ILUSTRE MUNICIPALIDAD DE OSORNO
CHILE

OSORNO, 13.08.2015.

MAT: REGLAMENTO SOBRE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN, DE LA ILUSTRE MUNICIPALIDAD DE OSORNO.

REGLAMENTO Nº 225

VISTOS:

El Decreto N ° 83, de fecha 12.01.2005, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los Órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

Las facultades que me confieren la ley Orgánica Constitucional de Municipalidades Nº 18.695 del año 1988 y sus posteriores modificaciones.

Las facultades que me confieren las letras i) del artículo 63 de dicho texto legal.

CONSIDERANDO:

La necesidad de otorgar un adecuado respaldo jurídico administrativo a la estructura de la Municipalidad de Osorno y la asignación de funciones a las respectivas unidades y con el fin de procurar un efectivo y coordinado ejercicio tendiente a cumplir los objetivos que le fija la ley, con el propósito de optimizar la gestión y dotar de una mejor funcionalidad al servicio prestado por las distintas Direcciones, en especial, de las funciones relacionadas con políticas de seguridad de la información.

RESUELVO DICTAR EL SIGUIENTE REGLAMENTO:

Generalidades.

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, base de datos, equipos computacionales y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren del acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar e instruir a los mismos acerca de sus responsabilidades por el

mantenimiento de controles eficaces, en particular aquellos relacionados con el uso de contraseñas y seguridad en el uso de equipamiento.

La institución deberá proveer los recursos y medios necesarios para la aplicabilidad de la presente política.

Objetivo.

El propósito de esta política es delimitar el uso aceptable de toda la información municipal y del equipamiento computacional, así como las redes de datos de la Municipalidad de Osorno.

Estas reglas están orientadas a proteger a los funcionarios y a la institución.

El uso inapropiado de los servicios de red y equipos informáticos expone a la institución municipal a posibles ataques de virus, compromiso de los sistemas y servicios de red, e incluso a problemas legales.

Alcance.

La presente Política de Control de acceso de la información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de información, los sistemas informáticos y todo el equipamiento computacional que se utilice en el ambiente tecnológico del organismo.

Debe ser conocida y cumplida por todos los funcionarios municipales, tanto de planta, como a contrata y además del personal a honorarios que cumple funciones en los diferentes programas que cuente el municipio.

El control de los accesos contemplara, uso de sistemas informáticos, uso de equipamiento informático de todo tipo, uso de correos electrónicos institucionales.

Responsabilidad.

Cada usuario de la información, jefaturas de las diferentes direcciones y/o departamentos, equipo informático y de los servicios de red de la institución deberá velar por el correcto cumplimiento de las normas aquí descritas, cualquier omisión voluntaria o involuntaria será sometida a la normativa vigente del estatuto administrativo.

ARTICULO 1.- Políticas de control de acceso.

I. Gestión de usuarios y permisos.

Se limitará y controlara la asignación y uso de permisos, debido a que el uso inadecuado de los permisos del sistema resulta ser, frecuentemente, el factor que más contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuarios que requieran protección contra accesos no autorizados, deberán prever una asignación de permisos, controlada mediante un proceso de autorización formal. Para ello se deben tener en cuenta los siguientes pasos:

a) Contar con sistema informático de solicitudes en línea que permita gestionar y actualizar los requerimientos de actualización de usuarios y permisos. Dicho sistema será considerado como proceso formal de autorización.

b) Identificar los usuarios y permisos asociados a cada uno de los sistemas, por ejemplo sistema contabilidad, conciliación bancaria, 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) Asignar los permisos a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional, siempre y cuando cuente con la autorización de su jefe directo, o en su defecto por la autoridad competente según sea el caso.

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.

Los propietarios de información serán los encargados de aprobar la asignación de permisos a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática, quien será el Jefe del Departamento de Informática.

ARTICULO 2.- 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, llevará a cabo un proceso formal, a fin de revisar los derechos de acceso de los usuarios. 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 accesos desde el recibo a través del sistema de solicitudes de la intranet por parte del superior jerárquico o por el departamento de personal.

e) El encargado de seguridad, una vez avisado por el sistema de solicitud de acceso 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.

ARTÍCULO 3.- Equipos asignados a los usuarios.

Los usuarios deberán garantizar que los equipos asignados sean protegidos adecuadamente.

Los equipos instalados en áreas de usuario, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desocupados.

El Responsable de Seguridad Informatica deberá coordinar con el Departamento de Personal las tareas de concientización a todos los usuarios a través de sesiones de capacitación, acerca de los requerimientos y procedimientos de seguridad para la protección de equipos asignados, así como de sus funciones en relación a la implementación de dicha protección.

El área de informática procederá a configurar cada equipo computacional con las sesiones de cada usuario y además dejará generado una sesión propia de la unidad de informática para su futura 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 en el sistema de solicitudes de accesos, de lo contrario cualquier situación anormal 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 hayan 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.

ARTICULO 4.- 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 del mismo, evitando el exceso de contar con duplicidad de archivos.

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

ARTICULO 5.- Uso de programas utilitarios de Sistema.

La mayoría de los equipos computacionales tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deberán considerar los siguientes controles:

a) Utilizar procedimientos de autorización para uso de programas utilitarios.

b) Administrar todos los programas utilitarios del sistema y software de aplicaciones.

c) Evitar que personas internas o ajenas al organismo instalen programas utilitarios y haga uso, sin la debida autorización del responsable de seguridad o del departamento de informática.

d) Registrar todo los programas utilitarios que se utilicen en el servicio.

e) Definir y documentar los niveles de autorización para utilitarios de sistema.

f) Remover todo el software basado en utilitarios y software de sistema innecesarios.

