I. Municipalidad de Coyhaique

REF : APRUEBA POLITICAS DE SEGURIDAD Y PLAN DE CONTINGENCIAS PARA EL RESGUARDO DE LOS BIENES, SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES DE LA MUNICIPALIDAD DE COYHAIQUE.

REGLAMENTO N° 03 /

COYHAIQUE, 12 ABR 2011

V I S T O S :

Las atribuciones que me confiere la Ley No. 18.695, Orgánica Constitucional de Municipalidades de fecha 31 de marzo de 1988 y sus modificaciones; el Decreto N° 83 de 12 de enero de 2005, del Ministerio Secretaría General de la Presidencia que Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; el Fallo del Tribunal Electoral Regional de Aysén, de fecha 17 de noviembre de 2008; el Acta de Constitución del Honorable Concejo de la Comuna de Coyhaique, de fecha 06 de diciembre de 2008;los Artículos 77° y 78° de la Ley 18883,

CONSIDERANDO :

Las observaciones contenidas en el Pre-Informe N°31 de 2010 de la Contraloría Regional de Aysén que señala la falta de controles de ambiente TI, el Decreto 6869 de 25 de octubre de 2010 que encarga a la Sección Informática la elaboración de una instrucción que permita dar cumplimiento a las exigencias contenidas en el Decreto N°83 de la Secretaría General de la Presidencia referido y el documento con las Políticas de Seguridad y Contingencia emitido por don Gustavo Fuentes Urzúa para análisis, discusión y aprobación final; Dicto el siguiente Reglamento Municipal:

REGLAMENTO DE POLÍTICAS DE SEGURIDAD Y PLAN DE CONTINGENCIAS PARA EL RESGUARDO DE LOS BIENES, SERVICIOS INFORMATICOS Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DE COYHAIQUE

ARTICULO 1° Apruébase el Reglamento de Políticas de Seguridad y Plan de Contingencias para el resguardo de los bienes, servicios informáticos y de telecomunicaciones de la Municipalidad de Coyhaique, cuyo texto es el que se señala a continuación:

1° ALCANCE DE LAS POLÍTICAS

OBJETIVO

Regular la actividad en cuanto al uso, aprovechamiento, conservación y resguardo de los bienes y servicios informáticos y de telecomunicaciones de la Municipalidad.

Las políticas definidas en el presente documento se aplicarán a todos los funcionarios que hagan uso de algún recurso informático, implementado en el Municipio.

2° DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

Política de Seguridad: Surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

Recurso Informático: Elementos informáticos (base de datos, sistemas de gestión, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Usuario: Son los funcionarios Municipales que hacen uso y tienen acceso a las tecnologías de la información y telecomunicaciones pertenecientes a la Municipalidad.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios de la Municipalidad, pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos.

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático que pone en riesgo los servicios de información o expone la información en si misma, sea o no protegida por reserva legal.
IP : Conjunto de reglas que regulan la transmisión de paquetes de datos a través de la red.

Certificado o firma Digital: Mecanismo utilizado para asegurar la integridad del mensaje y la autenticación del emisor.

Correo Electrónico Institucional: Al correo electrónico de la Municipalidad: ejemplo@coyhaique.cl

Cuenta de Usuarios: En el contexto de la informática, un usuario es aquel que utiliza un sistema informático, ahora bien, para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, entre otros, deberán identificarse. Para que uno pueda identificarse, el usuario necesita una cuenta (una cuenta de usuario) y un usuario, en la mayoría de los casos asociados a una contraseña, por tanto las cuentas de usuario constituyen la principal vía de acceso al sistema, estas aíslan al usuario del entorno, impidiendo que pueda dañar al sistema, permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros.

Internet: Red mundial de redes que se conectan utilizando un conjunto de protocolos y que funcionan como una sola red virtual.

Intranet: Red Interna. Red de comunicación en ambientes internos o cualquier tipo de organizaciones, que permite a los usuarios acceder a la información que cada una de sus áreas genera para fomentar el nivel de información y productividad.

