una evaluación detallada post desastre.
NC	Terremotos.	Activar la alarma de emergencia, para que el personal actúe con la debida rapidez y con la precaución requerida. Sacar y proteger los equipos que han sido afectado. Evaluar rápidamente que servicios fueron afectados y que están caídos, para ponerlos en funcionamiento en el menor tiempo posible. Hacer una evaluación detallada post desastre.

SERVIDORES

ESTRATEGIAS

Tipo	Amenazas	Soluciones para controlar Amenazas
C	Robos por parte de personas internas o externas.	Inventario de los servidores. Acceso restringido a la sala de servidores.
C	Intrusión, sabotaje y robo por parte de hackers o criminales informáticos de la información que ahí se registra.	Sistema de seguridad informática. Mantener actualizados los antivirus. Tener un IDS (sistema de detección de intrusos), que trabaje en conjunto con el Firewall. Creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados.
C	Daño físico y lógico hecho por criminales o usuarios	En el caso de daños físicos mantener un control de acceso restringido a la sala de servidores. Para los daños lógicos es necesario tener un sistema de seguridad informática que contenga como mínimo un IDS, Firewall, actualización de antivirus.
NC	Mal uso de los usuarios de forma casual	Capacitación de los usuarios. Que los usuarios conozcan los objetivos del área en la que se desempeñan, así puedan Comprender la importancia de la información. Los usuarios tiene que estar en conocimiento de las políticas de seguridad.
NC	Corte del suministro eléctrico que dejan inactivos los servidores	Usar protectores contra temporales cortes de energía eléctrica y en los servidores deben usarse fuentes de poder interrumpibles (UPS).
NC	Desperfecto o depreciación de los dispositivos que componen el servidor, como disco duro, placa madre, fuente de poder, etc.	Tener un inventario de cada servidor con sus dispositivos, en el cual aparezca la vida útil, fechas de reparaciones o cambio de dispositivos. Realizar una mantención frecuente de los Servidores. Tener un stock necesario en el caso que ocurra algún desperfecto en los dispositivos, los cuales no tengan reparación.
NC	Fallas en el software, estas pueden ser por errores en la compilación o por término de la licencia del software	Todo software tienen que tener sus licencias al día. Tener un inventario del software que ocupa cada servidor. Mantener actualizado el software.

NC cual tiene	Virus que estar en constante actualización.	Cada servidor tiene que tener un antivirus el

IDENTIFICACI''N DE LAS SOLUCIONES

Tipo	Amenazas o Contingencias	Soluciones para el Desastre
C	Robos por parte de personas internas o externas.	Evaluar cuáles son los servidores que han sido robados y los servicios afectados. Remplazar rápidamente el servidor que ha sido robado, por otro y levantar el servicio. Ver el sistema de registro de ingresos a la sala. Ver la cinta de video de vigilancia para identificar la persona que ha robado el servidor (en el caso de que exista).
C	Intrusión, sabotaje y robo por parte de hackers o criminales informáticos de la información que ahí se registra.	Verificar con el IDS (Sistema de Detección de Intrusos), de donde provienen los ataques y que daños han ocasionado (esto se puede realizar en el caso que exista un IDS implementado. En el anexo 1 de este documento se explica lo que es un IDS y lo importante que puede resultar como alternativa de solución). Detectar que información ha sido robada, para ver la forma en que puede ser remplazada Acudir a los respaldos de la información adulterada o robada, para volver a levantar servicios.
C	Daño físico y lógico hecho por criminales o usuarios	Evaluar cuáles son los servidores que han sido dañados y la magnitud del daño ocasionado. Reemplazar o reparar el servidor que ha sido dañado, enviándolo al servicio técnico, en el caso que corresponda.
NC	Mal uso de los usuarios de forma casual	Evaluar si se ocasionado algún daño en el servidor y si han sido afectados los servicios. En el caso que los daños dejen inactivo los servidores, es necesario cambiar el servidor y montar el servicio en otro equipo.
NC	Corte del suministro eléctrico que dejan inactivos los servidores	Activar rápidamente la UPS en los servidores o los generadores de energía eléctrica (esto se realizara si es que existe este método). Avisar a la empresa que presta el servicio, para que ellos analicen las fallas y den solución al problema Analizar que ocasiono el corte y el sector que abarca.

NC	Desperfecto o depreciación de los dispositivos que componen el servidor, como disco duro, placa madre, fuente de poder, etc.	Hacer una evaluación rápida del servidor que tiene problema. Ver si el desperfecto ha provocado que el servidor deje de dar los servicios. En el caso que el desperfecto provoque que el servidor no pueda dar los servicios requeridos, habrá que repararlo o cambiarlo y montar el servicio en otro equipo.
NC	Fallas en el software, estas pueden ser por errores en la compilación o por término de la licencia del software	Verificar rápidamente de donde proviene la falla. Hacer la reinstalación del software que ha fallado. En el caso que la licencia haya caducado hay que ponerse en contacto con el proveedor de la licencia.
NC	Virus	Poner en cuarentena el equipo. Ver cuáles son los virus con el que fue afectado el servidor. Desinfectar el servidor con el antivirus adecuado o el método que sea necesario. En el caso que el daño en el servidor sea severo y deje inactivo el servidor, es necesario levantar el servicio en otro servidor.

SERVICIO TECNICO

ESTRATEGIAS

Tipo	Amenazas	Soluciones para controlar Amenazas
C	Robos de los equipos que ahí se reparan o repuestos de los equipos, estos robos pueden ser de personal externo o interno	Tener un acceso controlado y restringido. Poseer un sistema identificación para el personal del servicio técnico Tener un inventario con todos los repuestos, equipos en reparación y equipos ya reparados.
C	Robo de información que manejan, como por ejemplo inventario de piezas o repuestos	Tener un respaldo de toda la información que se considere importante. Tener la información en un lugar seguro y fuera del alcance de personas ajenas al servicio técnico.
NC	Corte del suministro eléctrico que les impide realizar el trabajo de reparación de algún equipo.	Usar protectores contra temporales cortes de energía eléctrica.
NC	Extravío de repuestos.	Mantener los repuestos en orden en un lugar adecuado, si es posible en una bodega. Tener una lista detallada de todos los repuestos.

NC	Incendio	Tener en la sala un sistema contra incendio. Contar con extintores de incendio, los cuales deben tener una mantención adecuada para que cumplan la norma.
NC	Inundación.	La sala de servidores debe estar ubicada en un lugar en el cual este fuera del alcance de las posibles inundaciones. Se recomienda que esta sala no esté en subterráneos.
NC	Terremotos.	El lugar donde esté ubicada la sala de servidores tiene que ser una construcción sólida, si es posible antisísmica.
NC	Negligencia por parte del personal técnico en la reparación de algún equipo.	El personal que ahí trabaja tiene que tener los conocimientos adecuados para la reparación de los equipos. El personal tiene que estar en perfeccionamiento.