ARTÍCULO 6.- Computación y comunicaciones móviles.

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información municipal.

En este sentido, se deberá tener en cuenta cualquier dispositivo móvil y/o removible, incluyendo: netbook, notebook, laptop o PDA, teléfonos celulares y sus tarjetas de memoria, dispositivos de almacenamiento removibles, tales como CDs, DVDs y cualquier dispositivo de almacenamiento de conexión USB, tarjeta de identificación, dispositivos criptográficos, cámaras digitales, y además deberán incluirse todos los dispositivos que pudieran contener información relevante y confidencial del servicio.

Se desarrollaran procedimientos adecuados para estos dispositivos, que abarcaran los siguientes conceptos:

a) Uso y protección física necesaria.

b) El acceso seguro a los dispositivos.

c) La utilización de los dispositivos en lugares públicos.

d) El acceso a los sistemas de información y servicios del organismo a través de dichos dispositivos.

e) En el caso que el dispositivo lo acepte, se mantendrá con contraseña mientras esté fuera de servicio.

f) Los mecanismos de resguardo de información contenida en los dispositivos.

g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de incidentes del tipo de pérdida, robo o hurto. En consecuencia deberá entrenarse especialmente al personal que lo utilice. Se desarrollaran normas y procedimientos sobre los cuidados especiales sobre la posesión de dispositivos móviles.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del municipio.

ARTICULO 7.- Cualquier funcionario municipal, autorizado por el jefe del departamento al cual pertenece y/o por el encargado de informática, que requiera tener acceso a la información de la institución desde redes externas, podrán acceder remotamente mediante un proceso de autentificación, mediante el uso de conexiones seguras y asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.

Dichos accesos se podrán realizar a modo de consulta o por razones de soporte como administrador de sistema.

ARTICULO 8.- Restricción del Acceso a la información.

Los usuarios de sistema de aplicación, incluyendo al personal de informática, tendrán acceso a la información y a las funciones de los sistemas de aplicación en conformidad con las Políticas de Control de Acceso definidas, sobre la base de los requerimientos de cada aplicación.

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 las adjudicación de accesos a la funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico más elevado, las mismas serán llevadas a cabo por personal del área de informática, conforme a una autorización formal emitida por el propietario de la información.

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.

ARTICULO 9.- 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 involuntaria, 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 al manejo de respaldo de la información se deberá:

a) Realizar respaldos periódicos, ya sea semanal y/o mensual de los respectivos servidores.

b) La información de los servidores se extraerá en unidades externas las cuales serán trasladadas a un sitio diferente de donde fue generada. Dicha ubicación corresponde a una caja fuerte instalada en el Departamento de Tesorería Municipal.

c) De dichos respaldo se dejará constancia a través de una bitácora de respaldo en la cual firmará el Encargado de la seguridad de la Información que efectúa y entrega el medio de respaldo y el funcionario del Departamento de Tesorería que recepciona y almacena el respaldo.

d) Además, periódicamente y a medida que se realizan los respectivos soportes al equipamiento municipal se deberá ir efectuando los respectivos respaldos de cada una de las máquinas de los usuarios.

e) Así mismo se exigirá que los servidores principales cumplan con todas las políticas de seguridad y almacenamiento existente como pueden ser backup progresivo, *copia* en servidores de respaldo, en disco espejos u equipos remotos, realizado preferentemente en horarios nocturnos para no afectar la performance del servicio.

ARTICULO 10.- El presente Reglamento regirá a partir de la fecha de su dictación.

De conformidad a lo dispuesto en los artículos 6º y 7º de la Ley Nº 20.285, sobre Acceso a la Información Pública, a contar de su entrada en vigencia, publíquese en forma destacada el presente Reglamento en el sitio electrónico o página web de esta Municipalidad, a disposición permanente de los usuarios.

ANOTESE, COMUNIQUESE, TRANSCRIBASE EL PRESENTE REGLAMENTO A TODAS LAS UNIDADES DE LA MUNICIPALIDAD, PUBLIQUESE EN NUESTRO SITIO ELECTRÓNICO, SIN PERJUICIO DE PERMANECER UN EJEMPLAR DEL MISMO A DISPOSICIÓN Y PARA CONOCIMIENTO PUBLICO EN SECRETARIA MUNICIPAL, CUMPLASE Y ARCHIVESE.

MUNICIPALIDAD SECRETARIA MUNICIPAL OSORNO

YAMIL UARAC ROJAS
SECRETARIO MUNICIPAL

ALCALDIA MUNICIPAL OSORNO

HARDY VASQUEZ GARCES
ALCALDE DE OSORNO (S)

HVG/YUR/JCP/JHP/RPC/ldp

Distribución:

- Alcaldia.-
- Dirección Administración Municipal.-
- Dirección Asesoría Jurídica.-
- Dirección Secretaria Municipal.-
- Dirección Administración y Finanzas.-
- Dirección Control.-
- Dirección Transito.-
- SECPLAN.-
- Dirección de Obras.-
- DIDECO
- DAEM
- Departamento Salud
- 1er. Juzgado de Policía Local
- 2er. Juzgado de Policía Local
- Archivo Departamento de Informatica.-

DIRECCION JURIDICA I. MUNICIPALIDAD DE OSORNO