LAN: Conexión a la Red Local. Red de datos para dar servicio a un área geográfica limitada, que en este caso corresponda a la Municipalidad.

Mantenimiento Correctivo: Consiste en la reparación de alguno de los componentes de una impresora, escaner, computador o dispositivo periférico como el ratón, teclado, monitor, entre otros, o de ser necesario el cambio total de los mismos.

Mantenimiento Preventivo: Consiste en la revisión periódica de ciertos aspectos, tanto de hardware como de software en un PC, de una impresora, escaner, ratón, teclado, monitor, entre otros, siendo el propósito crear un ambiente favorable para el sistema y conservar limpias todas las partes que los componen, toda vez que el mayor número de fallas que presentan los equipos es por la acumulación de polvo en los componentes internos, ya que éste actúa como aislante térmico.

PC o COMPUTADOR: Máquina electrónica de computación.

Plan de Contingencia: Es el instrumento de gestión para el buen manejo de las tecnologías de la información y comunicaciones, el cual contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones del Municipio.

Privilegios de Acceso: Privilegio para tener acceso a carpetas y hacer cambios en ellas.

Red: Sistema de elementos interrelacionados que se conecta mediante un vínculo dedicado para proporcionar una comunicación local o remota (de voz, vídeo, datos, etc.) y facilitar el intercambio de información entre usuarios.

Respaldo de Datos: Es la generación de una copia, en un momento determinado, de los datos del sistema, con vistas a su eventual reposición en caso de pérdida. Todos los sistemas informáticos deben respaldarse cuidadosamente, en momentos predeterminados.

Router: Encaminador, direccionador, enrutador. Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento.

Servidor: Computador central de un sistema de red que provee servicios y programas a otras computadoras conectadas. Sistema que proporciona recursos (por ejemplo, servidores de archivos, servidores de nombres). En Internet este término se utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la red.

Software (programas, componentes lógicos): Programas o elementos lógicos que hacen funcionar un computador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del computador o la red.

Soporte Técnico: Es un rango de servicios que proporcionan asistencia con el hardware y/o software de un computador, o algún otro dispositivo electrónico o mecánico. En

general, los servicios de soporte técnico tratan de ayudar al usuario a resolver determinados problemas.

Switch: Un dispositivo de red capaz de realizar una serie de tareas de administración, incluyendo el redireccionamiento de los datos.

Virus informático: Programa cuyo objetivo es causar daños en un sistema informático y que a tal fin se oculta o disfraza para no ser detectado. Estos programas son de muy diversos tipos y pueden causar problemas de diversa gravedad en los sistemas a los que infectan.

WAN: Red de computadores conectados entre sí en un área geográfica relativamente extensa. Este tipo de redes suelen ser públicas, es decir, compartidas por muchos usuarios. En el caso de la Municipalidad se les denomina Red Externa.

WWW: Red Global Mundial (por sus siglas en ingles World Wide Web), es un sistema de comunicación de documentos de hipertexto enlazados y accesibles a través de Internet

UPS: Fuentes generador de energía autónomo.

Shareware: Dícese de los programas informáticos que se distribuyen a prueba por internet, con el compromiso de pagar al autor su precio, una vez probado el programa y/o pasado cierto tiempo de uso.

Equipos de Comunicación: Termino usado para describir cualquier tipo de equipo utilizado en la red de voz y datos del Municipio.

Contraseña: Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

3° DESCRIPCIÓN DE LAS POLITICAS

3.1° POLÍTICA DE ACCESO A LA INFORMACIÓN

- Todos los funcionarios Municipales, que hagan uso de algún sistema de Gestión o software de uso masivo, deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Municipalidad, el responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo a realizar por estas personas, previa justificación y conocimiento de Informática, cuando corresponda.
- El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin, en las políticas(3) sobre seguridad.
- Todos los permisos y configuraciones para el uso de los sistemas de información de la Municipalidad, deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad.

