MUNICIPALIDAD DE PUCON
ADMINISTRACION MUNICIPAL

DECRETO EXENTO Nº 1716 .-

Pucón, 30 de junio de 2022.-

VISTOS:

1. El Decreto Exento N°3222 de fecha 30 de diciembre de 2016, mediante el cual se Aprobó el **Reglamento Interno Uso y Seguridad de la Plataforma Tecnológica** de la Municipalidad de Pucón.
2. El Decreto Exento N°3446 de fecha 12 de diciembre de 2018, mediante el cual se Aprobó las modificaciones del **Reglamento Interno Uso y Seguridad de la Plataforma Tecnológica** de la Municipalidad de Pucón.
3. El Informe N° 196/2022 de fecha 28 de abril de 2022, de la Contraloría Regional de la Araucanía, que contiene observaciones en cuanto a actualización de procedimiento de respaldo, procedimiento de eliminación de la información en dispositivos electrónicos, procedimiento de acceso remoto.
4. El Reglamento Interno Uso y Seguridad de la Plataforma Tecnológica, de la Unidad de Informática, y sus modificaciones.
5. Instructivos de procedimiento de eliminación de la información en dispositivos electrónicos, y procedimiento de acceso remoto.
6. Las atribuciones que me confiere la Ley Nº18.695 "Orgánica Constitucional de Municipalidades", y sus posteriores modificaciones, contenidas en la Ley N° 20.742 de fecha 01 de abril de 2014.

CONSIDERANDO:

1. La necesidad de actualizar y mejorar el actual Reglamento Interno Uso y Seguridad de la Plataforma Tecnológica de la Municipalidad de Pucón, en cuanto a procedimiento de respaldo (página 25).
2. La necesidad de contar con la formalización del procedimiento de eliminación de la información en dispositivos electrónicos, y del procedimiento de acceso remoto.

DECRETO:

1. **APRUEBENSE**, las modificaciones propuestas por el Visto N°3 al Reglamento Interno Uso y Seguridad de la Plataforma Tecnológica, quedando como se adjunta.
2. **APRUÉBESE**, el instructivo "Instructivo para procedimiento de eliminación de la información en dispositivos electrónicos", e "Instructivo para procedimiento acceso remoto", como se adjuntan.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

MUNICIPALIDAD SECRETARIA MUNICIPAL PUCON

GLADIELA MATUS PANGUILEF
SECRETARIA MUNICIPAL

MUNICIPALIDAD DE PUCON ALCALDIA

CARLOS BARRA MATAMALA
ALCALDE

MUNICIPALIDAD ADMINISTRACION PUCON

VºBº ADMINISTRADOR MUNICIPAL

CBM/GMP/COS/ylm.-
DISTRIBUCION:
- Administración
- Informática
- Of. Partes.

REGLAMENTO INTERNO DE USO Y SEGURIDAD DE LA PLATAFORMA TECNOLOGICA MUNICIPALIDAD DE PUCÓN

I N D I C E

REGLAMENTO INTERNO DE USO Y SEGURIDAD DE LA PLATAFORMA TECNOLOGICA MUNICIPALIDAD DE PUCON

DISPOSICIONES GENERALES

Las disposiciones generales del presente reglamento se sustentan en la Ley 19.223, relativa a Delitos Informáticos y Reglamento de Conectividad y usos de Intranet del Ministerio del Interior.

La aprobación del presente reglamento mediante Resolución exenta y su debida notificación a todo el personal de la Municipalidad de Pucón, hará que se presuma conocido por todos, no pudiendo alegarse desconocimiento del mismo.

Los casos no previstos en el presente reglamento serán analizados por la Unidad de Informática y el Administrador Municipal para decidir las acciones a seguir.

1. **PROPOSITO**

   Definir políticas sobre el uso apropiado de la Plataforma Tecnológica disponible en la Municipalidad de Pucón.

2. **ALCANCES**

   Este reglamento se aplicará a toda persona que utilice directa o indirectamente la Plataforma Tecnológica de la Municipalidad de Pucón, tanto al personal de Planta, Contrata y Honorarios del Municipio, como a los usuarios de las zonas Wi-Fi públicas.

