CONTROL INTERNO - SECRETARIA DE PLANIFICACION

Republica de Chile
Provincia de Talca
Municipalidad de Constitución

DECRETO EXENTO Nº 1602 / E /

MAT.: Aprueba Reglamento sobre la Seguridad de la Información de informática Municipal.

Constitución, 12 ABR. 2024

V I S T O:

1. La Ley 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N° 18.695, Orgánica Constitucional de Municipalidades y sus modificaciones; la ley N° 19.880.- establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; La Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N° 18.883.- aprueba Estatuto Administrativo para los Funcionarios Municipales; el Reglamento N°1 de Organización Interna de la Municipalidad de Constitución del año 2020 y la Ley Orgánica Constitución de Municipalidades. El decreto N°2.564/R de fecha 29 de junio 2021, que declara asumo de funciones al Alcalde de la Municipalidad de Constitución Don Fabian Pérez Herrera;

CONSIDERANDO:

1. La Auditoria a las Tecnologías de la Información y Comunicaciones, TIC, realizada por la contraloría General de la República, según el Informe Final N° 19/2019 del 3 de Julio de 2019.

2. Las Observaciones que aún se mantiene pendientes y que esta Dirección de Control, mediante memorándums N° 51 y N° 167 del 16 de enero y 14 de febrero ambos del año 2024 , requirió a la unidad de informática subsanar.

3. Que, mediante la Presente dictación del presente Reglamento sobre normas de informática, se subsanan en parte las observaciones que aun se mantienen pendientes, y que aún se encuentran pendientes en el portal se seguimiento y observaciones y apoyo de la CGR.

DECRETO:

1.- APRUÉBASE, El siguiente reglamento sobre la seguridad de la Información de informática municipal.

César Mauricio
Arellano Sepúlveda
9697167-2
carellano@constitucion.cl

Firmado electrónicamente según Ley 19799
el 12-04-2024 a las 10:12:35 con Firma Electrónica Avanzada
Código de Validación: 1712931155936
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

REGLAMENTO SOBRE LA SEGURIDAD DE LA INFORMACION DE INFORMÁTICA MUNICIPAL

El presente documento, viene a explicar la descripción de procesos y actividades que se deben seguir en la realización de servicios del Departamento de Informática perteneciente a la I. Municipalidad de Constitución.

1. **INTRODUCCIÓN**

2. **NORMAS DE USO DE LOS COMPUTADORES**

3. **SOLICITUDES DE ADQUISICIÓN DE EQUIPOS**

4. **MANTENCIONES**
   - 4.1 Preventiva
   - 4.2 Predictiva

5. **NORMAS GENERALES EN EL USO DE SERVICIOS, SOFTWARE Y HARDWARE MUNICIPAL**
   - 5.1 Objetivo
   - 5.2 Normas generales de Uso
   - 5.3 Normas de Hardware
   - 5.4 Normas de Software
   - 5.5 Servicio al Usuario
   - 5.6 Política de Seguridad De La Información
   - 5.7 Políticas de Control de Acceso

6. **NORMAS DE USO DE INTERNET**
   - 6.1 Objetivo
   - 6.2 Políticas
   - 6.3 Normas de Buen uso y Comportamiento

7. **NORMAS DE USO DEL CORREO ELECTRÓNICO INSTITUCIONAL**
   - 7.1 Objetivo
   - 7.2 Políticas
   - 7.3 Normas de Generación de Cuentas
   - 7.4 Normas y Sugerencias de Buen uso y Comportamiento

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

1.- INTRODUCCIÓN

EL uso de La Tecnología Informática y de Comunicaciones (TIC) contribuye a superar los niveles de productividad y eficiencia Municipal, siendo la misión del Departamento de Informática, perteneciente a Secretaría Comunal de Planificación, proveer de servicios necesarios para brindar al usuario el máximo apoyo cuando se requiera conforme al presente reglamento. Para ello, los usuarios/funcionarios deben conocer las políticas y normas establecidas, que deben definirse clara y explícitamente para poder determinar eventuales responsabilidades administrativas.

2.- NORMAS DE USO DE LOS COMPUTADORES (equipos)

El usuario, recibirá de ser necesario y previo V°B° de su jefatura los equipos y servicios necesarios para su desempeño, este se hace responsable del cumplimiento de las normativas vigentes del adecuado uso de los equipos, software y datos que se les entreguen.

Se implementarán políticas y normas que garantizan el buen desempeño de los equipos computacionales en la red del Municipio, las cuales serán presentadas a continuación.

El Departamento de Informática es el área responsable de atender las necesidades y entregar la asesoría en el manejo correcto de software, configuración de equipo para impresión o conexión a Internet, mantenimiento del equipamiento informático instalado y soporte técnico para la organización.

3.- SOLICITUDES DE ADQUISICIÓN DE EQUIPAMIENTOS

Será necesaria la confección de una ficha técnica, para la adquisición de cualquier equipamiento computacional (Características de impresoras, scanner, computador, etc.) en la que se plasmará lo solicitado por el funcionario previa V°B° por el jefe(a) de la Dirección y/o jefe(a) de Departamento, según corresponda, la ficha será realizada por la Unidad de Informática y entregada al Departamento que la solicite.