3.2° POLÍTICA DE ADMINISTRACION DE CAMBIOS

- Todo cambio, sea este en el hardware y/o software que afecte los recursos informáticos, debe ser requerido por el usuario y aprobado formalmente por el

responsable de este, y comunicado a Informática cuando lo amerite, para ver factibilidad técnica.

- Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.
- Para la administración de cambios se efectuará el procedimiento correspondiente definido por la Municipalidad, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica (procedimientos de adquisiciones/Chile Compra).
- Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado, ya sea en papel o vía email.
- Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya o afecte la seguridad en la red interna del Municipio.

3.3° POLÍTICA DE SEGURIDAD

Para prevenir el acceso no autorizado, los usuarios deben usar dos credenciales de acceso para el ingreso a los computadores.

- Cada usuario será responsable de la información almacenada en equipo asignado para la ejecución de sus labores y deberá velar por la integridad y seguridad de la información, aplicando todas las medidas que estén a su alcance.
- Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de encendido y acceso al escritorio, protegido mediante claves, la que debe contener números y letras.
- Todo computador conectado a la red Municipal deberá solicitar credenciales de acceso al escritorio, con claves alfanuméricas.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante protector de pantalla.
- Si no ha habido ninguna actividad en un computador durante un cierto periodo de tiempo, el sistema debe automáticamente activar el protector de pantalla, y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El reestablecimiento de la sesión requiere que el usuario se autentique mediante su contraseña. Además es aconsejable que el usuario debe suspenda la sesión manualmente cada vez que se ausente de su oficina.
- Credenciales de acceso al escritorio y protector de pantalla de todos los usuarios deberán entregarse en sobre cerrado a la unidad de informática, donde serán almacenados en una caja fuerte. Se recomienda cambiar dos veces al año las contraseñas de acceso o cuando exista apertura del sobre por parte del personal de informática.
- El usuario no debe guardar sus contraseñas en una forma legible de 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 solicitar a Informática el cambio de esta. 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.

- Nunca debe compartirse la contraseña o revelarse a otros. El hacerlo expone al usuario a las consecuencias administrativas por las acciones que los otros hagan con esa contraseña.
- Está prohibido el uso de contraseñas de grupo, siempre y cuando estas originen cambios en la información.
- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan conexión a la red local (LAN), a menos que sea debidamente solicitado por directores y/o jefes de departamento/secciones, justificado vía email.
- No pueden transmitirse o llevar información confidencial fuera de la Municipalidad sin la aprobación previa del jefe directo. Esta política es particularmente aplicable a aquellos que usan computadores portátiles (Notebook y/o Netbook) u otros dispositivos de almacenamientos (pendrive, cd, dvd).
- Periódicamente debe hacerse el respaldo de los datos guardados en los computadores y servidores y las copias de respaldo deben guardarse en un lugar que garantice su seguridad.
- Los usuarios que hagan uso de un computador son responsables de definir qué información debe respaldarse, así como la frecuencia de respaldo (diario, semanal, quincenal, etc.).
- El acceso a las claves utilizadas para el ingreso al computador debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a terceras personas.
- Eliminar conexiones a Internet u otras redes LAN de equipos municipales en especial equipos portátiles del tipo Notebook y Netbook, salvo casos especiales autorizados por jefaturas y solicitadas vía e-mail.
- Siempre que sea posible, debe eliminarse la información confidencial de las computadoras, previo respaldo correspondiente, antes de enviarlas a alguna reparación.
- No deben estar las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial.
- El personal que utiliza un computador portátil que contenga información confidencial del Municipio, deberá proteger y resguardar dicha información, impidiendo o evitando el uso, la sustracción o pérdida de la misma, sobre todo cuando se encuentre de viaje.
- Informática solo podrá monitorear las comunicaciones con el fin de mantener el óptimo estado de la red de la Municipalidad. Informática se compromete a respetar los derechos de sus empleados, incluyendo su privacidad, siempre y cuando no atente contra los intereses del Municipio.
- Es política de la Municipalidad prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, de proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.
- Los servidores de red y los equipos de comunicación (routers, etc.) deben estar ubicados en lugares apropiados, protegidos contra daños y robo. Debe restringirse el acceso a estos lugares, a personas no autorizadas o ajenas al Municipio, mediante el uso de cerraduras u otros sistemas de acceso.
- Se debe incluir aislación, climatización, puerta con llaves en sala de servidores y sistema de apertura de puerta principal unidad de informática.

