I.MUNICIPALIDAD DE COLINA
SECRETARIA MUNICIPAL

DECRETO Nº : E-1922/2009 /

Colina, 19 de noviembre de 2009

VISTOS: Estos antecedentes: Ley Nº 19.880 de fecha 29 de mayo de 2003, Ley de Procedimientos Administrativos; Las facultades que me confieren los artículos Nos. 59 y 63 de la Ley Nº 18.695, Orgánica Constitucional de Municipalidades,

DECRETO:

1.- APRUEBESE el siguiente **MANUAL DE PROCEDIMIENTOS Y POLITICAS DE LA UNIDAD DE INFORMATICA**

1.- PROCEDIMIENTO INTERNET Y CORREO ELECTRÓNICO

CAPITULO I

PROCEDIMIENTO PARA EL USO DE INTERNET EN LA MUNICIPALIDAD DE COLINA

Las políticas y condiciones expresadas en este documento consideran los derechos y obligaciones de los Usuarios de Internet. Este documento establece principios operativos y políticas de uso aceptable relacionadas con el uso de Internet de parte del usuario y la conexión y servicios que posee este Municipio.

General

Internet es una asociación voluntaria de usuarios interesados y dispuestos a intercambiar información y datos con otros usuarios de Internet. No existe por ahora ningún grupo gobernante o reglamentario de los principios, políticas y procedimientos de uso de Internet o de la información y datos adquiridos vía Internet.

Para facilitar la relación contractual, entre los usuarios y la responsabilidad que se tiene con el municipio (que provee el servicio), se definen un protocolo de trabajo basados en principios y políticas a fin de establecer pautas operacionales y estándares aceptables de uso de Internet. A este respecto los usuarios deben cumplir en lo siguiente, como "Principios Reguladores del Uso Aceptable de Internet por el Usuario":

1. **Responsabilidad y Respeto.** Internet es una red mundial concebida para ser usada por personas con criterio formado. El usuario reconoce este principio y se compromete a actuar con respeto, cortesía y responsabilidad en todo momento dando el debido reconocimiento a los intereses y derechos de otros grupos usuarios de Internet. Esta pauta general conlleva en ella las siguientes responsabilidades específicas:

   a) **Conocimiento de Internet.** El Usuario se compromete a adquirir un conocimiento básico de Internet, sus principios operativos y procedimientos.
   b) **Usos Impropios.** El Usuario evitará la violación de ciertas pautas generalmente aceptadas sobre el uso de Internet como lo son la prohibición de correo en masa, publicidad en masa, piratería o copia de software, "mail bombing" (correo destructivo), spam o cualquier otro método o intento de negar servicio o acceso a otros usuarios, e intentos de violación de seguridad en sitios de terceros.

      No se debe bajar desde Internet, ni instalar ni utilizar programas que vayan acompañados de un contrato de licencia, a menos que se hayan aceptado los términos de esos contratos y se cancelen los respectivos derechos. Lo anterior es con el fin de evitar futuras multas por el uso indebido de programas protegidos por las leyes que protegen la propiedad intelectual.
      En cuanto a las transacciones comerciales por Internet, la Municipalidad no asegura, garantiza ni respalda ningún producto o servicio vendido o comprado por alguno de los usuarios a través de este medio. La adquisición de un producto o servicio a través de Internet es una transacción comercial personal realizada entre el usuario y un tercero, cualquier cuestión o disputa que se pueda tener acerca de dicho producto o servicio deberá ser tratada y resuelta directamente entre ellos.
   c) **Aceptación de las Leyes Locales.** El Usuario se asegurará que su uso de Internet está permitido por las leyes y normas legales del país pero no limitadas a aquellos principios de ley que protegen contra el uso de marcas registradas, secretos de intercambio, información propietaria u otro tipo de derechos de propiedad intelectual, difamación, invasión de propiedad, interferencia técnica, y exportación de datos técnicos o militares a paises prohibidos.
   d) **Validación de la Información.** El Usuario es responsable para validar la integridad de la información y datos que recibe o transmite a través de Internet. Además el usuario debe ser conciente que la información y datos que recibe desde Internet pueden afectar la operatividad de su sistema computacional y de los datos y programas allí contenidos.
   e) **Seguridad.** Se requiere que el Usuario proteja la seguridad de su cuenta y su uso. Las claves de acceso del Usuario serán

consideradas privadas y confidenciales y no serán entregadas o compartidas con ningún tercero.

f) **Discreción.** Se espera que el Usuario sea discreto en el uso y tratamiento de Información y datos en Internet y tener especial cuidado para asegurar que información sólo para aduRos no sea transmitida a usuarios adolescentes en Internet.

g) **Pornografía, Terrorismo, Discriminación Racial.** Debido a asuntos legales y sociales, NO SE ACEPTA ningún Usuario que baje, distribuya o publique imágenes, animaciones, texto o sonido con contenido pornográfico, terrorista, o de segregación racial. Si un Usuario publica, baja o distribuye cualquiera de tos ítems descritos, la Municipalidad suspenderá de inmediato la cuenta del Usuario y descontinuará el servicio para ese Usuario, sin perjuicio de las sanciones administrativas que pudiesen llevarse a cabo.

h) **Navegación.** Debido a diferentes tipos de navegación realizada por usuarios con fines personales, queda estrictamente prohibido el ingreso a páginas como facebook, fotolog y similares, como también realizar descargas directas sin haber sido autorizadas por Informática, las radios, juegos, concursos o televisión en línea son perjudiciales para el ancho de banda de Internet por lo tanto estas acciones también son vetadas lo mismo que para cualquier tipo de acción que no sea de índole laboral.

i) **Recomendación.** Cada usuario cerrara las ventanas de Internet cuando no lo este usando, igualmente cuando no este en su puesto de trabajo (colación o en comisión de servicio) , la página de inicio debe ser la municipal y no otra, la responsabilidad del uso de su computador es del que lo tiene asignado.