Teniendo las Características se remitirá mediante memorándum la solicitud a SECPLAN, y este a Administración Municipal para su V°B, finalmente deberán ser enviada a la unidad de adquisiciones de la Dirección de Administración y Finanzas, para su compra.

Es responsabilidad del Departamento de Informática la instalación del equipamiento computacional, como también la realización de las pruebas técnicas respectivas y la respectiva inducción de uso.

Es responsabilidad de los usuarios cuidar y mantener el buen estado de los equipos computacionales.

Todo equipamiento computacional (impresoras, scanner, computador, etc.) perteneciente al Municipio deberá permanecer en el lugar asignado, ya que frente a una auditoria se debe conocer el lugar físico donde se encuentra.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

Sólo se podrá trasladar temporalmente cualquier equipamiento computacional previo visado del Departamento de Informática el cual dará curso a dicha petición, informando de ello al encargado de inventario.

Sera responsabilidad del propio departamento o unidad, gestionar las bajas del equipamiento computacional, que se encuentre en mal estado, con falla u obsoleto y que este asignado en su inventario, previo V°B° del Departamento de Informática.

Referente al equipamiento computacional que fuese dado de baja y pueda ser reutilizado, la Unidad de Informática evaluara si los componentes de este equipamiento pueden ser reutilizados, dejándolos como piezas de repuestos.

4.- MANTENCIONES

Las mantenciones se realizan sólo a equipos, sistemas y software instalados por el Departamento de Informática.

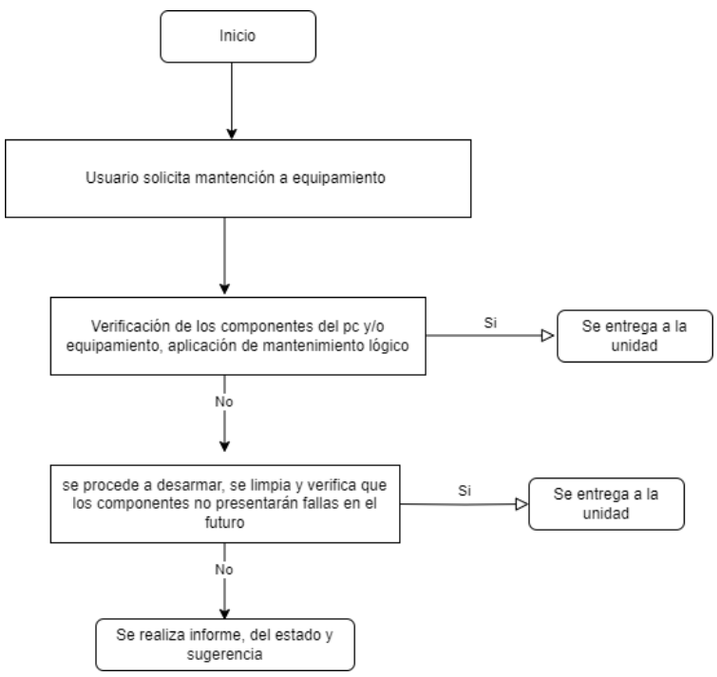
Se realizarán dos tipos de mantenciones de hardware y software, siendo estas:

4.1. Preventiva: Se dispondrá de un calendario de mantención preventiva para anticiparse a problemas o situaciones riesgosas que perjudiquen el buen funcionamiento de los servicios existentes.

4.2. Predictivo: Debido a permanentes fallas de un equipo o sistema computacional, la unidad de informática buscará la causa de dicha falla y procederá a su eliminación mediante la implementación o incorporación de nuevas tecnologías o restableciendo el sistema operativo del equipo si fuese necesario.

Esta mantención deberá ser coordina con la unidad, quedando registrada “Ficha de Mantención”, Anexo N°1.

Diagrama Mantención de Equipo.



Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

5.- NORMAS GENERALES EN EL USO DE SERVICIOS, SOFTWARE Y HARDWARE MUNICIPAL

5.1- OBJETIVO

El objetivo de estas normas es entregar las reglas adecuadas que permitan lograr un trabajo más seguro y eficiente, facilitando tanto las tareas del usuario, como las del personal de Informática.

Estas normas deben ser conocidas y respetadas por todos funcionarios/usuarios. La violación de alguna de ellas puede desencadenar en medidas disciplinarias para el usuario que ha incurrido en la falta.

Por consiguiente, el usuario será responsable de conocer y responder estas normas.

5.2.- LAS NORMAS GENERALES DE USO

Los equipos computacionales deben manipularse según se establece en el presente reglamento y conforme a las instrucciones de la Unidad de Informática, siendo el único autorizado para intervenir los equipos, ya sea para instalar software y sistemas que los usuarios requieran.

La Información contenida en los computadores es de propiedad del Municipio y en ningún caso podrá utilizarse para fines personales.

Queda prohibido:

1. Manipular alimentos sobre los equipos computacionales teniendo especial cuidado de no derramar liquido en ellos.

2. Exposición deliberada de los equipos, a polvo ambiental.

3. Exponer deliberadamente a temperaturas extremas pues altera el normal funcionamiento de los equipos.

4. La utilización de los equipos computacionales con fines recreativos, ni con fines particulares.

El usuario en lo posible debe mantener la limpieza externa de los equipos computacionales.

