República de Chile
Provincia Linares
Dirección de Adquisiciones
Depto. Informática

DECRETO EXENTO Nº 3591

PARRAL, 09 Agosto 2022

VISTOS:

1. La Ley Nº 18.695. Orgánica Constitucional de Municipalidades.
2. La Ley Nº 19.880. Establece bases de los procedimientos ante los órganos que rigen los actos de la Administración del Estado. Ley Nª 20.285 sobre Acceso a la información pública.
3. Decreto Supremo Nº 83/2005 aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
4. Decreto Supremo Nº 93/2006 Aprueba norma técnica para órganos de la adopción de medidas destinadas a minimizar los efectos perjudiciales mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
5. Decreto exento Nª1702 del 18 de Abril del 2022, que define la política de seguridad de la información de la Ilustre Municipalidad de Parral.
6. Decreto Nº 83 de MINSEGPRES del año 2004, que hace relación al control de accesos que mantiene el municipio a los sistemas de la información.

CONSIDERANDO:

1. **Que,** se debe crear una normativa para el uso, regulación y protección del acceso remoto a la red y servicios de red.

DECRETO

1. **APRUEBESE** la normativa para el uso, regulación y protección del acceso remoto

NORMATIVA PARA EL USO, REGULACIÓN Y PROTECCIÓN DEL ACCESO REMOTO

ARTICULO 1: El objetivo de este documento es garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información de la municipalidad, realizado por personal interno, en conjunto con definir las condiciones y directrices de regulación de la conectividad.

Este reglamento es de aplicación y de obligado cumplimiento para todo el personal de la Municipalidad que deba acceder a los sistemas descritos en este documento.

En el ámbito del presente procedimiento, se entiende por usuario a cualquier funcionario perteneciente o vinculado a la Municipalidad que utilice o posea acceso a los sistemas de información.

ARTÍCULO 2: La gestión de este procedimiento corresponde al departamento de informática, que tiene las competencias para interpretar las dudas que puedan surgir en la aplicación, proceder a la revisión en caso de ser necesario para actualizar el contenido, verificar el funcionamiento y efectividad.

Es responsabilidad de las direcciones de la municipalidad proveer y mantener las condiciones necesarias para el cumplimiento de esta política, así como establecer las reglas de uso del acceso remoto para los funcionarios que lo requieran.

Es responsabilidad de cada funcionario, departamento o dirección comunicarse con el departamento de informática para notificar bajas de los servicios, traslados, cambios de función o perfiles para aplicar las modificaciones correspondientes.

ARTÍCULO 3: Se deben realizar los esfuerzos necesarios para que la información de la Municipalidad no se vea comprometida. Para ello, es necesario el cumplimiento de los siguientes puntos:

1. Definir que los servicios, redes y sistemas de información que pueden ser accedidos remotamente por el funcionario que realiza el acceso remoto se limitan a la realización de sus funciones laborales y queda determinado por el Director/a o Jefatura a cargo.
2. Mantener un registro de los funcionarios que se encuentran trabajando con conexiones remotas y establecer los sistemas, servicios y redes a los cuales tiene acceso.
3. Mantener un listado de los equipos a los cuales se puede acceder remotamente.
4. Los equipos utilizados para el acceso remoto deben contar con protección ante software maliciosos.

ARTÍCULO 4: Se considera acceso local al realizado desde puestos de trabajo dentro de las propias instalaciones municipales a través de la red (cableada o inalámbrica). Se deben aplicar las siguientes medidas:

1. La configuración de los sistemas de información debe prevenir la revelación de información acerca de los servidores o servicios cuando aun no se han accedido a los mismos
2. La información revelada a quien intenta acceder a los servicios debe ser la mínima imprescindible
3. Se configurarán debidamente los mensajes de error de las aplicaciones para limitar la información que se ofrece al usuario.
4. Siempre que sea posible, el numero de intentos de acceso permitidos a los sistemas de información será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.

ARTÍCULO 5: Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros. El acceso desde fuera de las instalaciones de la Municipalidad conlleva el riesgo de trabajar en entornos de acceso desprotegidos, esto es, sin las barreras de seguridad físicas y lógicas implementadas en la red local de la Municipalidad. Fuera de este perímetro de seguridad aumentan las vulnerabilidades y la probabilidad de materialización de las amenazas, por lo que se hace necesario adoptar

medidas de seguridad adicionales que se aseguren la confidencialidad, autenticidad e integridad de la información. Adicionalmente a las medidas de seguridad aplicables en el acceso local se deben aplicar las siguientes medidas.

Con uso de sistema de conexión remota:

1. La conexión remota debe ser de uso personal y no compartido
2. Cerrar siempre la sesión al finalizar el trabajo
3. Bloquear siempre la sesión ante cualquier ausencia temporal, aunque sea un espacio de corto tiempo.

Cuando la conexión desde el exterior se realiza con equipos portátiles municipales, el usuario tendrá en cuenta:

1. Que dichos equipos son para uso exclusivo del trabajador y solo serán utilizados para fines profesionales.
2. No deben prestarse los equipos a terceros salvo autorización expresa por el/la directivo/a a cargo.

Si la conexión se realiza desde equipos de trabajo personales no corporativos, los usuarios deben considerar:

1. Que los equipos estén configurados con los requisitos de software necesarios que permiten trabajar en los mismos entornos y versiones que requieren los sistemas de información de la municipalidad.
2. En cualquier caso, los equipos desde los que se realiza la conexión remota deben disponer de las siguientes medidas de seguridad, estén o no bajo la responsabilidad del departamento de informática.
    a. Antivirus instalado y actualizado
    b. Cortafuegos activado
    c. Versión del sistema operativo actualizada
    d. Copia de seguridad periódicas de la información contenida en los equipos.

Cuando el acceso remoto a los servicios de información se realice vía web, se aplicaran las siguientes medidas de seguridad:

1. Los navegadores utilizados deben estar adecuados a las versiones oficiales o que permiten el uso de sistemas de información de la municipalidad, así como tener los parches de seguridad correspondientes, instalados y configurados.
2. Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada. O desactivar las características de recordar contraseñas en el navegador
3. Activar la opción de borrado automático al cierre del navegador de la información sensible registrada por el mismo (historial de navegación, descargas, formularios, cache, cookies, sesiones autenticadas, etc).

4. No instalar extensiones para el navegador que puedan alterar el normal funcionamiento de las aplicaciones

ANOTESE, REFRENDESE, COMUNIQUESE Y CUMPLASE

ALEJANDRA ROMAN CLAVIJO
SECRETARIA MUNICIPAL

PAULA RETAMAL URRUTIA
ALCALDESA DE PARRAL

JAH
DISTRIBUCION:
1.- Oficina de Partes
2.- Dirección de Control
3.- Departamento de Informática
4.- *COPIA DIGITAL (todos@parral.cl)*

ENCARGADO TECN. INFOR.	DIRECTORA ADQUISICIONES	DIRECTOR DE CONTROL
JULIO ABURTO HERNANDEZ	ERICA GAJARDO PEREZ	ENRIQUE GOMEZ HOFFER