IDENTIFICACION DE LAS SOLUCIONES

Tipo	Amenazas o Contingencias	Soluciones para el Desastre
C	Robos de los equipos que ahí se reparan o repuestos de los equipos, estos robos pueden ser de personal externo o interno	Ver cuál es el equipo o repuesto que ha sido robado. Recurrir a las cintas de grabación de vigilancia, para ver quien ha robado el equipo o repuesto. Si se ha identificado la persona que ha robado el equipo o repuesto es necesario comunicarlo a las autoridades o personal de seguridad de la municipalidad.
C	Robo de información que manejan, como por ejemplo inventario de piezas o repuestos	Recurrir a las cintas de grabación de vigilancia, para ver quien ha robado la información. Si se ha identificado la persona que ha robado la información es necesario comunicarlo a las autoridades o personal de seguridad de la municipalidad.
NC	Corte del suministro eléctrico que les impide realizar el trabajo de reparación de algún equipo.	Activar rápidamente los generadores de energía Eléctrica. Analizar de donde proviene el corte.
NC	Extravío de repuestos.	Recurrir a la bodega de repuesto y verificar si el repuesto se ha extraviado. Verificar el inventario de repuesto. En el caso de que el repuesto no se encuentre es necesario reportar la pérdida y reponerlo.
NC	Incendio	Activar el sistema contra incendio, en el caso que este no sea automático.

		⁂ Evaluar el daño ocasionado por el incendio y ver Cuáles son los equipos afectados. ⁂ Hacer una investigación de las causas del incendio.
NC	Inundación.	⁂ Activar la alarma de emergencia, para que el personal actúe con la debida rapidez. ⁂ Sacar y proteger los equipos que están siendo afectado por la inundación. ⁂ Hacer una evaluación detallada post desastre.
NC	Terremotos.	⁂ Activar la alarma de emergencia, para que el personal actúe con la debida rapidez y con la precaución requerida. ⁂ Sacar y proteger los equipos que han sido afectado. ⁂ Hacer una evaluación detallada post desastre.

SISTEMAS DE INFORMACION

ESTRATEGIAS

Tipo	Amenazas	Soluciones para Controlar Amenazas
C	Ataques a la información hecha por hacker o piratas informáticos.	⁂ Tener un IDS (Sistema de Detección de Intrusos), para todos los sistemas.
C	Ingreso de persona no autorizada.	⁂ Tener las claves protegidas.
C	Robo de claves de ingreso a los sistemas	⁂ Las claves de ingresos a los sistemas tiene que tener un método robusto, es decir, usar un método de encriptación para password.
C	Robo de las bases de datos de los sistemas	⁂ Las bases de datos tienen que ser respaldadas cada cierto tiempo, este tiempo tiene que ser definido por el jefe del departamento de informática. ⁂ Usar un método de encriptación para las bases De datos, en especial para los respaldos.
NC	Desperfecto en el servidor de sistemas y de bases de datos.	⁂ Mantención frecuente en los servidores relacionados. ⁂ Tener otros servidores en los cuales se pueda montar las bases de datos y los sistemas, en caso que fallen los servidores originales.
NC	Mal uso por parte de los usuarios.	⁂ Capacitación de los usuarios antes de usar los Sistemas.
NC	Falla en el diseño y la programación de funciones o procedimientos e inconsistencia	⁂ Si los sistemas son desarrollados en el departamento de informática, es necesario usar una metodología para el desarrollo.

	de datos.	Documentar todos los sistemas o los cambios realizados en ellos. Si los sistemas son desarrollados por empresas externar, es necesario pedir la documentación del sistema y de los cambios que se van realizando.
NC	Fallo en los software relacionados con el sistema.	Mantener actualizado el software. Tener licencia de todos los software que se ocupen, cuando corresponda.
XC	Fallas en el equipo en el cual se está ejecutando el sistema.	Los equipos tiene que estar en constante mantención Los equipos tienen que cumplir con los requerimientos mínimos para que los sistemas funcionen adecuadamente.

IDENTIFICACION DE LAS SOLUCIONES

Tipo	Amenazas o Contingencias	Soluciones para el Desastre
C	Ataques a la información, hecha por hacker o piratas informáticos e ingreso de personas no autorizadas.	Ver cuáles son los sistemas dañados y dar aviso a la empresa encargada de los sistemas. Acudir a los respaldos de la información adulterada o robada, para poner en funcionamiento el servicio. Hacer un análisis en detalle de los daños provocados y de las consecuencias provocadas.
C	Robo de claves de ingreso a los sistemas	Caducar la password que ha sido robada. Hacer un análisis de los sistemas para ver si se ha provocado algún daño.
C	Robo de las bases de datos de los sistemas	Acudir con rapidez a los respaldo de las bases de datos, para ponerlas en funcionamiento en el menor tiempo posible.
XC	Desperfecto en el servidor de sistemas y de bases de datos.	Verificar y analizar de donde proviene las fallas y que servidor ha fallado. Restablecer el funcionamiento del servidor, en el caso que el daño no permita que el servidor siga funcionando, es necesario levantar el servicio en otro servidor. Reportar los daños ocasionados por el desperfecto.
NC	Mal uso por parte de los usuarios.	Verificar en el sistema si se han provocado daños por el mal uso de los usuarios. En el caso que exista daño, es necesario reparar el daño.
XC	Falla en el diseño y la	Analizar de donde proviene la falla, qué la

	programación de funciones o procedimientos e inconsistencia de datos.	provoco y acudir a los manuales del sistema para tener claro los pasos necesarios que hay que seguir para reparar la falla. Si el sistema es desarrollado por empresas externas, es necesario avisar rápidamente para que ellos acudan a reparar la falla. Si el sistema queda inactivo, es necesario buscar otros métodos para el proceso de la información (como por ejemplo: planillas de cálculo), en el caso que el sistema esté en uso crítico.
NC	Fallo en los software relacionados con el sistema.	Verificar rápidamente de donde proviene la falla. Hacer la reinstalación del software que ha fallado. En el caso que la licencia haya caducado hay que ponerse en contacto con el proveedor de la licencia.
NC	Fallas en el equipo en el cual se está ejecutando el sistema.	Evaluar qué provoco la falla y cuáles son los Daños ocasionados. El usuario del equipo debe avisar rápidamente al departamento de informática, para que envíen al personal de servicio técnico para dar solución a la falla del equipo. Si el equipo no puede ser reparado en el momento, es necesario que se le asigne otro equipo al usuario, para que continúe con sus labores sin problema.

BASES DE DATOS

ESTRATEGIAS

Tipo	Amenazas	Soluciones para Controlar Amenazas
C	Robos por parte de piratas informáticos y adulteración de algún dato almacenado.	Tener un IDS (Sistema de Detección de Intrusos). Tener un sistema de seguridad informática robusto. Poseer un método de encriptación para las Bases de datos.
C	Robo físico del servidor de bases de datos y daños intencionados.	El servidor debe estar en un lugar (sala de servidores), en donde se tenga restringido el acceso para cualquier persona. Hacer respaldo de las bases de datos.
XC	Mal diseño de las bases de datos e inconsistencia entre el	El diseño de las bases de datos debe documentarse.

	sistema y la base de dato.	Los diseñadores de las bases de datos deben estar preparados y tener los conocimientos adecuados para su diseño
XC	Desperfecto en el servidor de bases de datos.	El servidor de las bases de datos tiene que estar en constante mantención. Tener otros servidores en los cuales se pueda montar las bases de datos, en caso que falle los servidor original.
XC	Virus que afecte al servidor de bases de datos.	El servidor de bases de datos debe estar protegido por un antivirus el cual debe estar actualizado.
NC	Falla en algún software que tenga relación con la base de dato.	Mantener actualizado el software. Tener licencia de todos los software que se ocupen, cuando corresponda.