5.3- NORMAS DE HARDWARE

El usuario no deberá abrir los equipos computacionales, como tampoco sacar o cambiar componentes de estos mismos.

Evitar instalar equipos sin la supervisión y autorización expresa del Departamento de Informática.
Cada computador es de responsabilidad del funcionario que lo tiene asignado.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

5.4.- NORMAS DE SOFTWARE

El equipo entregado al usuario contendrá en el disco duro el software básico asociado al funcionamiento y a las tareas desarrolladas, siendo estos los definidos por el Departamento de Informática como mínimo para su operación.

Cualquier otro software que requiera el usuario, deber ser solicitado al Departamento de Informática el cual evaluará si es necesaria, y posible su instalación.

La solicitud de algún sistema o software propietario o licenciado que se requiera debe ser enviada por el jefe de Departamento respectivo a la unidad de Informática, quien de acuerdo con los planes de implementación y las prioridades aprobará y derivará a SECPLAN, para su V°B° Final, posteriormente y de ser aprobado se enviará a Adquisiciones para su compra.

En el caso de adquisición de alguna licencia, software o hardware, se deberá enviar copia de factura y Orden de Compra al Departamento de Informática, para mantener un registro de las Licencias, en caso de ser solicitada en alguna Auditoria.

El usuario deberá mantener los archivos de su equipo ordenados, siendo de su responsabilidad conservar espacio suficiente en el disco para poder ejecutar sus aplicaciones, sin perjuicio de lo anterior podrá solicitar respaldo de los archivos como se indicará más adelante.

El departamento de informática instalará y mantendrá los softwares y/o sistemas que este haya desplegado en los equipos de propiedad del municipio.

Respecto la propiedad intelectual y licencias. El usuario no podrá copiar o distribuir programas sin licencias.

La Instalación de un software y/o sistema no autorizado por el departamento de informática puede provocar problemas graves de seguridad para la red municipal, siendo responsabilidad absoluta del usuario del equipo.

PROHIBICIONES:

No se podrá copiar o “piratear" sistemas o programas que su uso implique la propiedad de una licencia de uso, es ilegal y está estrictamente prohibido, ya que puede significar para el Municipio sanciones legales.

Los programas de dominio púbico (Shareware, Freeware), pueden usarse solo previa instalación por parte del Departamento de Informática.

El usuario no podrá alterar software y/o sistemas que se encuentran a su disposición.

La instalación y uso de software de juegos NO será autorizado baja ninguna circunstancia, por la que su uso está prohibido.
No se podrá cambiar la configuración de los equipos, la que ha sido predeterminada por el Departamento de Informática.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

Ninguno de los programas registrados debe instalarse en otro sistema o computador diferente del que se encuentre licenciado.

El usuario no deberá Instalar software no autorizado, (ni siquiera un simple protector de pantalla), ya que puede infectar el equipo y red.

Esto puede ocasionar pérdidas importantes de información, como también consecuencias irremediables.

Se prohíbe la instalación individual de programas, (excepto previa autorización del Departamento de Informática) como, por ejemplo:

- ✓ Demostraciones de Proveedores.
- ✓ Instalación de nuevas versiones para un software ya adquirido.
- ✓ Utilización de programas de diagnóstico.

Se prohíbe la conexión de computadores personales a la red Municipal, salvo que este haya sido verificado y visado por el Departamento de Informática.

5.5.- SERVICIO AL USUARIO

El Departamento de Informática tiene como función dar soporte computacional a los distintos Departamentos y Direcciones Municipales.

El Departamento de Informática se preocupará de mantener actualizado el software existente en los equipos computacionales de dominio del Municipio; siempre y cuando el equipo sea compatible.

El Departamento de Informática realizara mantención preventiva, correctiva a los equipos,
Programas y software pertenecientes al Municipio y que sean de su responsabilidad.

El Departamento de Informática programará, elaborará calendarios de planificación de mantención computacional para mantener al día los equipos.

Será de responsabilidad del Departamento de Informática prestar ayuda y asesoraría sólo cuando sea de temas que competan al Municipio.

Todo software instalado sin autorización podrá eliminarlo el Departamento de Informática.

El Departamento de Informática verificará la integridad, configuración y estado de los equipos, y que estén en el lugar asignado o autorizado.

5.6.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Al entregarse un equipo nuevo o reparado, este poseerá una contraseña predeterminada, que deberá cambiarse al ingresar por primera vez, será de uso personal y responsabilidad del usuario recordar esta contraseña.

La contraseña deberá tener las siguientes condiciones:

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

- Longitud Mínima de 8 Caracteres
- Letras en mayúsculas: A a Z
- Letras en minúsculas: a a z
- Números: 0 a 9
- Símbolos: (espacio) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _` { | } ~ (

La contraseña tendrá una duración de 180 días, pasado este tiempo el equipo solicitará al usuario el cambio de contraseña, por una nueva que no haya sido usada con anterioridad.

Se recomienda no usar contraseñas que sean fácilmente deducibles.