j) **Descargas.** Queda prohibida la instalación de software de descargas como por ejemplo: bittorrent, emule, kazaa, Ares y similares, como también el uso de aceleradores de descargas como por ejemplo: megadownload, DAP y similares.

k) **Barras hora, estado del tiempo y noticias.** Comúnmente el usuario adorna su PC con barras llamadas "sibebar" , estas aunque no crean también ocupan ancho de banda, estas también serán eliminadas.

l) **PC de propiedad particular.** Quedan para estos computadores o notebook las mismas normas descritas anteriormente, ya que por el uso de la red están sujetos a restricciones.

m) **Como nota,** el exceso de navegación por internet no solo afecta el uso de esta, si no que a la red en general alterando el uso inclusive de los sistemas.

n) **Mensajería instantánea**. En el municipio no se deben usar herramientas para este tipo de acción o directamente desde la página de correos, será sancionado el usuario que sea sorprendido chateando en las instalaciones.

CAPITULO II

PROCEDIMIENTO PARA EL USO DEL CORREO ELECTRONICO MUNICIPAL

1.- ÁMBITO DE APLICACIÓN

El presente Procedimiento tiene por objeto dictar las instrucciones y protocolos necesarios que permitan facilitar a los funcionarios de la Municipalidad de Colina de una dirección de correo electrónico de uso laboral en el dominio *www.colina.cl*.

Se hace referencia a cuentas de correo "de uso laboral'. Con ese término se pretende hacer referencia a cuentas de personas físicas, personales e intransferibles.
La integración del sistema de correo electrónico con la Base de Datos de los sistemas Municipales proporciona notables ventajas a la hora de a gestión, operación y utilización de las cuentas de correo electrónico pero ello con que todos los funcionarios han de estar integrados para realizar sus labores.

2.- PROCESO DE GENERACIÓN DE DIRECCIONES

La dirección de correo electrónico formará parte de os datos de los funcionarios Municipales de Colina, quedando integrados en la Base de Datos de usuarios y se facilitará de forma automática en la forma siguiente:

Inicialnombre+apellidopaterno@colina.cl

Siendo **Inicialnombre** la primera letra de su primer nombre y apellido una cadena de caracteres que se obtenga de apellido paterno del funcionario, tal y como se encuentran dados de alta en la base de datos de usuarios con las siguientes restricciones:

- No existirán ñ, se sustituirá por n, las vocales con tilde o diéresis se sustituirán por la correspondiente vocal sin tilde o sin diéresis. No existirán guiones.
- En los apellidos compuestos se eliminan los blancos intermedios, así por ejemplo "de las heras" quedará *delasheras*.

- La longitud máxima de la dirección de correo electrónico será de 25 caracteres, restricción esta dada por el diseño actual de la base de datos. En el caso de que una dirección de correo electrónico superara esta longitud, se truncará la cadena resultante aplicada a Apellido paterno por la derecha.

La dirección de correo electrónico se hará llegar a todos y cada uno de los funcionarios, así como la contraseña. Se dispondrá desde el Servicio Computacional de los medios en a cual podrán cambiar dicha contraseña.

3.- CICLO DE VIDA DE UNA DIRECCIÓN DE CORREO ELECTRÓNICO.

3.1 Alta de una cuenta de funcionario

En cualquiera de las situaciones que convierten a un individuo en funcionario de la Municipalidad de Colina se le facilitará una dirección de correo electrónico, y será almacenada como parte de sus datos en la Base de Datos de usuarios de la Municipalidad.

3.2 Baja de dirección de correo.

Se mantendrá la dirección de correo electrónico, indefinidamente (mientras existan los datos de un funcionario en los registros de la Municipalidad) de forma que dicha dirección no podrá ser nunca utilizada por otra persona, independientemente de que para el adjudicatario original se mantenga o no activa.

3.3 Desactivación de una dirección de correo electrónico.

Ante notificación de la Unidad de Recursos Humanos se desactivarán todas las direcciones de correo electrónico de todos los usuarios que no se encuentren registrados como funcionarios de la Municipalidad de Colina, dicha información deberá ser acreditada previamente por la mencionada Unidad.

3.4.- Borrado de buzones.

En pro a evitar el colapso del Servicio de Correo, se contemplan ciertos casos en los que se podrá proceder al borrado del contenido de los buzones. Previo a realizar el borrado se avisará mediante dos mensajes de correo electrónico que se enviarán con una semana y dos días de antelación.

- No haya sido leído en el plazo que se establezca al inicio de cada semestre.

- El tamaño del buzón supere el establecido como máximo para cada usuario.

La Municipalidad de Colina no asume ninguna responsabilidad en relación a los usuarios por los eventuales perjuicios que se pudieran causar por la eliminación de correos, mensajes u otros contenidos almacenados en los respectivos buzones.

4.- NORMATIVA GENERAL Y BUEN USO DEL CORREO ELECTRÓNICO.

Los beneficiados de cuentas de correo establecidas en este Reglamento estarán obligados a conocer y respetar los términos y condiciones de uso del correo electrónico en la Municipalidad de Colina, de acuerdo con lo establecido en este reglamento.

El incumplimiento de dichas normativas puede acarrear, la suspensión temporal o definitiva de su servicio para direcciones de correo de la propia Municipalidad de Colina, así como las sanciones que se pudieran derivarse de la normativa que en cada caso resulte de aplicación

5.- TÉRMINOS Y CONDICIONES DE USO DEL CORREO ELECTRÓNICO

En apoyo de los objetivos fundamentales de nuestra institución de Administración Municipal, se ofrece una serie de recursos de red, comunicaciones y de información a nuestros usuarios.
Se debe reconocer que la calidad de estos servicios depende en gran medida de la responsabilidad individual de los usuarios.