IDENTIFICACION DE LAS SOLUCIONES

Tipo	Amenazas o Contingencias	Solución para el Desastre
C	Robos por parte de piratas informáticos y adulteración de algún dato almacenado.	Analizar cuáles son las bases de datos robadas o adulteradas, para ver que servicios ha afectado y así poder actuar con rapidez. Acudir a los respaldos de la información adulterada o robada, para poner en funcionamiento el servicio. Hacer un análisis post desastre en detalle, de los daños provocados y de las consecuencias provocadas.
C	Robo físico del servidor de bases de datos y daños intencionados.	Si el servidor ha sido dañado, habrá que revisarlo y ver si los daños pueden ser reparados en la brevedad, en el caso que el daño sea mayor y deje inoperante el servidor habrá que remplazarlo. Si el servidor ha sido robado habrá que remplazar rápidamente por otro y así levantar el servicio en la brevedad. Ver el sistema de registro de ingresos a la sala de servidores. Ver la cinta de video de vigilancia para identificar la persona que ha robado el servidor. Si se ha identificado la persona que robo o daño el servidor, es necesario avisar a las autoridades o al personal de seguridad para que tome las medidas pertinentes.
XC	Mal diseño de las bases de	Analizar de cuál es la falla, qué la provoco y

	datos e inconsistencia entre el sistema y la base de dato.	acudir a los manuales del sistema para revisar el modelo de dato, para tener conocimiento de lo que hace la base de dato y así poder dar solución al problema. Si la base de dato es desarrollado por empresas externas, es necesario avisar rápidamente para que ellos acudan a reparar la falla. Si la falla en la base de dato provoca que el sistema queda inactivo, es necesario buscar otros métodos para el proceso de la información (como por ejemplo: planillas de cálculo), en el caso que el sistema esté en uso crítico.
NC	Desperfecto en el servidor de bases de datos.	Evaluar con rapidez cuál es el desperfecto, las causas que lo ocasiono y ver si han quedado inactivo los servicios. En el caso que los servicios queden inactivo, es necesario montar la base de dato en otro servidor. Reparar el servidor. Hacer un análisis de la los daños ocasionados por el desperfecto del servidor.
NC	Virus que afecte al servidor de bases de datos.	Poner en cuarentena el servidor hasta que acuda el personal de servicio técnico o el administrador de servidores. Analizar con las herramientas adecuadas el virus que ha afectado al servidor y las consecuencias que ha provocado. Reparar los daños provocados por el virus. Si el daño es mayor y deja el servidor inactivo por un tiempo inestimable es necesario levantar el servicio de bases de datos en otro equipo.
NC	Falla en algún software que tenga relación con la base de dato.	Verificar rápidamente de donde proviene la falla. Hacer la reinstalación del software que ha fallado. En el caso que la licencia haya caducado hay que ponerse en contacto con el proveedor de la licencia.

RED LAN

ESTRATEGIAS

Tipo	Amenazas	Solución para Controlar Amenazas
C	Robo o daños intencionados en algún dispositivo de la red, como switch, hub, router, etc.	Tener un inventario de todos los dispositivos que están conectado en la red. Tener protegidos los dispositivos de la red.
C y NC	Cortes intencionados o casual del cableado de la red.	Contar con un mapa de la red, para poder ver en qué lugar ha sido costado el cableado. El cableado tiene que ir por lugares que estén lejos del alcance de personas ajenas.
NC	Desperfecto de los dispositivos de red.	Los dispositivos de la red tiene que estar en constante mantención. Llevar un calendario con las fechas en que se han realizado las mantenciones.
NC	Mal diseño de la red.	El diseño de las redes tiene que ser por personal que tengan los conocimientos suficientes del tema o dejar en manos de empresas externas especialistas en el tema. Tener documentación de las rede.
NC	Corte del suministro electric.	Contar con generadores de corrientes en el caso de corte.

IDENTIFICACION DE LAS SOLUCIONES

Tipo	Amenazas o Contingencia	Solución para el Desastre
C	Robo o daños intencionados en algún dispositivo de la red, como switch, hub, router, etc.	Ver cuál es el dispositivo que ha sido robado o dañado. Revisar los mapas de la LAN para ver que secciones de la red se dañaron y quedaron sin servicio. Acudir donde esta dañada la red y reemplazar el dispositivo que ha sido robado. Si el soporte de la red es hecho por empresas externas, hay que avisar el desperfecto a la empresa para que acuda a reparar el desperfecto, en un tiempo corto. Recurrir a las cintas de grabación de vigilancia, para ver quien ha robado el equipo o repuesto. Si se ha identificado la persona que ha robado el equipo o repuesto es necesario comunicarlo a las autoridades o personal de seguridad de la municipalidad.
C	Cortes intencionados o casual	Ver el lugar donde se ha cortado el cableado.

NC	del cableado de la red.	Ver los mapas de la red para verificar los servicios que han sido afectados por el corte. Acudir al lugar para ver de qué forma se puede reparar el desperfecto. Si el soporte de la red es hecho por empresas externas, hay que avisar el desperfecto a la empresa para que acuda a reparar el desperfecto, en un tiempo corto
NC	Desperfecto de los dispositivos de red.	Acudir donde está el dispositivo afectado, para evaluar cuáles son las fallas y de qué forma será reparado o simplemente cambiado. En el caso que el soporte sea realizado por empresas externas, habrá que avisar a la empresa para que acuda en la brevedad a reparar el desperfecto del dispositivo.
NC	Mal diseño de la red.	Analizar cuál es la falla, qué la provoco y acudir a los mapas de la red para revisar la arquitectura de la red y así poder dar solución al problema. Si la red fue desarrollada por empresas externas, es necesario avisar rápidamente para que ellos acudan a reparar la falla.
NC	Corte del suministro eléctrico.	Activar rápidamente los generadores de energía eléctrica. Analizar de donde proviene el corte.

DEPARTAMENTO DE INFORMATICA

ESTRATEGIAS

	Amenazas	Solución para Controlar Amenazas
C	Daños físico al departamento por parte de personas internas o externas y robos de información equipos, etc.	Tener un sistema de control de acceso restringido. Sistema de identificación de ingreso. Sistema con cámaras de seguridad o vigilancia.
C	Ataques terroristas.	Contar con sistema de vigilancia y con cámaras de seguridad.
NC	Corte del suministro eléctrico	Contar con generadores de corrientes en el caso de corte.
NC	Incendio.	Tener en el departamento un sistema contra incendio. Contar con extintores de incendio, los cuales deben tener una mantención adecuada para que cumplan la norma.

NC	Inundaciones	▯▯ El departamento debe estar ubicado en un lugar en el cual esté fuera del alcance de las posibles inundaciones. Se recomienda que no esté ubicado en subterráneos.
NC	Terremotos.	▯▯ El lugar donde esté ubicado el departamento de informática tiene que ser una construcción sólida, si es posible construcción antisísmica.