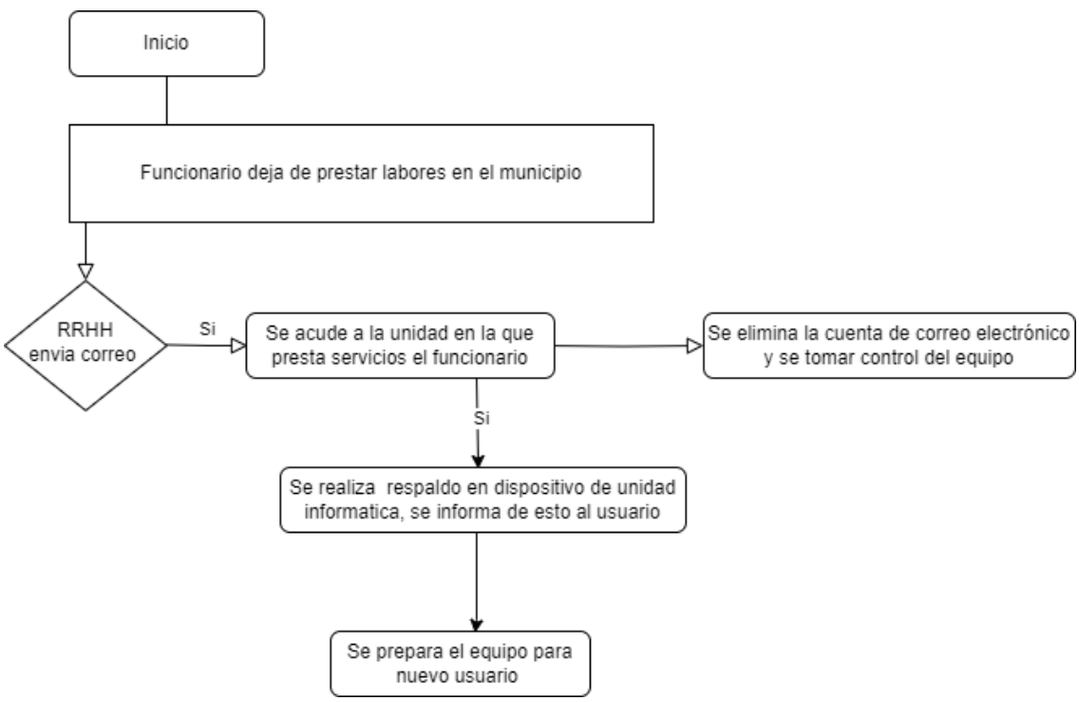
Los usuarios deberán utilizar únicamente los servicios para los que están autorizados. No utilice la cuenta de otra persona, ni intente apoderase de claves de acceso de otros, como tampoco intentar burlar los sistemas de seguridad bajo ningún punto de vista.

Será responsabilidad del usuario respaldar la información que se encuentra en el disco duro de su equipo (“Mis documentos, Escritorio, etc.) a través de los equipos de respaldo que cuenta en cada dirección, departamento y oficina (Discos externos, Pendrive, etc.).

Cada usuario de un Computador será responsable de mantener los debidos resguardos en cuanto a la confidencialidad de los datos almacenados.

En el caso de que se necesite eliminar o bloquear las credenciales de acceso de los funcionarios a servicios que estén bajo el control de la unidad informática, ya sea porque estos cambian de función o dejan de prestar servicios al municipio, se deberá avisar de forma anticipada a la unidad, para tomar los resguardos necesarios de la información, ya sea respaldándola o impidiendo su destrucción.

Para estos efectos la dirección de RRHH o el director de la unidad, deberá avisar por correo electrónico a la unidad con antelación.



Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

ACCESO Y PUBLICACIÓN PÁGINA WEB

Referente al acceso y publicaciones en la Página Web Institucional, solo el Departamento de Informática, tendrá el acceso para ingresar noticias municipales, en el caso que algún departamento debe publicar algún aviso adicional a lo ya mencionado, se deberá enviar un correo electrónico a la cuenta soporte@constitucion.cl, donde deberán indicar una reseña del contenía, fecha a publicar y adjuntar una imagen.

Por seguridad, solo se podrá configurar el acceso a FTP a los usuarios que deban publicar información en el sitio, no se entregará la contraseña, quedando la aplicación con las credenciales guardadas, se prohíbe cualquier intento fraudulento de obtención de dichas credenciales.

Se prohíbe la instalación ya sea de Plug-in, Template para wordpress, en la Página Web Institucional, sin haber pasado por la supervisión del comportamiento y VB del Departamento de Informática, ya que este podría afectar el buen funcionamiento de la página web.

5.7.- POLÍTICAS DE CONTROL DE ACCESO.

I. Gestión de usuarios y permisos.

Se establecerán restricciones y regulaciones para asignar y utilizar permisos, ya que el mal uso de los sistemas es la principal causa de fallas en los mismos.