En caso de no entender completamente alguno de estos apartados póngase en contacto con el Centro de atención a usuarios o en el buzón informatica@colina.cl.

Las condiciones que aquí se exponen pueden ser actualizadas para adaptarse a nuevas situaciones.

1. El correo electrónico y la información Municipal son para uso profesional y no comercial. En este sentido ningún funcionario puede modificar, copiar, distribuir, transmitir, ejecutar, reproducir, publicar, conceder licencias, crear obras derivadas, ceder ni vender ninguna información, software, productos o servicios obtenidos de los registros municipales.
2. Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y buzón de correo proporcionado por nuestra organización.
3. Es una falta grave facilitar y/o ofrecer nuestra cuenta y buzón a personas no autorizadas.

4. Los usuarios deben ser conscientes de la diferencia de utilizar direcciones de correo electrónico suministradas por nuestra institución o privadas ofrecidas por cualquier otro proveedor de Internet. El campo remite de las cabeceras de correo indica el origen al que pertenece el emisor de un mensaje, por lo que hay que tener en cuenta las repercusiones. Las direcciones de la Municipalidad (del tipo Inicialnombre+apellidopaterno@colina.cl) no pueden usarse para actividades privadas, y/o actividades no relacionadas con la Municipalidad.
5. Debe de ser consciente de los términos, prohibiciones y perjuicios englobados en Articulo N°6 "Abuso de Correo Electrónico".
6. Está prohibido la utilización en nuestras instalaciones de buzones de correo electrónico (y direcciones) de otros proveedores Internet:
    - Es ilegal utilizar como enrutador de correo otras máquinas que no sean las puestas a disposición por nuestra organización.
    - Es incorrecto enviar mensajes con direcciones no asignadas por los responsables de nuestra institución y en general es ilegal manipular las cabeceras de correo electrónico saliente.
7. El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión masiva e indiscriminada de información. Para ello existen otros canales más adecuados y efectivos.
8. La violación de la seguridad de los sistemas y/o red pueden incurrir en responsabilidades civiles y criminales. Nuestra organización colaborará al máximo de sus posibilidades para investigar este tipo de actos, incluyendo la cooperación con la Justicia.
9. No es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener ésta práctica deberá de hacerlo, Si nuestra organización recibe quejas, denuncias o reclamos por estas prácticas se tomarán las medidas sancionadoras adecuadas.
10. Está completamente prohibido realizar cualquier abuso de los tipos definidos en el Articulo N° 6 "Abuso de Correo Electrónico" Además de cualquiera de las siguientes actividades:

    - Utilizar el correo electrónico para cualquier propósito comercial o financiero.
    - No se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
    - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra organización.
    - Está prohibido falsificar las cabeceras de correo electrónico.
    - Las cuentas de nuestra organización no deben ser usadas para recoger correo de buzones de otro Proveedor Internet.

11. En el caso que se acceda al correo electrónico desde la Web, www.colina.cl los funcionarios tendrán la responsabilidad de mantener la confidencialidad de su contraseña y serán responsables de todas y cada una de las actividades que realicen bajo su cuenta. Los usuarios deberán dar aviso

inmediato al centro de atención de usuarios por cualquier uso no autorizado de su cuenta u otra infracción de seguridad.

12. Estará penalizado con la cancelación del buzón, el envío a foros de discusión (listas de distribución y/o newsgropus) de mensajes que comprometan la reputación de nuestra organización o violen cualquiera de las leyes chilenas.

6.- ABUSO EN EL CORREO ELECTRÓNICO

1. Introducción
2. Definición de términos
3. Tipos de abusos.
4. Problemas ocasionados

1. Introducción

Definimos Abuso en el Correo Electrónico como las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios. Algunos de los términos habitualmente asociados en Internet a estos tipos de abuso son *spamming, mail bombing, unsolicited bulk emai (UBE), unsollcíted commercial emaíl (UCE), junk mail phishing* etc. abarcando un amplio abanico de formas de difusión.

De tos tipos de abuso englobados en abusos en el correo electrónico, el que más destaca es el conocido como spam que es un término aplicado a mensajes distribuidos a una gran cantidad de destinatarios de forma indiscriminada. En la mayoría de los casos el emisor de estos mensajes es desconocido y generalmente es imposible responderlo (reply) de la forma habitual o incluso legar a identificar una dirección de retorno correcta.

2. Definición de términos

El correo en Internet es procesado por máquinas o servidores de origen, de encaminamiento y de destino utilizando el estándar de correo SMTP. Los agentes implicados en la transferencia de correo son:

2.1 Operador de Origen:

Es la organización responsable de la máquina que encamina el mensaje de correo hacia Internet.

2.2 **Operador de Encaminamiento:**

Es la organización responsable de las máquinas que encaminan el mensaje de correo entre el operador de origen y el operador de destino.

2.3 **Operador de Destino:**

Es la organización o responsable de la máquina que mantiene el control de los buzones de los destinatarios.

2.4 **Emisor:**

Es la persona origen del mensaje. Incluso cuando el emisor es un programa o sistema operativo, habrá una o más personas que sea(n) responsable(s) del mismo.

2.5 **Receptor:**

Es la persona que recibe el mensaje. Al igual que en el caso del receptor, puede no tratarse de una persona física, pero siempre habrá al menos un responsable más o menos directo de cada dirección de destino.

2.6 **Listas de correo:**

Son receptores de correo que actúan distribuyendo el mensaje a un número de destinatarios. Se las puede considerar como una especie de encaminadoras de correo. Estas listas pueden ser gestionadas por una persona o por un proceso automático.

No se les considera emisores ni receptores propiamente dichos, ya que la lista no es ni el origen ni el destinatario final de los mensajes. Sin embargo, pueden considerarse como tal en algunos casos: por ejemplo, los mensajes de control enviados para darse de alta o baja de una lista, y las respuestas del servidor a dichas acciones. Incluso en esos casos hay una persona detrás del servidor: el administrador del mismo.