3.4° POLÍTICA SOBRE HARDWARE y SOFTWARE

Los computadores del Municipio sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control establecidas en este documento, para proteger el software, el hardware y los datos.

- Los computadores del Municipio deberán ser instalados apegados a los lineamientos de seguridad que establezca el Municipio, en conjunto con Informática.
- Queda estrictamente prohibido modificar la configuración de hardware y software establecida por Informática para cada computador.
- Deben protegerse los equipos de riesgos del medio ambiente (por ejemplo, polvo, incendio y agua).
- Deben usarse protectores contra variaciones de energía eléctrica o fuentes de poder ininterrumpibles (UPS) con regulador de voltaje, para conectar los equipos críticos del Municipio, en forma especial los routers, servidores y atención de público.
- Cualquier falla en el computador o en la red debe reportarse a Informática, para que estos tomen medidas inmediatas en la atención y servicio del equipo.
- Al enviar una impresión verificar el estado exitoso o no de la operación, de existir alguna anomalía se debe comunicar de inmediato a Informática.
- Se debe procurar la protección de los equipos para disminuir el riesgo de robo, destrucción y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave de la oficina o área donde éstos se encuentren.
- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- No pueden moverse los equipos o reubicarlos sin la autorización del titular del área correspondiente y el visto bueno de Informática. Para llevar equipos fuera del Municipio se requiere de la autorización por escrito o email del titular del área correspondiente y el visto bueno del Administrador Municipal y de Informática.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente al Administrador Municipal y a Informática.
- En caso de ser necesario llevar al sitio de trabajo computadoras portátiles (Notebook o Netbook) de propiedad personal, es necesario contar con la autorización del titular del área correspondiente y notificar a Informática, para su evaluación técnica. Informática será la encargada de definir el grado de acceso a la red.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software del Municipio 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.
- No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido evaluado y que esté aprobado su uso por Informática.

- 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 o shareware, a menos que haya sido previamente aprobado por Informática.
- Para ayudar a restaurar los programas originales dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro, siendo Informática el responsable de esta tarea, siempre y cuando el software sea licenciado para el Municipio.
- No deben usarse medios de almacenamiento temporales (DVD, CD, Memorias USB, Discos externos) en cualquier computador del Municipio, a menos que se haya verificado previamente que están libres de virus u otros agentes dañinos.

3.5° POLÍTICA DE INFRAESTUCTURA (REDES Y TELECOMUNICACIONES)

La Municipalidad a través de Informática:

- Normará el direccionamiento y segmentación de la red (Internet, Protocolo), la configuración, los parámetros de seguridad y control de los equipos de ruteo.
- Mantendrá en operación la infraestructura de cableado de red; así como proveerá la conectividad hacia todas las plataformas.
- Las decisiones sobre infraestructura competen única y exclusivamente a la Municipalidad.
- Informática dará a conocer a todos sus usuarios, los sistemas de auditoria y control con los que se cuentan para la seguridad de la red de datos del Municipio, además de las restricciones de uso de cada herramienta.
- Con el fin de mejorar la productividad, la Municipalidad promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono y el correo electrónico. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, son propiedad del Municipio y no propiedad de los usuarios de los servicios de comunicación.
- Los sistemas de comunicación del Municipio 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; además de que no interfiera con la productividad de las labores propias del funcionario Municipal.
- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
- De manera consistente con prácticas generalmente aceptadas, el Municipio, con Informática, procesa datos estadísticos sobre el uso de los sistemas de telecomunicación, como por ejemplo, los reportes del uso telefónico (Tarificador) que contienen detalles sobre el número llamado, la duración de la llamada y la hora en que se efectuó la llamada entre otros; y el uso del Internet para medir el rendimiento del ancho de banda (tamaño del canal de comunicación).
- Todo cambio en los servidores y equipos de la red del Municipio, incluyendo la instalación de nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser autorizados por Informática, excepto si se trata de una situación de emergencia. Todo esto para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.
- Informática, tiene la facultad de auditar el tráfico de la red.
- En caso de que el usuario haga mal uso de la red, mediante acciones tales como descargas de formatos de audio, envío de archivos pesados, videos, etc.,