Los sistemas que admitan múltiples usuarios y necesiten protección contra accesos no autorizados deben implementar un proceso formal de autorización para controlar la asignación de permisos. Para lograrlo, se deben seguir los siguientes pasos:

a) Se deberá contar con un registro de los usuarios que considere los permisos de acceso a los sistemas municipales propios o arrendados, en dicho registro se podrá actualizar el estatus de estos usuarios y permisos. Dicho registro será considerado como proceso formal de autorización de la siguiente manera, la unidad requerida enviará un documento formal a Recursos Humanos, realizando la solicitud, posterior a esto RRHH enviará a la unidad informática el requerimiento, para ser registrado y este será enviado a Proexsi con copia a Control Interno.

b) Identificar los usuarios y permisos asociados a cada uno de los sistemas, por ejemplo, sistema contabilidad, conciliación bancaría, sistema de gestión documental sistema administración de base de datos y aplicaciones, etc., y las categorías de personal a las cuales deben asignarse los permisos.

c) Solo se asignarán permisos de usuario, cuando se cuente previamente con la autorización del jefe directo del individuo al que se le asignarán los permisos a un sistema o recurso municipal, cualquiera sea la intensidad del uso de los mismo, esta se realizara mediante el acto formal (Memo), donde se especifique el tipo de permiso (Lectura, Escritura, Modificación), de acuerdo a su función.
Ejemplo: permanente, temporal, esporádico y/o eventual.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

d) Mantener un proceso de autorización y un registro de todos los permisos asignados. Los permisos no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

e) Establecer un periodo de vigencia para el mantenimiento de los permisos, luego del cual los mismos serán revocados tanto en los sistemas de gestión como en los respectivos equipamientos si fuese necesario.

La jefatura, o el jefe directo, aprobarán la asignación de permisos a usuarios y solicitarán su implementación, lo cual será supervisado por el responsable de Seguridad Informática, y se enviará una copia de resolución que modifique el permiso a Control Interno.

En el caso de que se deba eliminar o bloquear los derechos de acceso para los funcionarios, cuando estos cambien de función o dejen de prestar servicios, se deberá oficializar por parte de Dirección de RRHH o Jefe Directo, mediante documento formal o correo electrónico, para tomar la medida correspondiente de los accesos, los cuales serán registrados y enviado copia a Control Interno de la misma manera que fueron solicitados los permisos de acceso.

REVISIÓN DE LOS DERECHOS DE ACCESO DEL USUARIO.

A fin de mantener un control eficaz en el acceso de los datos y servicios de información, El Encargado de Seguridad de la Información de la Municipalidad realizará un proceso formal para revisar los derechos de acceso de los usuarios el cual deberá ser realizado cada 6 meses.

Se deberán contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios.

b) Revisar las autorizaciones de permisos de acceso total.

c) Revisar las asignaciones de permisos, a fin de garantizar que no se obtengan permisos no autorizados.

d) En caso de contratación, remoción o término de contrato se actualizarán los derechos de acceso, una vez recibido dicha instrucción formalmente, mediante el medio habilitado por el superior jerárquico o por el Director de RRHH.

e) El encargado de seguridad, una vez informado por el medio habilitado de cualquier cambio de funcionarios dentro de servicio, hará la revisión pertinente a los permisos de dicho funcionario en los sistemas y el respectivo equipo para adecuarlos a su nueva función.

Se realizará 1 vez al año auditoría a todos los sistemas computacionales municipal y arrendados respecto al control de acceso, según los permisos registrados.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

POLÍTICAS DE SEGREGACIÓN DE FUNCIONES EN LOS SISTEMAS

Se deberá considerar una nómina a donde se tenga identificado las cuentas de los usuarios que posean acceso a los sistemas computacionales externos o arrendados, donde este asociado las labores que cumple el funcionario.

EQUIPOS ASIGNADOS A LOS USUARIOS.

Los usuarios deberán garantizar que los equipos asignados sean protegidos adecuadamente.
Los equipos instalados en áreas comunes, por ejemplo, estaciones de trabajo o servidores de archivos, requerirán una protección específica contra accesos no autorizados cuando se encuentran desocupados.

El Encargado de Seguridad Informática debe trabajar mancomunadamente con la dirección de RRHH para organizar sesiones de capacitación para todos los usuarios. Estas sesiones tienen como objetivo enseñarles sobre los requisitos y pasos necesarios para proteger los equipos asignados, y también sobre sus responsabilidades en la aplicación de estas medidas de seguridad.

La unidad de informática configurará cada equipo computacional con las siguientes sesiones, la primera para el usuario y la segunda que se mantendrá latente para la unidad de informática, quien la podrá en un futuro para auditoria y administración.

Los usuarios finales deberán cumplir con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
b) Mantener apagados los equipos cuando no se esté ocupando.

c) No facilitar su equipamiento a terceros sin reportarlo a la unidad informática, quien registrará el suceso en los medios dispuestos para tales efectos, de lo contrario cualquier situación anómala quedará bajo su responsabilidad.

d) Con relación a las claves de acceso a los sistemas, los usuarios deberán:

1. Mantener en forma confidencial las claves que se le asignen.
2. No registrar sus claves en papel.
3. No almacenar clave en un computador de manera desprotegida.
4. Compartir las claves con otros usuarios.
5. Cambiar las contraseñas a intervalos regulares. Las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que las claves normales; o en situaciones inmediata cuando haya indicios de un posible conocimiento o compromiso de la clave de acceso.