3. Tipos de abuso

Las actividades catalogadas como Abuso en el Correo Electrónico se pueden clasificar en cuatro grandes grupos:

3.1 **Difusión de contenido inadecuado.**

Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

Contenido fuera de contexto en un foro temático. Pueden definir lo que es admisible: el moderador del foro, si existe; su administrador o propietario, en caso contrario, o los usuarios del mismo en condiciones definidas previamente al establecerlo (por ejemplo, mayoría simple en una lista de correo).

Con el fin de evitar abusos en cuanto al envío de imágenes, sean éstas fotografías o dibujos o cualquier otro elemento grafico, los usuarios deberán garantizar que las personas que ahí aparecen, si las hay, y en la medida de lo posible, han dado su consentimiento para el uso de esa imagen según lo establecido en este Reglamento, incluyendo como ejemplo, la distribución, exposición pública y reproducción de dicha imagen. Esto tiene por finalidad evitar la distribución de imágenes trucadas o alteradas que perjudiquen la honra y la privacidad de las personas.

3.2 **Difusión a través de canales no autorizados.**

Uso no autorizado de una estafeta ajena para reenviar correo propio. Aunque el mensaje en si sea legítimo, se están utilizando recursos ajenos sin su consentimiento (nada que objetar cuando se trata de una estafeta de uso público, declarada como tal).

3.3 **Difusión masiva no autorizada.**

El uso de estafetas propias o ajenas para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado se considera inadecuado por varios motivos, pero principalmente éste: el anunciante descarga en transmisores y destinatarios el costo de sus operaciones publicitarias, tanto si quieren como si no.

3.4 **Ataques con objeto de Imposibilitar o dificultar el servicio.**

Dirigido a un usuario o al propio sistema de correo, En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de las líneas, de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario. Se puede considerar como una inversión del concepto de difusión masiva (1->n), en el sentido de que es un ataque (n->1)

En inglés estos ataques se conocen como mail bombing, y son un caso particular de *denial of service* (DoS). En castellano podemos llamarlos bomba de correo o saturación, siendo un caso particular de denegación de servicio.

Suscripción indiscriminada a listas de correo. Es una versión del ataque anterior, en la que de forma automatizada se suscribe a la víctima a miles de listas de correo. Dado que en este caso los ataques no vienen de una sola dirección, sino varias, son mucho más difíciles de contener.

3.5 **El Correo Electrónico no podrá ser utilizado para la realización de las siguientes acciones:**

3.5.1 Utilizar el correo electrónico en relación con encuestas, concursos listas de distribución, cadenas de mensajes, correo electrónico no deseado, spamming o cualquier otro tipo de mensajes no solicitados ni consentidos.

3.5.2 Difamar, abusar, acosar, acechar, amenazar o de otra forma de infringir los derechos (tales como los derechos de intimidad y a la propia imagen) de terceros.

3.5.3 Publicar, anunciar, cargar, distribuir o divulgar cualquier asunto, nombre, material o informaciones inapropiadas, profanas, difamatorias, obscenas, inmorales o ilícitas.

3.6.4 Publicar anunciar, cargar, distribuir o divulgar cualquier asunto, nombre, material o información que fomente la discriminación, la violencia o el odio hacia una persona en razón de su raza, religión o creencias.

3.5.5 Cargar o poner a disposición de cualquier otra forma archivos que contengan imágenes, fotografías, software u otro material protegido por las leyes de propiedad intelectual e industrial, incluyendo, a modo de ejemplo, las leyes sobre derechos de autor y marcas (o por el derecho a la intimidad y la propia imagen) a menos que el funcionario sea titular de los derechos respectivos o haya recibido todos los consentimientos necesarios para hacerlo.

3.5.6 Cargar archivos que contengan virus, archivos dañados, o cualquier otro programa o software similar que pueda perjudicar el funcionamiento de los equipos o la propiedad de terceros.

3.5.7 Descargar algún archivo enviado por otro usuario de un servicio de comunicación del que el funcionario conozca, o razonablemente debería conocer, que no pueda distribuirse de dicha forma.

3.5.8 Falsificar o eliminar avisos de derecho de autor, avisos legales o cualquier otro aviso relevante, designación o etiqueta indicativa del origen o a fuente del Software u otro material contenido en un archivo que ha descargado.

3.5.9 Infringir cualquier ley o normativa aplicable.

3.5.10 Crear una identidad falsa con el propósito de confundir a terceros.

3.5.11 Utilizar, descargar o de otra manera copiar o proporcionar (con o sin fines de lucrativos) a una persona física o jurídica, cualquier directorio o Base de Datos de los usuarios o funcionarios municipales, o cualquier otra información sobre los funcionarios y sus costumbres.

4. Problemas ocasionados

4.4.1 Efectos en los receptores.

Los usuarios afectados por el Abuso en el Correo Electrónico lo son en dos aspectos: costos económicos y costos sociales. También se debe considerar la pérdida de tiempo que suponen, y que puede entenderse como un costo económico indirecto.

Si se multiplica el costo de un mensaje a un receptor por los millones de mensajes distribuidos puede hacerse una idea de la magnitud económica, y del porcentaje mínimo de la misma que es asumido por el emisor. En lo que respecta a los costos sociales del Abuso en el Correo Electrónico debe considerarse, aparte de la molestia u ofensa asociada a determinados contenidos, la inhibición del derecho a publicar la propia dirección en medios como News o Web por miedo a que sea capturada.

4.4.2 Efectos en los operadores.

Los operadores de destino y encaminamiento acarrean su parte del costo: tiempo de proceso, espacio en disco, ancho de banda, y sobre todo tiempo adicional de personal dedicado a solucionar estos problemas en situaciones de saturación.