intrusión (husmear recursos compartidos, acceso sin autorización, adivinar contraseñas) será motivo de suspensión de todos los derechos de acceso a la red por parte de Informática, sin perjuicio de que se le aplique la normativa vigente interna.

3.6 POLÍTICA DE SERVICIOS DE INTERNET, RED, CORREO ELECTRONICO y ANTIVIRUS

Internet y Mensajería Instantánea.

- Informática será la encargada exclusivamente de autorizar y proveer el servicio de Internet y Mensajería Instantánea, a los usuarios del Municipio que cumplan con lo dispuesto en este documento.
- Los servicios de Internet y Mensajería Instantánea serán utilizados para fines estrictamente laborales y podrá tener acceso todo aquel funcionario que justifique su uso, avalado por la autorización del titular del área en donde se desempeñe el usuario.
- No se permite acceder a páginas que ocasionen lentitud y saturación de la red interna, sean estas de descarga de archivos, (emule, ares, p2p, etc), escuchar radio y televisión en línea, excepto transmisiones de concejo municipal en vivo, y todas aquellas páginas que tengan que ver con la gestión municipal.
- Informática velará por el óptimo funcionamiento de la plataforma de publicación del portal web www.coyhaique.cl y garantizará un servicio en línea de siete por veinticuatro horas los trescientos sesenta y cinco días del año.
- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos del Municipio.
- 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 del Municipio, a menos que estén cifradas y firmadas digitalmente.
- Red interna del Municipio, para solicitar la creación de un usuario deberá ser por escrito o email a Informática, avalado por el titular del área del usuario y anexando su justificación y a que aplicaciones deberá tener acceso.
- El correo electrónico queda restringido única y exclusivamente a los usuarios que así lo justifiquen, avalados por el jefe directo del usuario. Debe tomarse en cuenta que esta herramienta debe ser utilizada para fines de mejora de comunicación interna/externa. Informática, previa comunicación del jefe directo del usuario, creará y posteriormente configurara la cuenta de email en el computador correspondiente.
- Por ningún motivo deben enviarse cadenas ni contestar correos de los cuales se desconozca su procedencia. Es muy importante no leer el contenido y borrar inmediatamente cualquier correo del cual se desconozca la procedencia o el remitente. Deben utilizarse clientes de correos (Outlook) previamente aprobados por Informática.
- Aplicaciones (Sistemas Cas Chile u otros); La solicitud de una cuenta de usuario deberá realizarla el jefe directo por escrito o email, a Informática, indicando y especificando los privilegios de acceso a que tendrá derecho el usuario. El cambio de privilegios o eliminación de una cuenta, debe solicitarse por escrito o email.