IDENTIFICACION DE LAS SOLUCIONES

Tipo	Amenazas o Contingencias	Solución para el Desastre
C	Daños físico al departamento por parte de personas internas o externas y robos de información equipos, etc. También en este punto se menciona los ataques terroristas.	▯▯ Evaluar cuáles son las áreas y los servicios que han sido afectados. ▯▯ Poner en funcionamiento en el menor tiempo posible, los servicios afectados. ▯▯ Ver el sistema de registro de ingresos al departamento. ▯▯ Ver la cinta de video de vigilancia para identificar la persona que ha provocado el daño.
NC	Corte del suministro eléctrico	▯▯ Activar rápidamente los generadores de energía eléctrica. ▯▯ Analizar de donde proviene el corte.
NC	Incendio.	▯▯ Activar el sistema contra incendio, en el caso que éste no sea automático. ▯▯ Evaluar el daño ocasionado por el incendio y ver cuáles son las áreas afectadas. ▯▯ Hacer una investigación de las causas del incendio.
NC	Inundaciones	▯▯ Activar la alarma de emergencia, para que el personal actúe con la debida rapidez. ▯▯ Sacar y proteger los equipos y la información que estén siendo afectado por la inundación. ▯▯ Hacer una evaluación detallada post desastre.
NC	Terremotos.	▯▯ Activar la alarma de emergencia, para que el personal actúe con la debida rapidez y con la precaución requerida. ▯▯ Sacar y proteger los equipos y todos los dispositivos informáticos que han sido afectados. ▯▯ Hacer una evaluación detallada post desastre.

FASE 5: PRUEBAS DEL PLAN DE CONTINGENCIA

ACTIVIDADES ANTES DEL DESASTRE

FORMACION DE EQUIPOS OPERATIVOS

Perímetro	Actividades a Realizar
Sala de Servidores	▯▯ Tener un inventario de todo el equipamiento de la sala de servidores. ▯▯ Llevar un control detallado del ingreso a la sala. ▯▯ Tener un registro de las contingencias a las cuales ha visto expuesta la sala. ▯▯ Coordinar las mantenciones periódicas de los equipos de la sala. ▯▯ Establecer y llevar a cabo procedimientos para restaurar los servicios.
Servidores	▯▯ Tener detallado los servidores con los que se cuenta, especificando sus características principales, servicios que presta y los servicios que se ven afectado en caso de fallas. ▯▯ Organizar pruebas de hardware y software de los servidores periódicamente. ▯▯ Supervisar procedimientos de respaldo y restauración. ▯▯ Ejecutar trabajos de recuperación. ▯▯ Tener un control de los respaldos hechos a los servidores, de las contingencias a las cuales se han visto expuestos. ▯▯ Realizar respaldo de información. Para el respaldo de la Información debe existir políticas.
Servicio Técnico	▯▯ Tener un inventario de todos los equipos y repuestos con los que disponen. ▯▯ Llevar un control detallado de las reparaciones que han realizado a los equipos. ▯▯▯ Tener un registro de las contingencias a las cuales ha visto expuesta la sala. ▯▯ Programar y supervisar pruebas y mantenimientos a los sistemas contra incendio, Instalaciones eléctricas.
Sistemas de Información	▯▯ 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. ▯▯ Supervisar procedimientos de respaldo y restauración. ▯▯ Supervisar la carga de archivos de datos de las aplicaciones,

	y la creación de los respaldos de la información. - Establecer procedimientos de seguridad en las aplicaciones de recuperación de desastre. - Organizar la prueba de hardware y software. - Ejecutar trabajos de recuperación. - Realizar procedimientos de control de inventario y seguridad del almacenamiento de la información - Establecer y llevar a cabo procedimientos para restaurar los servicios. - Participar en las pruebas y simulacros de desastres.
Bases de Datos	- Ponerse en contacto con los diseñadores de las bases de Datos y trabajar con ellos. - Proporcionar soporte técnico para las copias de respaldo de las bases de datos - Supervisar procedimientos de respaldo y restauración. - Supervisar la carga de datos de las bases de datos, y la creación de los respaldos. - Establecer procedimientos de seguridad en las aplicaciones de recuperación de desastre. - Organizar la prueba de hardware y software relacionados a las bases de datos. - Ejecutar trabajos de recuperación. - Realizar procedimientos de control de inventario y seguridad del almacenamiento de los datos. - Participar en las pruebas y simulacros de desastres.
Redes	- Tener los mapas de la red, junto con todos los dispositivos que la forman. - Mantener contacto con la empresa externa que presta el servicio de soporte de la red, si es que este servicio lo entrega una empresa externa. - Llevar un control de las averías y problemas que ha tenido la red. - Realizar pruebas periódicas del hardware y software de la red.
Departamento de Informática	- Tener un inventario de todos los equipos informáticos con los que cuenta el Departamento. - Planificar y Realizar periódicamente simulacros de desastre. - Llevar un control de todas las contingencias a las cuales se ha visto expuesta el departamento de informática.

FORMACION DE EQUIPOS DE EVALUACION

- Revisar que las Políticas de seguridad sean cumplidas.
- Supervisar la realización periódica de simulacros de desastre.
- Supervisar el que los responsables de cada área (Perímetro), cumplan con las actividades que deben realizar.
- Evaluar las contingencias ocurridas en cada área, viendo cuales fueron las causas, los daños provocados y si los planes de contingencia han sido de utilidad.

ACTIVIDADES DURANTE EL DESASTRE

PLAN DE ACCION SALA DE SERVIDORES

Amenaza o Contingencia	Acciones a Realizar	Función que realizará
⊠ Robos de equipos, hecho por personas internas o externas a la municipalidad. ⊠ Destrozo intencionado realizado por personas internas o externas.	1º Ver cuáles son los equipos que Han sido robados o dañados. 2º Detectar cuáles son los servicios afectados. 3º Avisar a los departamentos afectados, que los servidores estarán Interrumpidos por un periodo de tiempo. 4º Levantar el servicio en otro equipo y probar que los servicios funcionen correctamente. 5º Avisar nuevamente a los departamentos afectados que los servicios han sido restablecidos.	⊠ Tener un inventario detallado de todos los equipos de la sala, con sus características principales, servicios que presta y los servicios que se ven afectado en caso de fallo de este. ⊠ Todos los equipos tienes que tener candados de seguridad. ⊠ Tener una lista de contactos, de las personas responsable de cada departamento que los servidores prestan servicios. ⊠ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ⊠ Tener actualizada la bitácora con las fechas y horas de las entradas y salidas a la sala de servidores y el motivo por el cual entró. ⊠ Llevar a cabo el plan de acción. ⊠ Llevar un control de todas las contingencias producidas.
Corte del suministro eléctrico	1º Avisar el desperfecto a la empresa que presta el servicio. 2º Ver que los protectores contra temporales cortes de energía eléctrica y que los UPS (en el caso que existan), se han activado correctamente, en el caso que existan. 3º Ver que los servicios sigan funcionando correctamente. 4º Hacer respaldo de la información almacenada en los	⊠ Tener los números de contacto de la empresa que presta el servicio. ⊠ Poseer un inventario detallado con todos los recursos existentes. ⊠ Llevar un Informe detallado de las mantenciones realizadas a los sistemas eléctricos. ⊠ Conocer en detalle el plan de acción y tener conformado el Equipo de trabajo. ⊠ Llevar a cabo el plan de acción. ⊠ Llevar un control de todas los cortes producidos