   También se aplica a todos los equipos y sistemas informáticos que la Municipalidad de Pucón haya dispuesto para la ejecución de labores funcionarias, de apoyo administrativo y de gestión (servidores, equipos PC, Notebooks, Netbook, Tablets, celulares smartphones, scanner, equipos de comunicaciones, equipos de control, equipos de seguridad, bases de datos, aplicaciones que apoyen los procesos profesionales, técnicos o administrativos, software licenciado, impresoras, periféricos e información electrónica) que se encuentren bajo responsabilidad operacional de la Institución.

   Se extiende su aplicación a la administración, mantención y control de las zonas geográficas de la ciudad de Pucón sobre las cuales se entrega un servicio limitado de conectividad Wi-Fi hacia internet en forma gratuita al público, y el equipamiento dispuesto para esa función.

3. TERMINOS/DEFINICIONES

Para los propósitos de esta política se aplicarán las siguientes definiciones:

Plataforma Tecnológica de la Municipalidad de Pucón, incluye el conjunto de recursos informáticos que en materia de Tecnologías de Información y Comunicaciones TIC (programas, soportes, archivos, datos, información, redes internas y públicas, equipos informáticos y de comunicación para el almacenamiento, la seguridad, el control, el tratamiento, la generación, comunicación y transmisión de datos en todos sus formatos) utilice la Municipalidad de Pucón.

Recursos informáticos: incluyen todo equipo informático (servidores, equipos PC, Notebooks, Netbook, Tablets, celulares smartphones, unidades de control, equipos de seguridad, impresoras, pendrives y periféricos), infraestructura de comunicaciones (módems, router, switch, hubs, access point, torres de comunicación, antenas, tendidos de fibra óptica y cableado de datos interiores o por vía pública), software (oficina, desarrollo, control, gráfico, diseño web, administración de dominio, administración de base de datos, seguridad, antivirus), aplicaciones y sistemas desarrollados para uso de la Municipalidad de Pucón (servicios Intranet, correo electrónico, sitio web, bases de datos, sistemas computacionales administrativos, control y de gestión), documentos electrónicos generados (word, excel, powerpoint, access, pdf, etc.) e información contenida en los sistemas de información. Es decir, todo el hardware y software propiedad de la Municipalidad de Pucón.

Usuario: Es toda persona que hace uso de cualquier recurso informático incluido en la Plataforma Tecnológica Municipal.

Usuario Interno: Es todo personal vinculado con la Municipalidad de Pucón que hace uso de un recurso interno de la Plataforma Tecnológica.

Usuario Externo: Es toda persona que hacen uso de las zonas Wi-Fi públicas. Son usuarios con responsabilidad limitada y acceso sólo a internet.

Custodio o Depositario: Todo único usuario interno autorizado para hacer uso de un recurso de la Plataforma se convierte automáticamente en custodio sin necesidad de documento de por medio. También lo es todo personal al cual se le ha asignado un recurso informático o de comunicaciones por escrito, y que no necesariamente hace uso directo del mismo.

Material no autorizado: incluye la 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.

Red de Datos: es el conjunto de recursos informáticos que permite la comunicación de datos e información a través de la Municipalidad de Pucón incluyendo el Internet.

Red: incluye cualquier sistema de enlaces por cables, fibra o inalámbricos, junto a equipos como routers, switches, transeivers, módems, sistemas de datos, voz, dispositivos de almacenamiento, unidades de control y equipos de seguridad.

Sistemas de información: incluye cualquier sistema o aplicación de software que sea administrado por la Unidad de Informática de la Municipalidad de Pucón y de los cuales es responsable, aplicaciones de servidor, sistemas operativos y aplicaciones de Internet.

Zonas Wi-Fi públicas: zona geográfica destinada a dar conectividad controlada y limitada a Internet al público en forma gratuita.

Red de Voz: es el conjunto de elementos destinados a la comunicación por voz dispuestos en todas las dependencias municipales, incluye Teléfonos, Centrales Telefónicas, Cintillos, mesas de control de llamados, grabadoras, unidades de registro, altavoces, Switches, conversores y enlaces por cable e inalámbricos dispuestos para este fin.

Tecnologías de Información y Comunicaciones TIC, grupo de elementos y técnicas utilizadas en el tratamiento y transmisión de datos e información.

Comité Web: Conjunto de funcionarios responsables de los contenidos del sitio Web Municipal. Presidido por el Administrador municipal, y encargado operativo el Jefe de Comunicaciones.