- No debe concederse una cuenta a personas que no sean funcionarios de la Municipalidad a menos que exista una autorización superior por escrito o email. En cuanto a los accesos y privilegios, solo deben ser de consulta y listado.
- Privilegios especiales, tal como la posibilidad de modificar o borrar archivos de otros usuarios, sólo debe otorgarse a aquellos directamente responsables de la administración o de la seguridad de las aplicaciones.
- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que Informática determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, mantenimiento remoto).
- Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben de entrar al sistema mediante cuentas que indiquen claramente su identidad.
- Antivirus; Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a Informática para proceder a chequear y analizar el computador, y así evitar daños mayores en la red interna.
- Las licencias de antivirus corporativos serán definidos por Informática, así como sus políticas de implementación las cuales deberán ser respetadas al cien por ciento, dado el enorme riesgo en que se pone a toda la infraestructura de la red de datos del Municipio.
- La herramienta antivirus debe ser institucional y cubrir por licenciamiento ilimitado a todos los computadores del Municipio. No podrá usarse ninguna otra herramienta antivirus en equipos del Municipio sin la autorización previa de Informática. Debe utilizarse esta herramienta para examinar todo los datos que provengan tanto interno como externos al Municipio.
- En caso de inclusión de un nuevo funcionario o cese de funciones, la sección de personal debe notificar por escrito o email a Informática, para proceder a dar de baja los accesos y privilegios otorgados a dicho funcionario.
- Antes de proceder a la baja de la cuenta, se deberá realizar un respaldo de la información contenida en el equipo que tenía bajo su resguardo el usuario dado de baja, quedando dicho respaldo a disposición del jefe directo del área.
- En caso de mal uso de algún servicio o si fuera detectado cualquier cambio en las políticas de implementación del antivirus por parte del usuario, en primera instancia será motivo de suspensión de todos los derechos de acceso por parte de Informática, e informado al jefe directo de tal medida.

3.7° POLÍTICA DE SOPORTE TÉCNICO

- Informática deberá proveer servicio de soporte a todos los funcionarios de la Municipalidad, para garantizar la correcta operación del equipamiento informático.
- Solo se prestará servicio de mantenimiento preventivo y correctivo, asesoría técnica y de cualquier otra índole a usuarios del Municipio que tengan bajo su resguardo equipo informático.
- El servicio de soporte será en base a tareas rutinarias de algún software o hardware.
- Informática podrá efectuar un servicio interno de mantención preventiva y/o correctiva, en casos menores, de lo contrario, y encaso de ser necesario la reparación de equipos, informática enviara al proveedor de este, o algún servicio técnico reconocido.

- La mantención preventiva se realizará con base a un calendario establecido y cada unidad administrativa del Municipio será notificada con al menos 3 días de anticipación a la fecha y hora de atención correspondiente. Si por argumentos razonables de parte del usuario no pudiese facilitar el equipo en la fecha y hora programadas, deberá acordarse con Informática una nueva fecha y hora para su atención.
- Cualquier cambio o actualización que se requiera realizar en los equipos de computación de la Municipalidad (cambios de CD/DVD, aumento de memoria, o algún periférico) debe tener previamente una evaluación técnica y autorización de Informática.
- La reparación técnica de los equipos, que implique la apertura de los mismos, será evaluada por Informática, y de ser necesario se remitirá al proveedor para hacer efectiva la garantía, si corresponde.
- Los equipos de informática (PC, impresoras, servidores, etc.) no deben moverse o reubicarse sin la autorización del jefe directo del área involucrada, y de la aprobación previa de informática.

3.8° POLÍTICA DE ALMACENAMIENTO Y RESPALDO

- Los datos almacenados o contenidos en servidores, deberán ser almacenados y respaldados de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.
- El resguardo de los respaldos de la información deberá realizarse interna y/o externamente a la Municipalidad, esto de acuerdo con la importancia de la información para la operación del Municipio.
- Los funcionarios que hagan uso de un computador municipal, son responsables de los respaldos de su información, siguiendo las indicaciones técnicas dictadas por informática y con una frecuencia mínima de un año. Informática será la autorizada para realizar el seguimiento y control de esta política.

3.9° POLÍTICA DE CONTINGENCIA

- La administración de la Municipalidad debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas informáticos y de comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, incendio, inundación etc.