	servidores.	
Ataques terroristas	1º Poner al tanto a las autoridades y a los usuarios que los servicios han sido dañados, por lo que no están activos y que se está trabajando en reponer los servicios en la brevedad. 2º Analizar cuáles son las magnitudes de los ataques y los daños ocasionados. 3º Ver cuáles son los servicios y áreas afectadas. 4º Reponer los servicios afectados en la brevedad, realizando las tareas necesarias.	Tener una lista de contactos con todos los organismos de seguridad. Poseer un inventario detallado con todos los recursos existentes. Conocer en detalle el plan de acción y tener conformado el Equipo de trabajo. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Incendio.	1º Cortar el suministro eléctrico. 2º Analizar las magnitudes del incendio y en el caso que corresponda avisar a bomberos para que acudan al lugar. 3º Evacuar al personal. 4º Retirar los equipos de la sala de servidores, si las magnitudes del incendio lo permiten. 5º Ver cuales son los servicios afectados y avisar a los departamentos o áreas afectadas 6º Poner en funcionamiento los servicios en una sala de emergencia.	Tener una lista de contactos con todos los organismos de seguridad. Poseer un inventario detallado con todos los recursos existentes y de los servidores más importantes. Verificar la permanencia y mantención de los extintores de incendio. Ubicar en un lugar apropiado el extintor de incendio (se recomienda fuera de la sala de servidores). Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.

Inundaciones.	1º Cortar el suministro eléctrico. 2º Retirar los equipos para evitar daños. 3º Avisar a los departamentos que han sido afectados por el fallo en los servicios. 4º Levantar los servicios en la brevedad en una sala de emergencia.	▯▯ Tener una lista de contactos con todos los organismos de seguridad. ▯▯ Detallar todos los servidores existentes y el tipo de información que manejan. ▯▯ Poseer un inventario detallado con todos los recursos existentes. ▯▯ Conocer en detalle el plan de acción y tener conformado el Equipo de trabajo. ▯▯ Llevar a cabo el plan de acción. ▯▯ Llevar un control de todas las contingencias producidas.
Terremotos.	1º Cortar el suministro eléctrico. 2º Evacuar al personal. 3º Analizar las magnitudes del terremoto y ver si se pueden retirar los equipos de la sala.	▯▯ Tener una lista de contactos con todos los organismos de seguridad. ▯▯ Poseer un inventario detallado con todos los recursos existentes, principalmente de los servidores. ▯▯ Las vías de evacuación tiene que estar bien señaladas. ▯▯ Conocer en detalle el plan de acción y tener conformado el Equipo de trabajo. ▯▯ Llevar a cabo el plan de acción ▯▯ Llevar un control de todas las contingencias producidas.

PLAN DE ACCION SERVIDORES

Amenaza o Contingencia	Acciones a Realizar	Función que Realizará
▯▯ Robos por parte de personas internas o externas.	1º Ver cuales son los servidores robados. 2º Detectar cuáles son los servicios afectados. 3º Avisar a los departamentos afectados, que los servidores estarán	▯▯ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ▯▯ Poseer un inventario detallado con todos los servidores existentes, describiendo los servicios que presta y los departamentos de la municipalidad que se verán afectados en el caso de que no puedan prestar sus servicios.

	interrumpidos por un periodo de tiempo. 4º Levantar el servicio en otro equipo y probar que los servicios funcionen correctamente. 5º Avisar nuevamente a los departamentos afectados que los servicios han sido restablecido.	▯▯ Tener una lista de contacto de todos los departamentos municipales. ▯▯ Llevar a cabo el plan de acción ▯▯ Llevar un control de todas las contingencias producidas.
▯▯ Intrusión, sabotaje y robo por parte de hackers o criminales informáticos, de la información que ahí se registra. ▯▯ Daño físico y lógico hecho por criminales o usuarios. ▯▯ Mal uso de los usuarios de forma casual.	1º Acudir a los IDS para ver cuáles son los ataques, daÒos provocados, los servicios afectados y por quien fue provocado el ataque o intrusión. 2º En el caso que los servicios han sido afectados, se deber- avisar a los departamentos que han quedado sin servicio. 3º Poner en funcionamiento los servicios, acudiendo a los respaldos, si es necesario. 4º Revisar que los servicios funcionen correctamente, después de ser restaurados. 5º Avisar a los departamentos que los servicios han sido restablecidos.	▯▯ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ▯▯ Poseer un inventario detallado con todos los servidores existentes, describiendo los servicios que presta. También debe estar detallado cuales es el nombre del servidor, el sistema operativo con el que cuenta, la informaciÛn que se guarda, los fechas de actualizaciones de la informaciÛn. ▯▯ Llevar a cabo el plan de acción ▯▯ Llevar un control de todas las contingencias producidas.
▯▯ Corte del suministro eléctrico que dejan inactivos los servidores	1º Avisar el desperfecto a la empresa que presta el servicio. 2º Ver que los protectores contra temporales cortes de energía eléctrica y que los UPS, se han	▯▯ Tener los números de contacto de la empresa que presta el servicio. ▯▯ Tener una lista de contacto con todos los departamentos municipales para dar aviso de las fallas. ▯▯ Conocer en detalle el plan de acción y tener conformado el

	activado correctamente (esto es en el caso de que existan protectores y UPS). 3º Ver que los servicios sigan funcionando correctamente. 4º Hacer respaldo de la información almacenada en los servidores.	equipo de trabajo. - Poseer un inventario detallado con todos los servidores existentes, describiendo los servicios que presta. - Llevar a cabo el plan de acción - Llevar un control de todas las contingencias producidas.
- Desperfecto o depreciación de los dispositivos que componen el servidor, como disco duro, placa madre, fuente de poder, etc.	1º Ver cuáles son los servidores afectados y evaluar los daños que tiene. 2º Detectar los servicios afectados y avisar al departamento que ha quedado sin servicio. 3º Hacer un respaldo de la información. 4º Ver cuál es la pieza que ha fallado y cambiarla, es necesario levantar el servicio en otro servidor. 5º Avisar a los departamentos afectados que los servicios se han restablecido.	- Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. - Poseer un inventario detallado con todos los servidores existentes, describiendo los servicios que presta, el hardware por el que está compuesto, vida útil del equipo. - Tener un calendario de mantenciones en que se indique la fecha se ha realizado la mantención, el motivo de la mantención y la fecha de la siguiente mantención. - Llevar a cabo el plan de acción. - Llevar un control de todas las contingencias producidas.
- Fallas en el software, estas pueden ser por errores en la compilación o por término de la licencia del software.	1º Ver cuáles son los servidores afectados y evaluar los daños que tiene, debido a la falla del software. 2º Detectar los servicios afectados y avisar al departamento que ha quedado sin servicio. 3º Hacer un respaldo de la Información.	- Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. - Poseer un inventario detallado con todos los servidores existentes, describiendo los servicios que presta, el nombre del equipo, departamentos a los que presta servicio, software que ocupa. - Tener un calendario con todas las actualizaciones del software que se le ha hecho a cada servidor y de las