7.- NORMAS PARA EL USO DE CORREO ELECTRONICO

Como todo sistema de comunicación humano, el correo electrónico tiene sus normas y costumbres que todo usuario de Internet debería intentar respetar siempre, y que corresponden a los siguientes términos:

1 De:
2 Asunto:
3 Contenido de los mensajes
4 Formato de los mensajes
  4.1 Mayúsculas
  4.2 Configuración
5 Archivos adjuntos
6 Longitud de las líneas de texto
7 Responder el correo
8 Firmas automáticas

1. De:

Contiene el nombre del emisor del mensaje y su dirección de correo electrónico. Los programas de correo recogen esta información de la configuración sobre el mail que hayamos introducido, normalmente al configurar por primera vez el programa.
Nunca deberíamos poner acentos o caracteres especiales, como a "ñ' en esta parte ya que lo más probable es que el nombre llegue ilegible al destinatario debido a los computadores intermedios que recogen el correo y lo llevan de un sitio a otro y que no pueden manejar estos caracteres.

2. Asunto:

El asunto es una breve pero suficiente descripción del contenido del mensaje. En la distribución es extremadamente importante ya que por él se guiarán los usuarios para leer o no la carta.
En esta parte tampoco deberían colocarse nunca acentos, por el mismo motivo que no los debe hacer en el caso anterior.

3. Contenido de los mensajes:

Cuando enviemos un texto a distribución hay que tener muy presente que nos van a leer varias personas. Es recomendable pensar bien lo que se escribirá y evitar expresiones que pueden no ser entendidas o mal interpretadas por miembros de otras organizaciones. También debemos considerar que lo que a nosotros nos resulta gracioso a otros les puede parecer de muy mal gusto por lo que deberemos extremar el cuidado del lenguaje.

4. Formato de los mensajes:

4.1 MAYÚSCULAS. El uso de palabras enteras escritas con mayúsculas se utiliza para gritar. Por lo tanto, un mensaje escrito en mayúsculas produce muy mal efecto en quién lo lee ya que da la impresión de que el remitente está gritando.

4.2 CONFIGURACIÓN. El programa de correo debe estar configurado para enviar los mensajes en formato MIME *(quoted printable)* de esta forma el receptor podrá leer los acentos y otros caracteres especiales. En la actualidad todos los programas de correo basados en un entorno gráfico como Windows en nuestro caso, permiten el uso de acentos, por lo que éste no debería ser un motivo para no leer correctamente los mensajes por parte del destinatario.

El formato **HTML** permite enviar mensajes con tipos de letras, colores, fondo, tablas, etc. Es un sistema muy potente para facilitar la comunicación. Pero tiene el inconveniente que ocupa mucho más espacio que el texto normal por lo que puede molestar a algunos usuarios. Todos los programas de correo actuales admiten HTML, la recomendación es mandar mensajes en este formato sólo cuando sea necesario (inclusión de tablas o gráficos).

5. Archivos adjuntos:

Nunca se deben mandar archivos voluminosos sin el previo consentimiento de todos los miembros de la misma. Lo mejor es preguntar quién quiere el archivo y mandárselo personalmente a todos ellos. Por poner un ejemplo, un archivo de 1Mb distribuido a 200 destinatarios supone un tráfico de 200Mb, lo que carga innecesariamente la red y molesta en gran forma a los que no lo quieren.

6. Longitud de las líneas de texto

Debe configurarse adecuadamente el programa de correo para que las líneas no superen los 70 caracteres de ancho, ya que de otra forma los usuarios pueden recibir las lineas truncadas, haciendo difícil la lectura.

7. Responder el correo

Para responder a un correo se debe pulsar el botón de réplica que todos los programas poseen. Es conveniente citar el texto original al que se está respondiendo, borrando el texto irrelevante o al que no se responde.

8. **Firmas automáticas**

Todos los mensajes deberían ir firmados con nombre y la unidad desde la que se escribe, si es pertinente se pone también el cargo desempeñado. Debe incluirse igualmente la dirección de correo electrónico para facilitar las réplicas personales.

8.- LEY DE DELITO INFORMÁTICO

A continuación se reproduce el texto de la Ley de Delito informático en vigencia en Chile desde el 18 de Mayo de 1993.

Articulo 1

El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicara la pena señalada en el inciso anterior, en su grado máximo.

Articulo 2

El que con el animo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a el, será castigado con presidio menor en su grado mínimo a medio.

Articulo 3

El que maliciosamente altere, dañe o destruye los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Articulo 4

El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentara en un grado.

2.- PLAN DE CONTINGENCIA

Introducción

Entendemos por plan de contingencia el conjunto de procedimientos alternativos a la operativa normal de una institución o empresa, cuya finalidad es la de permitir el funcionamiento de ésta, aún cuando alguna de sus funciones deje de hacerlo como consecuencia de algún incidente tanto interno como ajeno a la organización.

Definición: Un incidente o desastre puede definirse como la interrupción prolongada de os recursos informáticos y/o de comunicación que limiten a los usuarios del sistema acceder a la información relevante para el desempeño de su labor.

Una interrupción del flujo de información puede ser activada por las siguientes causas:

- Fuego
- Explosión
- Inundación
- Terremoto
- Tormenta de alta intensidad
- Gases o material peligroso
- Robo
- Interrupción de a red eléctrica
- Fallas en la comunicación
- Huelgas
- Rotura de conductos de agua
- Hacker, virus! spam
- Etc.

Requerimientos necesarios para desarrollar el Plan de Contingencia

1. Generar una descripción de todos los usuarios del sistema.

2. Generar una nómina del personal considerado clave dentro de las operaciones del sistema informático con los datos mínimos siguientes:
   Nombre, Dirección de vivienda, Teléfonos, usuario de acceso y claves.
   Esta información deberá ser de extrema confidencialidad.