Sitio Web Municipal: Sitio web oficial de la Municipalidad de Pucón, al cual se accede a través de las direcciones www.municipalidadpucon.cl .

Software : es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora. Se considera que el software es el equipamiento lógico e intangible de un ordenador. En otras palabras, el concepto de software abarca a todas las aplicaciones informáticas, como los procesadores de textos, las planillas de cálculo y los editores de imágenes, administración de bases de datos, etc.

Hardware : en el caso de la informática y de la computación, el hardware permite definir las partes físicas tangibles de un computador o de un sistema informático, es decir, no sólo define un equipo en su totalidad, sino que también a los componentes físicos internos (disco duro, placa madre, microprocesador, circuitos, cables, etc.), y también a los periféricos (escáners, impresoras, pendrives, etc.).

Jefes de Sistemas: serán los responsables finales de la administración de un sistema computacional, y serán nombrados mediante Decreto Alcaldicio.

4. GENERALIDADES

Para cautelar la seguridad y estabilidad de la Plataforma Tecnológica y evitar daños ocasionados por virus informáticos, hackers e intervenciones no autorizadas, así como detectar abusos internos se ha hecho necesario definir políticas de seguridad para permitir a la Municipalidad de Pucón proteger, controlar y administrar esta Plataforma de manera segura, rápida y confiable.

La Municipalidad de Pucón asigna al personal los equipos y sistemas de información y comunicaciones necesarios para la ejecución de las actividades laborales, en la medida de la disponibilidad de los mismos y con la aprobación de la autoridad respectiva, convirtiéndose estas personas en usuarios internos, responsables y custodios de estos recursos.

El acceso a los equipos y sistemas de información, comunicación y control de la Municipalidad de Pucón es un privilegio y tiene por objetivo brindar facilidades para cumplir con los fines laborales, de cada área o unidad en los que se asignaron.

Cada usuario interno tiene el deber de: respetar y custodiar la integridad de los equipos informáticos y de comunicación asignados, realizar los cuidados mínimos necesarios de higiene y protección sobre ellos, cumplir las licencias y acuerdos relacionado con los software adquiridos e instalados y las aplicaciones internas desarrolladas, así como actuar según políticas implementadas en este documento .

Las violaciones a las políticas y disposiciones establecidas en este reglamento con respecto al uso total o parcial de la Plataforma Tecnológica, puede originar en la restricción o prohibición del acceso a ésta, u otras acciones disciplinarias o legales por parte de la Municipalidad de Pucón.

La Municipalidad de Pucón no asume responsabilidad alguna por el mal uso de los recursos de la Plataforma Tecnológica asignados a los usuarios internos, sin embargo como propietaria de ellos, puede disponer de la información generada en estos recursos para apoyar las acciones disciplinarias y legales que crea convenientes en caso que se vea afectada por acciones de desprestigio o falta a la seguridad informática por parte de estos usuarios.

5. POLITICAS Y NORMAS

5.1. SOBRE EL USO DE LOS RECURSOS DE LA PLATAFORMA TECNOLÓGICA

El uso de los recursos de la Plataforma Tecnológica es para asuntos relacionados con las labores profesionales, técnicas o administrativas derivadas de las tareas en la Municipalidad de Pucón que le han sido designadas, siendo el uso personal limitado.

El empleo de los recursos sin indicación expresa por documento al Encargado de la Plataforma Tecnológica de la Municipalidad de Pucón, se encuentra por defecto terminantemente prohibido. Los usuarios internos se limitarán a trabajar con los recursos TIC asignados y en caso de requerir más recursos deberán solicitarlos a la Unidad de Informática a través de su jefatura.

El uso personal de los recursos informáticos, software, servicios y periféricos, excepto las aplicaciones de acceso a información laboral, es permitido al usuario para actividades académicas, siempre y cuando esté autorizada debidamente, acate las políticas implementadas en este documento, no interfiera con las actividades operativas normales de la Municipalidad de Pucón, no afecten a los demás usuarios y no influyan negativamente en el desempeño de tareas y responsabilidades asignadas al cargo, en caso contrario debe ser negado.

No está permitido imprimir trabajos personales empleando los recursos institucionales (papel, tóner, tinta, cinta). Ningún usuario está autorizado a usar los recursos informáticos para acceso, descarga, transmisión, distribución o almacenamiento de material: obsceno, ilegal, nocivo o que contenga derecho de autor, para fines ilegales.