	4º Reparar el defecto del software. Es necesario levantar el servicio en otro servidor. 5º Avisar a los departamentos afectados que los servicios se han restablecido.	próximas actualizaciones. - Tener todo el software que se requiere para las mantenciones o desperfecto en un lugar en que pueda ser encontrado rápidamente. - Llevar a cabo el plan de acción. - Llevar un control de todas las contingencias producidas.
- Virus	1º Poner en cuarentena el servidor. 2º Ver cuáles son los servicios afectados y avisar oportunamente a los departamentos que han quedado sin servicios. 3º Reparar el desperfecto ocasionado por el virus y levantar el servicio en otro servidor mientras el desperfecto es solucionado. 4º Una vez levantado el servicio provisorio, es necesario avisar a los departamentos afectados, que los servicios han sido restablecidos.	- Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. - Poseer un inventario detallado con todos los servidores existentes, describiendo los servicios que presta. - Tener un calendario con las actualizaciones del antivirus. - Monitorear que las actualizaciones del antivirus se haga correctamente. - Llevar a cabo el plan de acciÛn - Llevar un control de todas las contingencias producidas.

PLAN DE ACCION SERVICIO TECNICO

Amenaza o Contingencia	Acciones a Realizar	Función que Realizará
⊠⊠ Robos de los equipos que ahí se reparan o repuestos de los equipos, estos robos pueden ser del personal externo o interno. ⊠⊠ Extravío de repuestos.	1º Ver cuáles son los equipos robados o repuestos. 2º Analizar la importancia de la información contenida en el equipo robado. 3º Avisar a los guardias de seguridad de la institución, sobre el robo. 4º Acudir al respaldo de la información en el caso de que esta es imprescindible, para ser copiada en otro equipo.	⊠⊠ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ⊠⊠ Poseer el número de contactos del personal de seguridad de la municipalidad. ⊠⊠ Tener un inventario de todos los recursos con los se cuenta. ⊠⊠ Llevar un control de los equipos que ingresan y salen del servicio técnico indicando nombre del equipo, a que usuario pertenece, el tipo de informaciÛn que maneja el equipo, fecha y hora de ingreso y salida, nombre de la persona que lo ingreso y saco, arreglos que se le hicieron. ⊠⊠ Tener un sistema de respaldo de la información de los equipos que serán reparados. ⊠⊠ Guardar los respaldos en un lugar seguro. ⊠⊠ Llevar a cabo el plan de acciÛn. ⊠⊠ Llevar un control de todas las contingencias producidas.
⊠⊠ Robo o extravío de la información que manejan, como por ejemplo inventario de piezas o repuestos, registros de equipos reparados.	1º Ver cuáles son los documentos que se han sido robados y la información que estos contenían. 2º Acudir a los respaldo de la información en el caso que sea requerida. 3º Dar aviso del robo al personal de seguridad de la institución.	⊠⊠ Conocer en detalle el plan de acción y tener conformado el Equipo de trabajo. ⊠⊠ Poseer el número de contactos del personal de seguridad de la municipalidad. ⊠⊠ Tener respaldada toda la información. ⊠⊠ Tener un inventario de todos los recursos con los se cuenta. ⊠⊠ Llevar a cabo el plan de acción. ⊠⊠ Llevar un control de todas las contingencias producidas.
⊠⊠ Corte del suministro eléctrico que les impide realizar el trabajo de reparación de algún equipo.	1º Avisar el desperfecto a la empresa que presta el servicio. 2º Ver que los protectores contra temporales cortes de energía eléctrica.	⊠⊠ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ⊠⊠ Poseer el número de contacto con la empresa que presta el servicio. ⊠⊠ Tener el número de contacto con las personas encargadas

		del sistema eléctrico de la municipalidad. Llevar a cabo el plan de acciÛn. Llevar un control de todas las contingencias producidas.
Incendio	1º Cortar el suministro eléctrico. 2º Analizar las magnitudes del incendio y en el caso que corresponda avisar a bomberos para que acudan al lugar. 3º Evacuar al personal. 4º Retirar los equipos, si las magnitudes del incendio lo permiten.	Conocer en detalle el plan de acciÛn y tener conformado el equipo de trabajo. Tener una lista de contactos con todos los organismos de seguridad. Tener un inventario de todos los recursos con los se cuenta. Verificar que los extintores de incendio siempre estén con su mantención al día. Llevar a cabo el plan de acciÛn. Llevar un control de todas las contingencias producidas.
Inundación.	1º Cortar el suministro eléctrico. 2º Retirar los equipos para evitar daños	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener una lista de contactos con todos los organismos de seguridad. Tener un inventario de todos los recursos con los se cuenta. Llevar a cabo el plan de acciÛn. Llevar un control de todas las contingencias producidas.
Terremotos.	1º Cortar el suministro eléctrico. 2º Evacuar al personal. 3º Analizar las magnitudes del terremoto y ver si se pueden retirar los equipos de la sala.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener una lista de contactos con todos los organismos de seguridad. Tener un inventario de todos los recursos con los se cuenta. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Negligencia por parte del personal técnico en la reparación de algún equipo.	1º Ver cuáles son los equipos mal reparados y evaluar cuáles son los daños. 2º Cambiar las piezas defectuosas	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener un control de todos las reparaciones que se realizan y por quién fueron realizadas.

y reparar nuevamente el equipo. reparaciones de equipos en la intranet. □□ □□		□□ Tener procedimientos de para actualizaciones, de respaldo y Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.

PLAN DE ACCION SISTEMAS DE INFORMACION

Amenaza o Contingencia	Acciones a Realizar	Función que Realizará
□ □□ Ataques a la información hecha por hacker o piratas informáticos. □ □□ Ingreso de persona no autorizada. □ □□ Robo de claves de ingreso a los sistemas □ □□ Mal uso por parte de los usuarios.	1º Hacer una análisis de los sistemas que han sido dañado, para ver cuáles son los departamentos afectados. 2º Dar aviso a la empresa que presta el servicio de los sistemas. 3ºAvisar a los departamentos afectados que los sistemas se encuentran fuera de servicio. 4º Reparar rápidamente el desperfecto para poner en funcionamiento el sistema. 5º Una vez reparados los sistemas, es necesario avisar a los departamentos afectados que los sistemas han vuelto a su funcionamiento.	□□ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo.□ □□ Poseer una lista con todos los sistemas, describiendo su nombre, a los departamentos que presta servicios, nombre de la empresa desarrolladora, roles de los usuarios, lista de contacto de la empresa desarrolladora, contacto del inspector técnico, encargado del sistema.□ □□ Tener una lista con todos los departamentos y los usuarios que tienen acceso a dicho sistema, indicando el privilegio como usuario que tienen.□ □□ Definir los periodos de capacitación, tanto para usuarios básicos como avanzados.□ □□ Hacer llegar a los usuarios de los sistemas las políticas sobre el uso de la información y del cuidado de las claves de usuarios.□ □□ Debe tener una lista con los contactos de la empresa que presta el servicio para avisar en caso de fallas. □□ Tener una lista de contactos de los departamentos a los cuales se les asocian los sistemas. □□ Llevar a cabo el plan de acción. □□ Llevar un control de todas las contingencias producidas.