3. Cada usuario del Sistema Informático que labore en la Municipalidad tendrá asignada una cuenta de acceso en forma

individual, quien responderá personalmente por el uso que se le dé a la misma.

4. La Subdirección de Informática, designará una persona como responsable de administrar la generación del backup de los sistemas provistos por las empresas contratadas.

5. Se deberá establecer una coordinación con documento escrito, entre la persona designada por a Municipalidad y la entidad que provea el servicio de custodia y resguardo del contenido del backup. En forma bilateral.

6. No se entregará ningún backup a persona que no esté debidamente identificada como personal con autorización para tal efecto. Estas autorizaciones deberán definirse en la Subdirección de Informática y el Proveedor de almacenamiento de los backup con el conocimiento de la Dirección de Secplan.

7. Se buscará constantemente los mejores mecanismos para optimizar las operaciones de backup, resguardo y restauración cuando sea necesario.

8. La descripción y los programas ejecutables de las aplicaciones que se vayan incorporando en la Municipalidad deberán agregarse a la bodega en donde estén almacenados los backup.

9. Los diagramas de la red eléctrica, de ubicación de equipo, inventario de hardware y software, etc. Deberá incluirse en la bodega de almacenamiento de backup's.

10. Una vez identificada la ocurrencia de un evento de ésta naturaleza, la persona que lo detecte debe reportar a su jefe inmediato superior quien lo comunicará a la Subdirección de Informática quien a su vez deberá coordinar la ejecución del plan. Esta comunicación deberá hacerse a través de los canales informales y formales.

Plan de Contingencia

1. Almacenar la descripción de todos los usuarios del sistema informático que trabajan directamente en la Municipalidad, en el área de resguardo existente fuera de las instalaciones del Municipio.

2. Almacenar la Nómina del Personal Clave, para poner en marcha un plan de restauración de las operaciones informáticas, fuera de las instalaciones que ocupa el Municipio.

3. Generar un backup o respaldo de las diferentes aplicaciones existentes en la Municipalidad con base a un criterio de periodicidad predefinido de acuerdo a lo indicado en el procedimiento de respaldo.

4. Cada usuario de a red tendrá asignado un área de almacenamiento en el servidor de archivos para que respalde la información laboral asociada a sus funciones en la Municipalidad, de manera que se garantice su inclusión en el respaldo generado periódicamente.

5. El administrador de la red, haré entrega de cada respaldo, al delegado (preestablecido), de la institución responsable de su almacenamiento en un lugar diferente a as instalaciones de la Municipalidad, a través de un documento que describa el contenido del respaldo.

6. Cada respaldo deberá estar rotulado de acuerdo al procedimiento de respaldo.

7. Cuando se cambie a las personas encargadas de efectuar los respaldos, resguardo y/o restauraciones, se deberá notificar a las partes involucradas con la prontitud que sea posible.

8. Se deberá dar la capacitación al personal de la Muntcipalidad, para sensibilizarlo de la importancia de mantener el resguardo de la información para garantizar la continuidad del acceso a la información relevante a cada área funcional de la Institución en caso de desastre.

Plan de Restauración de Operaciones

1. Ante el evento de un incidente, el Subdirector de informática, con su equipo de trabajo, hace una evaluación de la interrupción de las operaciones del servicio informático para diagnosticar las características del incidente.

2. En función del resultado del análisis preliminar se contacta y coordina con el personal pertinente, indicado en la Nómina de Personal Clave para la atención de desastres informáticos Asi como informa sobre el incidente a sus superiores. Esta comunicación se deberá realizar con la prontitud que el caso amerite y mantener un sistema de información continuo hasta que los efectos del incidente queden restaurados en su totalidad.

3. Obtenido el diagnóstico descrito en párrafo anterior, el Subdirector de Informática conjuntamente con su equipo de trabajo, define la estrategia a seguir para restaurar la continuidad del servicio informático.

4. Si fuera necesario se convocará al personal relacionado con la etapa de recuperación de las condiciones de operatividad de los sistemas informáticos (Nómina de Personal Clave).

5. Se contactará al servicio de resguardo de información y recursos informáticos previstos para atender un desastre, (Para ello, el Subdirector de Informática y/o el Administrador de Sistemas contará con los contactos correspondientes).

6. Una vez se restablezca la normalidad de las operaciones, se revisarán las bases de datos, servidores, impresoras, etc (de acuerdo a la cobertura de la incidencia), para cerciorarse de que realmente se ha puesto a punto as condiciones tal como se encontraba el sistema antes del desastre.

3.- PROCEDIMIENTO DE CLAVES

Introducción

Al diseñar un esquema de políticas de seguridad, conviene dividir el trabajo en varias políticas diferentes, específicas a un campo: cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, bitácora del sistema, seguridad física, personal, etc.

• **Políticas de cuentas:** Establecen que es una cuenta de usuario de un sistema computacional como está conformada, a quien se le puede otorgar, quien es el encargado de asignarías, como deben ser creadas y comunicadas. Ejemplos:

- Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos.
- Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
- El nombre de usuario de una cuenta deberá estar conformado por la primera letra de su nombre y su apellido paterno.

• **Políticas de contraseñas:** Son una de las políticas mas importantes, ya que por lo general, las contraseñas constituyen, sino la única, la mejor forma de autentificación y, por tanto, la única línea de defensa contra ingresos fraudulentos o ataques. Estas establecen quien asignará la contraseña. que longitud debe tener, a que formato deberá apegarse, como será comunicada, etc. Ejemplos:

- La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el usuario Todas las contraseñas deberán contar con al menos cuatro caracteres.
- Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras fáciles ni que relacionen directamente al usuario, como sus iniciales, su apodo, la fecha de nacimiento, etc.; tampoco secuencias conocidas de caracteres. como "abcd", "1234" o similares datos personales ni acrónimos.

