República de Chile
Provincia de Linares
Dirección de Adquisiciones
Departamento de Informática

DECRETO EXENTO N°: 988 /

PARRAL, 08 MAR. 2022

VISTOS:

1.- Las Facultades que me confiere la Ley N° 18.695/88, Ley Orgánica Constitucional de Municipalidades y sus posteriores modificaciones.
2.- La Sentencia definitiva de fecha 10 de junio del 2021 dictada por el Tribunal Electoral Regional del Maule.
3.- Acta de Proclamación de fecha 16 de junio del 2021 del Tribunal Electoral Regional del Maule.
4.- Juramento prestado en Sesión de instalación del Honorable Concejo Comunal de Parral celebrada el 28 de junio del 2021.
5.- Declaración de Asunción de funciones efectuada por el Decreto Afecto N° 1.282 del 29 de junio del 2021."
6.- El reglamento interno sobre el uso de Tecnologías de la Información de la Ilustre Municipalidad de Parral año 2011.
7.- El Decreto Exento N° 4569 de fecha 30 de Septiembre de 2011, que aprueba el Reglamento Interno sobre el Uso de Tecnologías de la Información de la Ilustre Municipalidad de Parral año 2021.-

CONSIDERANDO:

1.- **Que**, se debe crear el procedimiento de control de acceso a aplicaciones del Departamento de Informática, debido a la necesidad de mantener actualizados los sistemas de gestión, acción y directrices de la información.

DECRETO:

1.- **APRUEBESE**, Procedimiento de control de acceso a aplicaciones del Departamento de Informática.

PROCEDIMIENTO CONTROL DE ACCESO A APLICACIONES

El procedimiento de control de acceso a aplicaciones Municipales tiene como propósito describir los mecanismos de control y de eventos, definiéndose como principalmente como los procesos de identificación de personas autorizadas para tener acceso a aplicaciones, software, servidores, correo electrónico, entre otros.

El objetivo es definir los procedimientos de acceso para mantener un control sobre los equipos de comunicación, herramientas, softwares y aplicaciones de uso Municipal.

DEFINICIONES

1. **Plataforma Tecnológica:** Incluye el conjunto de recursos que en materia de tecnologías de información y comunicaciones TIC (programas, soportes, archivos, datos, información, redes internas y públicas, equipos para el almacenamiento, la seguridad, control, tratamiento, generación, comunicación y transmisión de datos en todos sus formatos) que utilice la Municipalidad.
2. **Recursos Informáticos:** Incluyen todo equipo informático (servidores, pc´s, laptops, pocket, palm, unidades de control, equipos de seguridad, impresoras, periféricos entre otros), infraestructura de comunicaciones (modem, router, switch, hubs, acces point, torres de comunicación, antenas, tendidos de fibra óptica y cableado de datos interiores o por vías públicas), software (oficina, desarrollo, control, grafico, diseño web, administración de dominio, administración de base de datos, seguridad, antivirus), aplicaciones y sistemas desarrollados para uso de la Municipalidad de Victoria (servicios intranet, correo electrónico, sitio web, base de datos), documentos electrónicos

generados(Word, excel, power point, pdf, entre otros) e información contenida en los sistemas de información.

3. **Usuario:** Toda persona vinculada a la Municipalidad que hace uso de sus recursos informáticos.

4. **Material no autorizado:** Transmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales.

5. **Sistemas de información:** Incluye cualquier sistema o aplicación de software que sea administrado por el Departamento de Informática de la Municipalidad y de los cuales es responsable, aplicaciones, servidor, sistemas operativos y aplicaciones de internet.

6. **Programa Utilitario:** Los programas o softwares utilitarios están diseñados para una función determinada, por ejemplo, un editor, un depurador o un programa para recuperar datos perdidos.

RESPONSABILIDAD

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

ARTICULO 1.- Políticas de control de acceso.

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) El director/a o Jefatura debe solicitar mediante correo electrónico al encargado del departamento de informática los accesos necesarios dentro de los equipos de trabajo permitiendo gestionar y actualizar los requerimientos 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 bancaría, sistema de gestión documental, sistema administración de base de datos y aplicaciones, etc. Además, definir las categorías de personal a las cuales deben asignarse los permisos.

c) 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.

d) Dependiendo de la aplicación, software o proceso se establece un periodo de vigencia 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

e) Para revocar, eliminar o suprimir los permisos a un usuario, el director/a o jefatura tiene el deber de informar al Departamento de Informática mediante un correo electrónico elevando la solicitud de la acción a ejecutar.

f) El acceso a los sistemas de uso Municipal contemplan un usuario que los identifica más una contraseña propia de cada funcionario.