No está permitido a los usuarios internos el uso de los recursos informáticos para generar ganancias económicas personales o desarrollar actividades o labores de terceros, así como utilizar los Sistemas de información y Software con fines comerciales, ni con cualquier otro fin diferente a los que específicamente define las normativas de la Asociación de Distribuidores de Software (ADS).

No está permitido usar los equipos informáticos incluidas las impresoras de la Municipalidad de Pucón para fines que no sean propias de la labor del usuario interno.

No está permitido el uso de los equipos informáticos, servicios y red de datos para propagar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva, esto será reportado a Encargado de la Plataforma Tecnológica de la Municipalidad de Pucón para que inicie las acciones pertinentes.

El uso de equipos personales conectados a las Redes de Datos Municipales (con excepción de las zonas Wi-Fi públicas) serán autorizados por escrito por el Administrador Municipal y serán configurados y supervisados por el personal de la Unidad de Informática, para evitar vulneraciones a la seguridad interior.

5.2. SOBRE LA INTEGRIDAD DE LOS RECURSOS DE LA PLATAFORMA TECNOLÓGICA

Se considera que el usuario interno está incurriendo en falta grave por negligencia cuando destruye o daña los recursos informáticos de la Plataforma Tecnológica que se le hayan asignado para realizar su labor o actividad o cuando manipula cualquier otro recurso informático de la Municipalidad de Pucón que no es de su uso normal.

Está prohibido manipular comidas y/o líquidos cerca de los recursos informáticos que puedan originar directa o indirectamente su mal funcionamiento siendo el usuario responsable por el deterioro del mismo, en estos casos se informará vía documento al Jefe de la Unidad de Informática para que éste determine las acciones a seguir o el reemplazo del equipo.

No está permitida la manipulación maliciosa de los recursos informáticos que puedan originar daños en los servidores, equipos PC, periféricos, equipos de comunicaciones, la estructura de red, las aplicaciones desarrolladas, la base de datos, el servicio de Internet, el servicio de Intranet, el correo electrónico y los servicios y/o recursos informáticos y de comunicaciones asociados.

Está prohibido dañar el equipamiento disponible en los distintos Departamentos y Unidades de la Municipalidad de Pucón (ya sea rayarlos, pegar etiquetas o stickers, y extraer partes o piezas de los mismos, o usarlos en forma brusca o inadecuada).

Está prohibido el uso y manipulación de equipos por personal externo a la institución que no cuenten con la autorización del Jefe de la Unidad de Informática.

Está prohibido divulgar sus contraseñas asignadas como usuario interno (inicio sesión, sistemas computacionales, email, intranet, etc.), ya que son personales e intransferibles.

Está prohibido usar el nombre de una cuenta y/o clave perteneciente a otro usuario interno, así como entregar claves que no estén bajo su responsabilidad directa.

Está prohibido destruir y/o violar los datos de otros usuarios sin las respectivas autorizaciones.

Está prohibido eliminar toda la información que haya creado o recibido durante su periodo laboral, al generarse el término de la relación laboral con la institución. Toda la información contenida en el recurso informático que se le había asignado para su labor, es propiedad de la Municipalidad de Pucón.

Está prohibido intentar interferir otras computadoras o cuenta utilizando “caballos de Troya”, virus o cualquier otro método de hacking.

5.3. SOBRE EL ACCESO A LA RED DE DATOS

La cuenta y la contraseña de acceso a la de la Red de Datos, a las Bases de Datos, al Correo, a la Intranet, a los Sistemas computacionales administrativos, control y de gestión, Contables y otros que se creen por la Unidad de Informática, son de propiedad de la Municipalidad de Pucón y son para uso estrictamente personal y se encuentran bajo responsabilidad del usuario interno al que se le asigna dicha cuenta con excepción de las cuentas genéricas de uso en los equipos y en servicios de internet Wi-Fi.

El acceso a la red datos y a los servicios de información debe hacerse desde un equipo debidamente registrado y/o autorizado por la Unidad de Informática.

No está permitido el acceso desde cualquier equipo y sistemas de información para obtener información o archivos de otros usuarios internos sin su permiso o para acceder a información que no es de su área o competencia, salvo requerimiento por escrito de su jefe directo o por decisión de las autoridades de la Municipalidad de Pucón.