- Los usuarios no deben construir contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar, por ejemplo: "Juan 1", "Juan2", "Juari3".
- Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores, por ejemplo: "12341 "4321"
- Políticas de control de acceso: Especifican como deben los usuarios acceder al sistema, desde donde y de que manera deben autentificarse. Ejemplos:
  - Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y cifrada.
  - Esta prohibido acceder al sistema con una cuenta diferente de la propia, aun con la autorización del dueño de dicha cuenta.
  - Al momento de ingresar al sistema, cada usuario podrá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual permitirá detectar fácilmente el uso no autorizado del sistema

- **Políticas de uso adecuado:** Especifican lo que se considera un uso adecuado o inadecuado del sistema por parte de os usuarios. así como lo que está permitido y lo que esta prohibido dentro del sistema computacional.

Antes de diseñar el esquema de políticas de uso adecuado, conviene hacer las siguientes preguntas:

- (Se permite irrumpir en cuentas ajenas?
- (Se permite adivinar contraseñas?
- (Se permite interrumpir el servicio?
- (Puede leerse un archivo ajeno cuyos permisos ante el sistema incluyen el de lectura para todos?
- (Puede modificarse un archivo ajeno cuyos permisos ante el sistema incluyen el de escritura are todos?
- (Pueden los usuarios compartir sus cuentas?
- (Puede copiarse el software que no lo permita en su licencie?
- (Puede obtenerse una "licencia para hackear"?
-

La respuesta a todas estas preguntas debe ser negativa
Existen dos enfoques: permisivo (todo o que no esté explícitamente prohibido está permitido) y paranoico (todo lo que no este explícitamente permitido esta prohibido) Cual de estas elegir, dependerá del tipo de organización y el nivel de seguridad que esta requiera.
Tras haber aclarado estos últimos puntos, se puede proceder a algunos ejemplos:

- Esta terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de maquinas locales o remotas

- La cuenta de un usuario es personal e intransferible, por lo cual no se permite que se comparta ni cuenta ni contraseña con persona alguna, aun si acredita la confianza del usuario.
- Esta estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de cómputo propios o ajenos.
- Esta estrictamente prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador
- No se permite bajo ninguna circunstancia el uso de cualquiera de Fas computadoras con propósitos de ocio o lucro.

4.- PROCEDIMIENTO DE RESPALDO

Introducción

El respaldo de datos tiene como finalidad resguardar la información relevante y critica de la Municipalidad, en un medio magnético u óptico, para que en caso de indisponibilidad del servicio por falla, catástrofe de tipo incendio, inundación, terremoto o cualquiera atribuible a fuerza mayor, ésta quede a buen recaudo y pueda ser recuperada de manera simple y directa.

Los elementos a respaldar son diversos, pero se pueden clasificar en tres grupos:

Base de datos municipal, donde reside toda la información de las áreas contables, RR.HH, tránsito, seguridad, juzgado, Intranet, etc.

Software, que abarca los Sistemas de Gestión Municipal, los programas ejecutables o software de aplicación, Sistema Operativo.

Datos de usuarios, que implica la información de correos, información de la 180, datos de cuentas de usuario, configuraciones, permisos, etc.

Procedimiento

Para resguardar de manera correcta la información, se ha dispuesto la siguiente metodología de respaldo.

La base de datos se respaldará de manera diaria en los servidores principal y secundario que dispone la Municipalidad, los que están físicamente separados y por más de 5 Km.

Una vez a la semana se hará dos copias en DVD que serán entregadas y resguardadas en las dependencias de la Municipalidad y otra copia irá las bodegas de almacenamiento de IRON MOUNTAIN o la empresa que la reemplace en el futuro.

Estos respaldos permanecerán por un plazo de 5 años, al término de los cuales podrán ser destruidos, debiendo completarse un acta que refleje el detalle de la operación.

Las personas autorizadas para realizar esta labor será el encargado de soporte de la empresa CAS-CHILE S.A. de I. y el Administrador Municipal o en quien este último delegue dicha labor.

Para un registro adecuado, se deberá registrar en una bitácora os respaldos realizados, indicando a fecha, hora y funcionario.
Del mismo modo, cada DVD será rotulado con la información indicada precedentemente.

PROCEDIMIENTO DE ACCESO LÓGICO Y FÍSICO

Introducción

Al diseñar un esquema de políticas de seguridad, conviene dividir el trabajo en varias políticas diferentes, especificas a un campo: cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, bitácora del sistema, seguridad f personal, etc.

Seguridad lógica

La seguridad lógica se define como todos aquellos recursos computacionales lógicos o programas (Sistemas operativos, programas de desarrollo, bases de datos, procesadores, entre otros.) que intervienen en el manejo de la información, además de los procedimientos realizados en el manejo y administración de programas. La educación de los usuarios en el manejo correcto de los programas y la información que éstos procesan, es fundamental a la hora de medir los diferentes aspectos de la seguridad lógica, como son:

Disponibilidad de la información
La información debe estar siempre disponible a la mano del usuario que necesite de la misma,

Confidencialidad de la información

El usuario que dispone de la información debe estar previamente autorizado por el administrador del sistema, es decir que el usuario debe tener los privilegios adecuados para el acceso de la información

Integridad de la información
No se debe realizar ningún tipo de operación sobre la información por personal que no esté autorizado.

Consistencia del sistema
Los objetivos y procedimientos del sistema deben cumplirse como se planteó en el manual del sistema, cualquier cambio debe ser realizado por personal autorizado.

Autenticación
El ingreso al sistema debe ser únicamente por usuarios debidamente autorizados con os accesos y privilegios respectivos al sistema.

Control de acceso al sistema
Deben existir procedimientos o sistemas de control automatizados que le permitan al administrador conocer en cualquier momento los accesos al sistema por usuarios autorizados o no.

Auditoria de programas
Deben existir procedimientos o sistemas de control automatizados que le permitan al administrador conocer en cualquier momento las actividades reo durante los accesos a los programas por usuarios autorizados o no.
Además se debe controlar la Instalación o desinstalación de programas licenciados o no.