3.10° POLÍTICA DE AUDITORIA

- Todos los sistemas automatizados que operen y administren información sensitiva, valiosa o crítica para la Municipalidad, como son los sistemas de aplicación (Cas Chile) deben contar con un seguimiento, que permita auditarlos (creación de registros, modificación, eliminación).
- Todos los archivos de auditoría deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

- Todos los archivos de auditorías de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.
- Todos los archivos de auditorías deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.
- Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.
- Los lugares en los cuales exista equipamiento informático que la Municipalidad considere criticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada por personal de Informática o por el personal que labora cotidianamente en esos lugares.
- En los centros de cómputo o áreas que la entidad considere criticas deberán existir elementos de control de incendio y alarmas.
- Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.
- Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la municipalidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de informática.
- Los equipos de microcomputadores (PC, servidores ,equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa de informática.
- Los funcionarios Municipales se comprometen a NO utilizar la red eléctrica exclusiva de computación para conectar equipos eléctricos diferentes a su equipo de computo, como, cargadores de celulares, radios, hervidores eléctricos, estufas y en general cualquier equipo que generen caídas de la red eléctrica.
- Los particulares en general, entre ellos, los familiares de los funcionarios Municipales, no están autorizados para utilizar los recursos informáticos de la Municipalidad.

4° PLAN DE CONTINGENCIA PARA LA CONTINUIDAD DE LOS SERVICIOS Y APLICACIONES CRÍTICAS DEL MUNICIPIO

El Plan de Contingencias es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y las Telecomunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la Municipalidad.

El plan de contingencias deberá ser revisado semestralmente. Así mismo, es revisado/evaluado cuando se materializa una amenaza.

Objetivo

Establecer las políticas y procedimientos para ser usados para los sistemas de información en el caso de una contingencia, para proteger y asegurar la funcionalidad de estos servicios.

Sistemas/aplicaciones/servicios de misión critica

Los siguientes sistemas/aplicaciones/servicios de misión crítica deberán ser recuperados en el caso de un desastre:

- Sistemas en Línea (Cas).
- Conectividad LAN Conexión de Red Interna
- Conectividad Red Externa (DEM, Casa Cultura, etc).
- Correo Electrónico Institucional
- BD Base de Datos Institucional
- Sitio Web Municipal

4.1° CORTES EN EL SUMINISTRO DE ENERGÍA ELÉCTRICA

Acciones Preventivas a la Contingencia

- Contar con dos generadores eléctricos para continuidad en el servicio de lugares críticos como son atención de público, cajas, equipos de comunicación, telefonía y servidores.
- Contar con UPS de emergencia que suministre energía regulada en los puntos críticos de computación del Municipio, centro de cableado, comunicaciones y telefonía.
- Supervisar regularmente que la UPS cumple con su objetivo.
- Contar con equipo de emergencia contra incendios en los lugares críticos del Municipio.
- Contar con tierras físicas exclusiva para los equipos de informática.
- Contar con un procedimiento de operación en caso de un mal funcionamiento de la UPS.
- Determinar semestralmente el tiempo efectivo y real de respaldo del UPS.
- Contar con un procedimiento para reportar el incidente a las áreas involucradas (Edelaysen, Proveedores de Mantenimientos eléctrico, etc.)
- Contar con un procedimiento para notificar a los usuarios de sistemas críticos, para la probable baja de los servicios de telecomunicación.
- Contar con procedimiento de ejecución de respaldos de emergencia a la información del servidor de datos del Municipio.
- Contar con una tabla de claves (nros . de teléfonos) de prioridades para dar aviso a los usuarios prioritarios con el fin de optimizar tiempo y recursos.
- Asignar jerarquía a los equipos computacionales, para planificar acciones mayores para darlos de bajas y reemplazarlos.

Acciones Durante la Contingencia

<u>En caso de interrupción del suministro eléctrico en lapsos cortos consecutivos:</u>

- Monitorear el UPS cada 20 min. para programar acciones mayores.
- Valorar la decisión de dar de baja (apagar) los equipos activos y/o servicios para evitar daños y/o pérdida de información y de equipos.

En caso de una interrupción del suministro eléctrico no mayor a una hora:

- Comunicarse con la empresa proveedora del servicio eléctrico, para validar el tiempo de corte de energía.
- Monitorear el UPS cada 10 min. para programar acciones mayores.
- Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso.
- Desconectar electrodomésticos (cafeteras, equipo de sonido, estufas eléctricas, ventiladores, etc.)
- Contar con los procedimientos para dar de baja los equipos activos.