6. Elegir claves que tengan una longitud mínima de ocho caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos, y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos y no sean palabras de diccionario o nombres comunes.

e) Mantener respaldada su información local.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

ESTACIONES DE TRABAJO Y PANTALLAS LIMPIAS.

Adoptar una política de estaciones de trabajos ordenados y limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias y estructuradas a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera
del mismo.

Se entiende por pantallas limpias y estructuradas, en mantener todos los componentes lógicos del equipo ordenado y estructurarlos por tipo de archivos y carpetas para facilitar la búsqueda, respaldo y mantenimiento de este, evitando contar con duplicidad de archivos.

La misma política se debe aplicar al uso de gestores de mensajería y/o correos electrónicos.

RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN.

Todo funcionario que, en desarrollo de sus funciones, necesite acceder a un sistema informático municipal, lo accederá según las políticas de control de acceso definidas, en general y/o en particular de cada sistema.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El propietario de la información involucrada será responsable de la adjudicación de accesos a las funciones.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.

c) Controlar los derechos de acceso de los usuarios, por ejemplo, acceso modo consulta, acceso total o como administrador.

d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible contengan solo la información que resulte pertinente para el uso de la salida, y que, para el desarrollo de esta, se almacene en la respectiva base de datos el usuario, fecha y hora de la generación.

ALMACENAMIENTO DE LA INFORMACIÓN.

El respaldo de información o Backup es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, o perdidas de información ya sea por equivocación e

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

involuntariamente, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

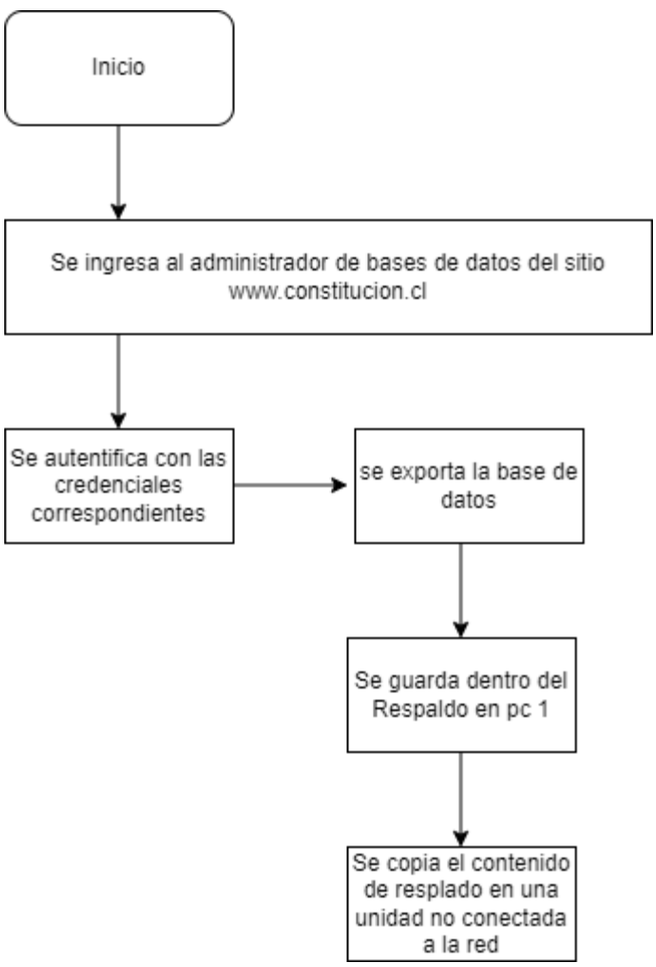
En relación con el manejo de respaldo de la información se deberá:

a) Realizar respaldos periódicos, ya sea semanal y/o mensual de los respectivos servidores municipales, el respaldo se almacenará en 2 ubicaciones distintas, una desconectada de la red, y contendrá la data del sitio web corporativo y la base sql del mismo.

b) Se dejará constancia de los respaldos efectuados a través de una bitácora de respaldo en la cual firmará el Encargado de la seguridad de la Información.

c) Además, periódicamente y a medida que se hagan las mantenciones al equipamiento municipal, se efectuará los respectivos respaldos de cada máquina de los usuarios.

d) De ser necesario el uso de recursos compartidos en alguna unidad, se deberá solicitar por escrito a la unidad de Informática, quien asignará y mantendrá el recurso y las credenciales de acceso.



6.- NORMAS DE USO DE INTERNET:

6.1 OBJETIVO

Internet es la unión de todas las redes y computadoras distribuidas en todo el mundo, así que podemos definir como una red global en la que interactúan usuarios

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

interesados en intercambiar información con otros, el buen uso del servicio y consumo consciente de los recursos, además del respeto a los lineamientos de seguridad que permitirá mantener una red operativa, estable y funcional.

6.2 POLÍTICAS

Las configuraciones de los computadores para acceder al servicio de Internet son responsabilidad exclusiva del Departamento de Informática.

El Departamento de Informática debe filtrar todo contenido que vaya en contra del interés municipal. Se podrá negar el acceso a cualquier equipo que viole las políticas o interfiera con la navegación de los demás usuarios.