Seguridad física
La seguridad física se define como os mecanismos para asegurar el correcto funcionamiento de aquellos recursos físicos o equipos computacionales (Servidores, estaciones de trabajo, video cámaras. impresoras, unidades de backup, routers, switches. hubs, entre otros.) que intervienen en el manejo de los datos o información, además de los procedimientos realizados en el manejo y administración de los equipos computacionales, como también el acceso a dependencias restringidas de operación computacional.

La educación de los usuarios en el manejo correcto de la infraestructura computacional que éstos utilizan, es fundamental a la hora de medir los diferentes aspectos de la segur/dad física, como son:

Disponibilidad del equipo computacional
El equipo debe estar siempre disponible "a la mano" del usuario que necesite del mismo y siempre y cuando éste se encuentre debidamente autorizado para usarlo.

Confidencialidad del equipo computacional

El usuario que dispone del equipo debe estar pro y/amente autorizado por el personal encargado de administrar los equipos computacionales, en caso contrario deben existir los mecanismos de control adecuados.

Integridad del equipo
No se debe realizar ningún tipo de operación sobre el equipo computacional por personal que no esté autorizado, en caso contrario deben existir los mecanismos de control adecuados.

Consistencia del equipo
El objetivo y funcionamiento del equipo debe desarrollarse como se planteó en el manual de/equipo computaciona4 cualquier cambio debe ser realizado por personal autorizado.

Autenticación del equipo
El acceso al equipo computacional debe ser únicamente por personal debidamente autorizado con los medios de acceso y privilegios respectivos al equipo, en caso contrario deben existir los mecanismos de control adecuados.

Control de acceso al equipo
Deben existir procedimientos o sistemas de control, ya sean manuales o preferiblemente automatizados, que le perm al administrador de los equipos computacionales conocer en cualquier momento los accesos al equipo por personal autorizado o no.

Auditoría del equipo
Deben existir procedimientos o sistemas de control automatizados que le permitan al administrador del equipo computacional conocer en cualquier momento las actividades realizadas durante los accesos al equipo por personal autorizado o no. Además se debe controlar la instalación o desinstalación de componentes físicos al equipo.

Confidencialidad del espacio físico
El usuario que dispone del espacio físico debe estar previamente autorizado por el administrador del espacio físico.

Control de acceso a las áreas restringidas de operación computacional Deben existir procedimientos o sistemas de control automatizados que le permitan al administrador del espacio físico conocer en cualquier momento los accesos a/área respectiva por personal autorizado o no.

5.- PROCEDIMIENTO DE IMPRESIÓN

Introducción

Dentro de la red computacional municipal existe una variedad de dispositivos que permiten y facilitan el funcionamiento de ésta y que permiten realizar de mejor forma las labores de los funcionarios. Como ejemplo, se pueden mencionar los PC Servidores, Impresoras, etc. Cada usuario de a Municipalidad tiene asignada una impresora de red, de tipo láser en la que puede imprimir todos aquellos documentos de tipo laboral que requiera y/o se e encomiende.

Como todos los recursos, éstos son limitados y tienen una vida útil determinada por el fabricante. Para el caso de as impresoras, requiere de dos insumos claramente identificados: papel y toner. Ambos son directamente dependientes, pues a mayor impresión de hojas, mayor es el consumo de toner. De igual forma, la impresión de documentos con mucha gráfica e imágenes produce un mayor consumo de toner.

Normativa de uso de Impresoras.

- Cada impresora debe estar correctamente configurada para permitir a impresión en dos tipos de papel básicos; estos son Carta y Ejecutivo(J
- • El usuario debe privilegiar la impresión del mínimo de copias posible, siendo siempre los borradores o aquellos documentos de más de 10 páginas, impresos a dos caras.
- Se evitará emitir copias excesivas de borradores y privilegiar el trabajo en el computador hasta tener el documento completo y en el formato definitivo.
- El uso persistente de la impresora provoca, además del consumo excesivo ya indicado de papel y toner (y energía), una menor vida útil de los componentes, una mayor tasa de falla y por ende, un mayor tiempo fuera de uso por reparaciones, quedando fuera de uso cuando realmente se necesita.

Finalmente, las impresoras deben ser apagadas al término de a jornada laboral y encendidas al comienzo de ésta.

6.- PROCEDIMIENTO DE REVISIÓN PARA DISPOSITIVOS EXTERNO

Introducción

El uso de dispositivos de almacenamiento de información como pendrive, cámaras fotográficas, celulares o discos duros externos, es cotidiano en el trabajar del usuario y para mantener la integridad de la información y el buen funcionamiento de los equipos informáticos.

Procedimiento

Para resguardar de manera correcta la información, se ha dispuesto la siguiente metodología de revisión.

Cada Pendrive, cámara fotográfica o disco duro externo antes de ser explorado debe ser escaneado por el usuario.

No debe ejecutarse jamás algo que el usuario desconozca, ya que puede ser un programa con fines maliciosos.

Los teléfonos celulares quedan prohibidos para ser conectados a los equipos municipales, todo software que este instalado se eliminara.

Cada vez que el usuario desconozca del tema debe llamar a informática para orientarlo sobre este, cabe recordar que cada usuario es responsable de su PC.

ANOTESE, COMUNIQUESE Y ARCHIVESE

MARIO OLAVARRIA RODRIGUEZ
ALCALDE

CARLOS GARCIA LECAROS
SECRETARIO MUNICIPAL
MOR/DSR/CGL/EAQ/phf
DISTRIBUCION:

- Administradora Municipal
- Asesoría Jurídica.
- Dirección de Administración y Finanzas.
- DIDECO
- Dirección de Aseo y Ornato.
- DOM
- SECPLAN
- Dirección de Operaciones.