Robo de las bases de datos de los sistemas	1º Evaluar rápidamente cuáles son las bases de datos que han sido robadas y ver cuáles son los servicios afectados. 2º Dar reporte del robo, a las autoridades pertinentes. 3º Avisar a los departamentos que han sido afectados, que los sistemas estarán interrumpido por un momento. 4º Dar solución en forma rápida, acudiendo a los respaldo de bases de datos si es necesario. 5º Una vez puesto en funcionamiento los sistemas es necesario avisar a los dopartamentos afectados que se ha restablecido el funcionamiento de los sistemas.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Poseer una lista con todos los sistemas, describiendo cuáles son sus características y a los departamentos que presta servicios. Tener un respaldo de todas las bases de datos. Tener la documentación de todas las bases de datos de los Sistemas. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que se provoque un fallo en ellos. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Desperfecto en el servidor de sistemas y de bases de datos.	1º Ver cuáles son los servidores afectados y evaluar los daños que tiene. 2º Detectar los servicios afectados y avisar al departamento que ha quedado sin servicio. 3º Hacer un respaldo de la información, en el caso que sea necesario. 4º Ver cuál es la pieza que ha fallado y cambiarla, es necesario levantar el servicio en otro	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener un registro de todos los sistemas y sus bases de datos respectivas. Tener una lista con los servidores que prestan el servicio a los sistemas y las bases de datos. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que se provoque un fallo en ellos. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.

	servidor. 5º Avisar a los departamentos afectados que los servicios se han restablecido.	
Falla en el diseño y la programación de funciones o procedimientos e inconsistencia de datos.	1º Evaluar rápidamente cuales son los sistemas afectados y avisar a los departamentos. 2º Avisar a la empresa que presta el servicio, sobre el desperfecto del sistemas, para que ellos acudan a repararlo o lo hagan de forma remota. 3º Una vez reparado el desperfecto es necesario levantar el servicio y avisar a los departamentos afectados.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Llevar a cabo el plan de acción. Tiene que tener todos los sistemas con su respectivo nombre, servicio que presta, departamento que lo ocupa, empresa desarrolladora. Debe tener una lista con los contactos de la empresa que presta el servicio para avisar en caso de fallas. Contar con el modelo de datos del sistema. Tener toda la documentación del sistema. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que se provoque un fallo en ellos. Llevar un control de todas las contingencias producidas.
Fallo en los software relacionados con el sistema. Fallas en el equipo en el cual se está ejecutando el sistema.	1º Analizar el tipo fallo, si es físico o lógico. 2º Cambiar rápidamente el equipo (si es una estación de trabajo critica), hasta que sea reparado. 3º Llevar al servicio técnico el Equipo para su reparación. 4º Asegurarse que el sistema funcione correctamente en el equipo.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener la documentación todos los sistemas y a los departamentos que presta servicios. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.

PLAN DE ACCION BASES DE DATOS

Amenaza o Contingencia	Acciones a Realizar	Función que Realizara
Robos por parte de piratas informáticos y adulteración de algún dato almacenado.	1º Evaluar rápidamente cuáles son las bases de datos que han sido robadas y ver cuáles son los servicios afectados. 2º Dar reporte del robo, a las autoridades pertinentes. 3º Avisar a los departamentos que han sido afectados, que los sistemas estarán interrumpidos por un momento. 4º Dar solución en forma rápida, acudiendo a los respaldo de bases de datos si es necesario. 5º Una vez puesto en funcionamiento los sistemas es necesario avisar a los departamentos afectados que se ha restablecido el funcionamiento de los sistemas.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Poseer con una lista de todas las bases de datos y con los sistemas a los cuales se relaciona. Tener respaldada toda las bases de datos. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que se provoque un fallo en las bases de datos y los sistemas. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Robo físico del servidor de bases de datos y daños intencionados.	1º Ver si el servidor ha sido robado o dañado, en el caso que el servidor ha sido dañado es necesario enviarlo al servicio técnico para que lo repare. 2º Detectar cuáles son los servicios afectados. 3º Avisar a los departamentos afectados, que los servidos estarán interrumpidos por un periodo de	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener una lista con todas las bases de datos que se cuentan. Poseer la documentación que describa los servicios que se ven afectados si no está en funcionamiento el servidor que contiene las bases de datos. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que el servidor de bases de datos no esté en funcionamiento.

	tiempo. 4º Levantar el servicio en otro equipo y probar que los servicios funcionen correctamente. 5º Avisar nuevamente a los departamentos afectados que los servicios han sido restablecido.	Tener una lista de contactos de los encargados de la seguridad de la municipalidad. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Mal diseño de las bases de datos e inconsistencia entre el sistema y la base de dato.	1º Evaluar rápidamente cuáles son las bases de datos afectadas y avisar a los departamentos. 2º Avisar a la empresa que presta el servicio, sobre el desperfecto de la base de dato, para que ellos acudan a repararlo o lo hagan de forma remota. En el caso que este servicio lo haga el mismo personal del departamento de informática, es necesario acudir a la documentación de las bases de datos, para ver de donde proviene la falla y realizar la reparación necesaria. 3º Una vez reparado el desperfecto es necesario levantar el servicio y avisar a los departamentos afectados.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener el modelo de dato de las bases de datos. Tener una lista con todas las bases de datos y los sistemas que se relacionan. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que el servidor de bases de datos no esté en funcionamiento. Tener el contacto con la empresa que presta el servicio. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Desperfecto en el servidor de bases de datos.	1º Ver cuáles son las razones por la que fallo el servidor. 2º Detectar los servicios afectados y avisar al departamento que ha quedado sin servicio.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que el servidor de bases de datos no esté en funcionamiento.

	3º Hacer un respaldo de la información, en el caso que sea necesario. 4º Llevar el equipo al servicio técnico para que sea reparado, es necesario levantar el servicio en otro servidor. 5º Avisar a los departamentos afectados que los servicios se han restablecido.	Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Virus que afecte al servidor de bases de datos.	1º Poner en cuarentena el servidor. 2º Ver cuáles son las bases de datos y los servicios afectados y avisar oportunamente a los departamentos que han quedado sin servicios. 3º Reparar el desperfecto ocasionado por el virus y levantar el servicio de bases de datos en otro servidor mientras el desperfecto es solucionado. 4º Una vez levantado el servicio provisorio, es necesario avisar a los departamentos afectados, que los servicios han sido restablecidos.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Actualización periódica del antivirus. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que el servidor de bases de datos no esté en funcionamiento. Tener la documentación que describa el servidor donde se encuentran las bases de datos, con todas las características. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.
Falla en algún software que tenga relación con la base de dato.	1º Ver cuál es el desperfecto, en el caso que quede inhabilitado el servidor, es necesario enviar el equipo al servicio técnico. 2º Avisar a los departamentos	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Poseer una lista de contacto con los diferentes departamentos para avisar en el caso que el servidor de bases de datos no esté en funcionamiento.

afectados que estarán sin servicio por un periodo de tiempo corto. 3º Levantar el servicio en otro servidor. 4º Una vez levantado el servicio es necesario avisar a los departamentos que los servicios han sido restablecidos.		▯▯ Tener la documentación que describa el servidor donde se encuentran las bases de datos, con todas las características. ▯ ▯▯ Llevar a cabo el plan de acción. ▯ ▯▯ Llevar un control de todas las contingencias producidas.