El uso de Internet es personal e intransferible no permitiendo que segundas personas hagan uso de este.

Cada usuario es el responsable de acciones efectuadas a través de este servicio.

El incumplimiento por parte del usuario del buen uso del servicio puede ocasionar la suspensión del acceso.

La información consultada en cualquier horario de trabajo a través de Internet debe apoyar directamente las funciones relacionadas con el campo de responsabilidad laboral del usuario y/o servir como herramienta para desempeñar sus funciones.

6.3 NORMAS DE BUEN USO Y COMPORTAMIENTO

Quien acceda a otra red nacional o internacional mediante la red de la institución debe acatar las reglas que rijan.

El usuario no debe utilizar ninguna conexión privada a internet a través de las estaciones de trabajo conectadas simultáneamente a la red municipal.

Para evitar problemas de informática que afecten a la red municipal, se prohíbe la instalación de programas y la modificación de los programas, paquetes y configuraciones ya instaladas en los computadores.

El uso de pendrive y otros dispositivos de almacenamiento deben ser estrictamente chequeados antes de usarlos por el usuario.

Se prohíbe utilizar los servicios de red para juegos a través del servicio de internet o Intranet.

Se prohíbe acceder a todo material presente en internet que viole las leyes presentes o futuras y que su consumo, almacenaje y distribución sea constituyente de un delito, también se sancionará la producción de cualquier material que afecte a terceras personas y les cause menoscabo o perjuicio.

Todo contenido que se envíe vía Internet será de completa responsabilidad del usuario que los emite.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

Está prohibido el uso de programas “Point to point" (P2P) para bajar archivos de música o video desde internet, los cuales provocan un sobre consumo del ancho de banda, mermando la capacidad de navegación y acceso de los demás usuarios del municipio que requieren acceso a internet para sus labores dentro del municipio.

Se prohíbe realizar a través de Internet cualquier actividad ilegal o maliciosa que cause molestias o daño a segundas o terceras personas dentro o fuera de la red Municipal.

7.- NORMAS DE USO DEL CORREO ELECTRÓNICO:

El servicio de correo electrónico es una plataforma de comunicación brindada por el Municipio la que permite a los usuarios enviar y recibir mensajes a todo el mundo electrónicamente. Este servicio se utiliza para mejorar la comunicación entre los funcionarios y entre entidades públicas y/o privadas.

7.1 OBJETIVO

El objetivo de esta política es dar un ordenamiento en el uso del servicio de correo electrónico, definiendo las actuaciones consideradas abusivas y prohibidas.

7.2 POLÍTICAS

Es responsabilidad del usuario mantener la confidencialidad de la clave de acceso.

La cuenta de correo electrónico es personal e intransferible no permitiéndose que segundas personas hagan uso de ella.

Cada usuario es el responsable de las acciones efectuadas en su cuenta.

Es responsabilidad del usuario limpiar su cuenta periódicamente para que exista espacio disponible.

Todo usuario es responsable por los archivos adjuntos que envía.

El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y posterior baja del sistema del servicio.

7.3 NORMAS DE GENERACIÓN DE CUENTAS

Se asignará solamente una cuenta por usuario con un espacio determinado.

Las cuentas de correo electrónico corporativas asignadas serán usadas en labores propias del Municipio y se compondrán de la siguiente manera primeraletradelnombre.apellido@constitucion.cl

Estas cuentas podrán ser eliminadas previa autorización por escrito del jefe directo del funcionario a quien esté asignada la cuenta.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

Las cuentas de correo de uso general por algún departamento serán traspasadas al usuario que la subrogue o al nuevo funcionario el cual debe informar por escrito al departamento de informática.

Las cuentas de correo no podrán ser usadas para fines personales, por ejemplo; recibir información de cuentas de cobranza, correos masivos de cualquier índole u otras informaciones que no correspondan al trabajo.

7.4 NORMAS Y SUGERENCIAS DE BUEN USO Y COMPORTAMIENTO

Las que siguen son algunas de las reglas del buen comportamiento para aplicar al correo electrónico:
Se prohíbe expresamente abrir cualquier documento adjunto (ej. Rar o Zip), independiente del correo que provenga, a todo funcionario municipal independiente de su calidad jurídica sin previamente revisarlo por la solución antivirus presente en el equipo municipal.

Cuando escriba un mensaje a alguien que no conoce, preséntese siempre, indicando como se llama y quien es, y por supuesto firme sus mensajes.

No utilice expresiones con uso de lenguaje abusivo, soez, vulgar, obsceno y/o cuestionable.

Escriba el mensaje con la mayor corrección posible, evita las faltas de ortografía, utilice las comas y los puntos adecuadamente, ya que de lo contrario se mezclan las ideas, el texto se hace difícil de entender y obliga a releerlo para interpretar su sentido.

No de "ordenes" cuando quiera que alguien le explique algo, o cuando pida alguna información, pídalo por favor.

Sea breve y claro, recuerda que los mensajes largos se hacen pesados y no se lean.

No sea redundante, las cosas se dicen una vez, y no hace falta repetirlas más en el mensaje.

Tenga cuidado con lo que dice, ya que es frecuente guardar todos los mensajes que se reciben, y el destinatario de su mensaje, puede renviar su mensaje a otras personas en cualquier momento.