Las aplicaciones a las cuales se establece control de acceso se mencionan:

1. CAS-CHILE
2. SINGIFLOW
3. CORREO ELECTRONICO
4. PLATAFORMA WEB
5. SERVIDORES MUNICIPALES
6. SESIONES ACCESO A COMPUTADORES ESCRITORIO O PORTATIL
7. PORTAL DE SERVICIOS MUNICIPALES

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 Departamento de Informática 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) Establecer y 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 por parte del superior jerárquico o por el departamento de personal.
e) El encargado de seguridad, una vez notificado en la solicitud sobre un cambio de algún funcionario 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 Informática 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 al Departamento de informática, 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. No 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 existan 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.- Los mecanismos de control de acceso de servidores queda definido mediante los siguientes puntos:

- Identificación de personas y autorizaciones al acceder a la Sala de Servidores
- Sistema biométrico para el acceso físico a la Sala de Servidores
- Alarma de puerta abierta Sala de Servidores
- Circuito cerrado de televisión dentro de la Sala de Servidores. Se entiende por Sala de Servidores oficina cerrada ubicado en el Departamento de informática que alberga todos los Servidores de la municipalidad.

Se establece una lista de funcionarios del departamento de informática autorizados a acceder a la Sala de Servidores. Estas personas tienen las llaves de acceso al centro de servidores, quedando bajo su responsabilidad el acceso y control de los servidores Municipales.

Adicionalmente se implementa una bitácora de acceso a la Sala, registrando el nombre de la persona que solicitó el acceso, el motivo, fecha, hora de su ingreso, hora de salida y firma en la Bitácora de Accesos de la sala de servidores por parte de la secretaria de la unidad o personal de informática que esté presente.

Adicionalmente en la bitácora se deberá dejar registrados con fecha y hora cualquier evento anormal que ocurra en la sala de servidores como, por ejemplo: corte de luz, baja de voltajes, baja de automáticos, falla en aire acondicionado, goteras, ruidos, humos, cambio de equipos, ups, manipulación dudosa de equipos por personal interno y externo, o cualquier otra situación. La bitácora deberá ser revisada y visada al menos una vez al mes por el encargado de la unidad o el funcionario que se asigne para dicha labor.

ARTICULO 5.- Uso de programas utilitarios del sistema.
La mayoría de los equipos computacionales tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles del sistema y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deberá 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 todos los programas utilitarios que se utilicen en el servicio.
e) Definir y documentar los niveles de autorización para utilitarios del sistema.
f) Remover todo software basado en utilitarios y software de sistemas innecesarios.

ARTICULO 6.- Computación y comunicaciones móviles
Cuando se utilizan dispositivos informáticos móviles que se debe tener especial cuidado en garantizar que no se comprometa la información Municipal.

En ese sentido, se deberá tener en cuenta cualquier dispositivo móvil y/o removible, incluyendo notebook, netbook, laptop o tablet, teléfonos celulares y sus tarjetas de memoria, dispositivos 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 desarrollarán procedimientos adecuados para estos dispositivos, que abarcarán los siguientes conceptos:

a) Uso y protección física innecesaria.
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 caso que el dispositivo lo acepte, se mantendrá con contraseña mientras este fuera de servicio.
f) Los mecanismos de resguardo de información contenida en los dispositivos.
g) La protección contra softwares maliciosos.

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 desarrollarán normas y procedimientos sobre los cuidados especialmente 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.

ARTICULO 7.- Restricción del acceso a la información
Los usuarios del 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 las bases de requerimientos de cada aplicación.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitaciones 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. 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 el personal del Departamento de Informática, conforme a una autorización formal emitida por el propietario de la información.
b) Restringir el conocimiento de información de los usuarios acerca de las funciones de los sistemas de aplicaciones a las cuales no tienen autorización de acceso.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, acceso modo consulta, acceso total o como administrador.
d) Garantizar las salidas de los sistemas de aplicación que administran información sensible, contenga solo información que resulte pertinente para uso de salida, y que el desarrollo de esta, se almacene en la respectiva base de datos del usuario.

ANOTESE, REFRENDESE, COMUNIQUESE Y CUMPLASE.

SECRETARIA MUNICIPAL ★ ILUSTRE MUNICIPALIDAD DE PARRAL ★

ALEJANDRA ROMAN CLAVIJO
SECRETARIA MUNICIPAL

I. MUNICIPALIDAD DE PARRAL ★ ALCALDESA ★

PAULA RETAMAL URRUTIA
ALCALDESA DE PARRAL

MHT/ARC/EGP/JAH
DISTRIBUCIÓN
1.- Oficina de Partes
2.- Dirección Control
3.- Departamento de Informática
4.- COPIA DIGITAL (todos@parral.cl)