En caso de una interrupción del suministro eléctrico mayor a una hora:

- Dar aviso de la contingencia a los usuarios prioritarios (Licencias Conducir, Permisos Circulación, DEM).
- Preparar el apagado de los equipos prioritarios (Servidores).
- Monitorear la UPS para programar acciones mayores (apagar todos los equipamientos de Informática).

Acciones Después de la Contingencia

- Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para restablecer los equipos de comunicación y servidores.
- Restablecer los equipos de comunicación y servidores que se dieron de baja, en forma paulatina.
- Validar el correcto funcionamiento de los equipos de comunicación y servidores.
- Notificar a los usuarios afectados el restablecimiento de los servicios y su condición.
- Identificar y evaluar los daños de los equipos de comunicación, servidores, UPS, y canalizarlos a las áreas involucradas.

4.2° INCENDIOS

Acciones Preventivas a la Contingencia

- Contar con extinguidores cargados en cada una de las áreas.
- Capacitación del personal de cada área para el uso adecuado de extinguidores.
- Contar con señalamientos de rutas de evacuación.
- Contar con lámparas emergentes con batería.
- Contar con sistemas de alarmas.
- Contar con respaldos internos y externos de los servidores (Se encargará Informática).

- Contar con respaldos de la información importante del disco duro de cada equipo de informática (Se encargará cada Usuario).
- Apagar servidores no prioritarios.

Acciones Durante la Contingencia

- Utilizar los extinguidores por personal capacitado.
- Respetar los señalamientos de rutas de evacuación.
- Si es necesario, utilizar lámparas emergentes con batería.
- Activar el sistema de alarmas.
- Asegurar que se tengan los respaldos externos de los servidores
- Apagar servidores.

Acciones Después de la Contingencia

- Realizar un reporte de los daños
- Analizar el plan de contingencias y realizar las modificaciones correspondientes.

4.3° FILTRACIÓN DE AGUA Y HUMEDAD

Acciones Preventivas a la Contingencia

- Dar mantenimiento preventivo una vez por año con impermeabilizantes a los techos y paredes donde exista el riesgo de humedad.
- Colocar en lugares seguros el hardware, software y documentos importantes.
- Apagar equipos de computación, desconectándolos del suministro eléctrico.
- Contar con bolsas de plástico para cubrir equipos de telecomunicaciones, servidores y documentos importantes que puedan mojarse.
- Contar con bolsas de plástico para cubrir equipos, impresoras y documentos importantes que puedan mojarse (Se encargará cada Usuario).

Acciones Durante la Contingencia

- Colocar en lugares seguros el hardware, software y documentos importantes.
- Apagar equipos de computación y desconectarlos de la red eléctrica.
- Cubrir con bolsas de plástico equipos de computación, servidores y documentos importantes que puedan mojarse.

Acciones Después de la Contingencia

- Realizar un reporte de los daños
- Analizar el plan de contingencias y realizar las modificaciones correspondientes.

4.4° DOCUMENTOS NECESARIOS PREVIOS A LAS CONTINGENCIAS.

- Contar con una copia del inventario del mobiliario y equipo existente en el área.
- Contar con un listado de configuraciones del centro de informática (configuración física de switch, router, modem, etc.).

ARTICULO 2° Encárguese al Comité de Gobierno Electrónico Local el seguimiento, supervisión y cumplimiento del presente Reglamento.

ANÓTESE, COMUNÍQUESE Y TRANSCRIBASE el presente Reglamento a las Direcciones, Departamentos, Secciones y Oficinas Municipales, sin perjuicio de quedar una copia a disposición y para conocimiento público en la Secretaría Municipal, hecho ARCHIVESE.

CARLO GHISONI HUTT
Alcalde (S)

PATRICIO RAMOS ROJAS
Secretario Municipal (S)

JCF/RGE
Distribución:
- ✓ Todas las Direcciones Municipales (11)
- ✓ Contraloría Regional de Aysén
- ✓ Oficina de Partes y Archivo