Identificación clara del remitente y el destinatario. Debe escribir el nombre de la persona a la que va dirigido el mail.

No responder un mail con monosílabos diciendo solamente” OK’ o “Yo no-.
Explica en forma concisa de que se está hablando.

Si se quiere enviar un correo a varias personas, utilizar el campo "CC* o "CCO" para escribir las direcciones que desee se mantengan oculta.

El Email oficial no debe ser usado para intereses o ganancias personales.

No escribir a listas de correos o a servidores las cuales no estén relacionadas directamente con su trabajo.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

Algunas listas de correos o de servidores generan cantidades masivas de correos a los suscriptores. Esto satura el espacio disponible en el disco duro de la estación de trabajo y degrada el funcionamiento del sistema de Email entrantes.
Todos los individuos son responsables de administrar las fuentes de tecnología de la información y son responsables de sus acciones.

El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS (Correos masivos no autorizados) de información, ni de mandar anexos que pudieran contener información nociva para otro usuario como virus, juegos o pornografía.
Buenas Prácticas
El correo electrónico no es mensajería instantánea, por lo tanto, no envíe un correo electrónico para comunicar un hecho que requiere inmediatez en la comunicación.

- No pida confirmación de lectura de ningún tipo, el correo electrónico fue diseñado para informar si el correo NO LLEGA.
- Busque correos en la bandeja de SPAM, es posible que algún remitente este clasificado de tal forma y los correos lleguen a la casilla SPAM.
- No responder correos en cadena.
- No abrir correos con adjuntos si no han sido solicitados.
- No imprima correos electrónicos a menos que sea estrictamente necesario.
  El Municipio Designara Mediante Acto Formal al “Encargado de Seguridad de la Información”, a su vez se creará el “Comité de la Seguridad”, quienes velaran por la seguridad de la información.

DEFINICIONES

a) Información: Grupo de datos ya supervisados y ordenados, que sirven para la toma de decisiones simples o estratégicas dentro de la institución.

b) Usuarios: Persona (externa, funcionario público, personal contratado a cualquier título y bajo cualquier régimen legal por el Municipio, practicantes y cualquier colaborador) que utiliza algún recurso tecnológico institucional, tal como computador, notebook, Tablet, Smartphone, etc. o accede a los servicios de red corporativos.

c) Incidente de Seguridad de la Información: Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información.

d) Encargado de Seguridad de la Información: planifica, desarrolla, controla y gestiona políticas, procedimientos y acciones para mejorar la seguridad de la información de la Municipalidad, debidamente designado por la autoridad correspondiente.

e) Información o datos personales: Son aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables, como por ejemplo el RUT o la dirección.

f) Información o datos sensibles: Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial,

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.

las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

g) Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

h) Información confidencial: Propiedad de la información, la cual pretende garantizar el acceso sólo a las personas autorizadas.

i) Nombre de usuario o Login: Cadena de caracteres que se utiliza para identificar a un Usuario en la entrada a un sistema operativo, software, servicio tecnológico (Aplicación Web, Portales Web, Correo electrónico, Etc.) o redes privadas entre otros servicios.

j) Encargado o responsable del software: Es la persona, jefe o director de área que se relaciona directamente con la funcionalidad específica del módulo de software que utiliza. Por ejemplo, el módulo de contabilidad gubernamental, su responsable directo es el Jefe del Departamento de Contabilidad, el módulo de tesorería, su responsable es el Tesorero Municipal.

k) Programas P2P: Las aplicaciones P2P (peer to peer) son programas que permiten el intercambio de archivos entre internautas.

ANÓTESE, ARCHÍVESE Y COMUNÍQUESE

ILUSTRE MUNICIPALIDAD DE CONSTITUCIÓN - ALCALDE -

FABIÁN PÉREZ HERRERA
ALCALDE

Carlos Mauricio Arellano Sepúlveda
9697167-2
carellano@constitucion.cl

Firmado electrónicamente según Ley 19799
el 02-04-2024 a las 08:54:46 con Firma Electrónica Avanzada
Código de Validación: 171205888658 1
Validar en https://www5.esigner.cl/esignercryptofront/documento/verificar/

esign Confianza Digital

MUNICIPALIDAD DE CONSTITUCIÓN - SECRETARIO MUNICIPAL -

ALDA VELIZ SYFRIG
SECRETARIO MUNICIPAL

Distribución
1. Alcaldía
2. Administración
3. Administración y Finanzas
4. Secretaria Municipal.
5. Desarrollo Comunitario.
6. Unidad de Proyectos Sociales
7. Dirección de Obras
8. Asesoría Jurídica
9. Relaciones Públicas
10. Gabinete
11. Dirección de Rentas y Permisos.
12. Dirección de Cultura y Turismo
13. Dirección de Tránsito.
14. Dirección Aseo y Ornato
15. Juzgado Policía Local.
16. Secretaria de Planificación.
17. Departamento Turismo.
18. Comunicaciones.
19. Transparencia Municipal.

FPH/AVS/CAS/RCM/JMD/cvr.

Documentos con Validez Legal Ley Nº 19.799. Certificado por E-Sign S.A.