PLAN DE ACCION REDES

Amenaza o Contingencia	Acciones a Realizar	Función que Realizara
▯▯ Robo o daños intencionados en algún dispositivo de la red, como switch, hub, router, etc. ▯▯ Cortes Intencionados o casual del cableado de la red. ▯▯ Desperfecto de los dispositivos de red. ▯▯ Mal diseño de la red.	1º Ver cuáles son los dispositivos que han sido robados o dañados. 2º Avisar a la empresa externa que presta este servicio para que repare en la brevedad el desperfecto. 3º Analizar rápidamente cuales son las áreas que han quedado desconectadas de la red. 4º Avisar a los departamentos afectados sobre el desperfecto. 5º Una vez que la empresa que presta el servicio ha reparado el desperfecto es necesario avisar a los departamentos que los servicios se han restablecido.	▯▯ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ▯▯ Tener la documentación de la red, en la que muestre los mapas de red, dispositivos que la componen y los distintos departamentos que están conectados. ▯▯ Marcar todos los dispositivos de la red. ▯▯ Poseer con la lista de contacto con los distintos departamentos, para avisar en el caso de algún desperfecto. ▯▯ Tener el contacto con la empresa externa que presta el servicio. ▯▯ Llevar a cabo el plan de acciÓn. ▯▯ Llevar un control de todas las contingencias producidas.
▯▯ Corte del suministro eléctrico.	1º Avisar el desperfecto a la empresa que presta el servicio.	▯▯ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo.

2º Ver que los protectores contra tempo- han activado correctamente. 3º Ver que los dispositivos de la red sigan	rales cortes de energía eléctrica, se funcionando correctamente.	▯▯ Poseer el número de contacto con la empresa que presta el servicio. ▯▯ Llevar a cabo el plan de acción. ▯▯ Llevar un control de todas las contingencias producidas.

PLAN DE ACCION DEPARTAMENTO DE INFORMATICA

Amenaza o Contingencia	Acciones a Realizar	Función que Realizara
▯▯ Daños físicos al departamento por parte de personas internas o externas y robos de información, equipos, repuestos, materiales.	1º Analizar los daños que se han ocasionado o los robos producidos y ver de donde provienen. 2º Analizar si los daños provocados han interrumpido algún servicio de los que presta el departamento de informática a otros departamentos. 3º Si se ve afectado algún servicio es necesario ponerlo en funcionamiento rápidamente. 4º Dar aviso al personal de seguridad.	▯▯ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ▯▯ Tener el contacto del personal de seguridad de la municipalidad. ▯▯ Tener un inventario de todos los recursos informáticos y respaldo de toda la información que se maneja. ▯▯ Mantener un control riguroso de las personas que ingresan al departamento. ▯▯ Procurar el cumplimiento de ciertas normas por parte del personal del departamento, como registrar las salidas que realizan. ▯▯ Mantener las oficinas cerradas cuando no se encuentre nadie en ellas. ▯▯ Llevar a cabo el plan de acción. ▯▯ Llevar un control de todas las contingencias producidas.
▯▯ Ataques terroristas.	1º Poner al tanto a las autoridades y a los usuarios que los servicios han sido dañados, por lo que no están activos y que se está trabajando en reponer los servicios	▯▯ Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. ▯▯ Tener una lista de contactos con todos los organismos de seguridad. ▯▯ Poseer un inventario detallado con todos los recursos

	en la brevedad (si es que se ve afectado algún servicio). 2º Analizar cuáles son las magnitudes de los ataques y los daños ocasionados. 3º Ver cuáles son los servicios y áreas afectadas. 4º Reponer los servicios afectados en la brevedad, realizando las tareas necesarias.	existentes. - Llevar a cabo el plan de acción. - Llevar un control de todas las contingencias producidas.
- Corte del suministro eléctrico	1º Avisar el desperfecto a la empresa que presta el servicio. 2º Ver que los protectores contra temporales cortes de energía eléctrica, se han activado correctamente. 3º Ver que los servicios sigan funcionando correctamente.	- Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. - Poseer el número de contacto con la empresa que presta el servicio. - Tener el número de contacto del personal encargado de la mantención eléctrica de la municipalidad. - Llevar a cabo el plan de acción. - Llevar un control de todas las contingencias producidas.
- Incendio.	1º Cortar el suministro eléctrico. 2º Analizar las magnitudes del incendio y en el caso que corresponda avisar a bomberos para que acudan al lugar. 3º Evacuar al personal. 4º Retirar los equipos del departamento y la información importante, si las magnitudes del incendio lo permiten. 5º Ver cuáles son los servicios afectados y avisar a los departamentos o áreas afectadas.	- Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. - Certificar periódicamente que los extintores de incendio estén en mantención periódica. - Tener una lista de contactos con todos los organismos de seguridad. - Poseer un inventario detallado con todos los recursos existentes. - Llevar a cabo el plan de acción. - Llevar un control de todas las contingencias producidas.

	6º Si algún servicio ha sido afectado es necesario reponerlo en la brevedad.	
Inundaciones	1º Cortar el suministro eléctrico. 2º Dar aviso al personal de seguridad de la municipalidad. 3º Retirar los equipos y la información importante para evitar daños. 4º Avisar a los departamentos que han sido afectados por el fallo en los servicios. 5º Levantar los servicios (en el caso que existan servicios inhabilitados), en la brevedad en una sala de emergencia.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener una lista de contactos con todos los organismos de seguridad. Poseer un inventario detallado con todos los recursos existentes. Llevar a cabo el plan de acción Llevar un control de todas las contingencias producidas.
Terremotos.	1º Cortar el suministro eléctrico. 2º Evacuar al personal. 3º Analizar las magnitudes del terremoto y ver si se pueden retirar los equipos o información importante.	Conocer en detalle el plan de acción y tener conformado el equipo de trabajo. Tener una lista de contactos con todos los organismos de seguridad. Poseer un inventario detallado con todos los recursos existentes. Llevar a cabo el plan de acción. Llevar un control de todas las contingencias producidas.

ACTIVIDADES DESPUES DEL DESASTRE

Amenaza o Contingencia	Evaluación de Daños	Pasos cumplidos del Plan de Acción	Funcionamiento de servicios después del Plan de Acción

- En la columna 1 debe especificar la contingencia que ha ocurrido.
- Para completar la columna 2 debe detallar los daños ocurridos.
- En la columna 3 tendrá que detallar que pasos se cumplieron del plan de acción.
- La columna 4 deberá especificar de qué forma están funcionando los servicios o actividades dañadas por la contingencia, después de haber aplicado el plan de acción.

Anótese, regístrese, comuníquese, transcríbase a todas las unidades de la Municipalidad, publíquese en la página WEB y archívese en su oportunidad.

MUNICIPALIDAD DE * ALCALDE * PUENTE ALTO

GERMÁN CODINA POWERS
ALCALDE

MUNICIPALIDAD DE SECRETARIO MUNICIPAL PUENTE ALTO

MIGUEL ÁNGEL ROMÁN AZAR
SECRETARIO MUNICIPAL