No se deberá usar cuentas y contraseñas ajenas a las asignadas por el personal de la Unidad de Informática al usuario interno. Así mismo es responsabilidad de los usuarios internos no facilitar a otros su cuenta y su contraseña personal, que puede devenir en robo de información o manipulación de los documentos electrónicos, en los equipos informáticos, salvo que por necesidad de reparación el personal de la Unidad de Informática los requiera para reconstruir su perfil y documentación en el equipo dañado. En este caso el usuario interno posteriormente deberá solicitar el cambio de su contraseña.

No se permitirá ningún intento de vulnerar o atentar contra los sistemas de protección o seguridad de red. Cualquier acción de este tipo será comunicada inmediatamente a la Unidad de Informática para que ésta pueda iniciar cualquier acción de carácter administrativo, laboral o legal que corresponda.

Los usuarios internos no están autorizados para la utilización de los recursos de red con fines de proselitismo político, ni religioso, respetándose en todo momento las disposiciones y los derechos individuales de las personas.

Los usuarios internos no están autorizados a instalar programas ajenos a los autorizados por la Unidad de Informática.

No está autorizado cualquier programa ajeno a la red municipal que afecte el comportamiento de la misma o que haga uso de los equipos de comunicación intensivamente y merme sus rendimientos.

Los usuarios internos no están autorizados para almacenar y/o transmitir material difamatorio utilizando la Plataforma Tecnológica Municipal.

Los usuarios internos no están autorizados para efectuar descarga y distribución de archivos de música, videos y similares con fines no laborales utilizando la Plataforma Tecnológica Municipal.

Los usuarios internos no están autorizados para utilizar el recurso internet para acceder a radios, tv online, YouTube, redes sociales como Facebook, twitter, etc., ya que hacen uso de los equipos de comunicación intensivamente mermando el rendimiento de la red y de internet. Además, va en desmedro del rendimiento en las labores propias.

No está autorizada la instalación de puntos de acceso inalámbricos (access point – Wi-Fi) que se encuentren fuera de la administración (configuración y supervisión) de la Unidad de Informática, porque implican una brecha de seguridad a la información que se maneja dentro de la Municipalidad de Pucón.

No están autorizadas las acciones de usuarios, custodios o terceros (personal externo) que estén destinadas a modificar, reubicar o sustraer los recursos informáticos (equipos, periféricos, software, información, etc.) ni para alterar de manera fraudulenta su contenido.

El usuario no deberá acceder a los sistemas de información, servicios y bases de datos para los cuales no se le ha otorgado expresamente permiso, ni imprimir información confidencial y sacarla fuera de los ambientes de la Municipalidad de Pucón con la finalidad de publicarla o manipularla para perjudicar el funcionamiento de la institución o a personal del municipio.

Los usuarios externos no están autorizados para acceder a los sistemas de información municipal.

El término de la relación laboral con la institución que deberá ser informada inmediatamente por escrito a la Unidad de Informática, por la Oficina de Personal o la Administración Municipal, facultará al personal de la Unidad de Informática a inhabilitar inmediatamente la(s) cuenta(s) de usuario interno y/o modificar la(s) contraseña(s) actual(es), y transferir toda la información que haya creado durante su periodo laboral al personal designado y reconocido por la jefatura, previa autorización a solicitud escrita dirigida al Administrador Municipal y a la jefatura correspondiente.

5.4. SOBRE EL ACCESO A LOS SISTEMAS COMPUTACIONALES

Los accesos a los diferentes sistemas de información por los usuarios internos deberán ser solicitados vía documentación escrita elaborada por su respectiva jefatura y dirigidos hacia el Jefe de la Unidad de Informática, indicando claramente el nivel de privilegios o de acceso al sistema solicitado.

PROCEDIMIENTO DE SOLICITUD DE CUENTA DE ACCESO PARA SISTEMAS COMPUTACIONALES.

El Jefe de departamento que requiera cuenta de acceso para un funcionario de su dependencia, es decir, para un usuario interno, deberá hacerse responsable de completar el Formulario de Solicitud de Cuenta de Acceso, y presentarla en la Unidad de Informática, para su tramitación.

El Formulario de Solicitud de Cuenta de Acceso, podrá ser solicitado electrónicamente vía email, a la Unidad de Informática, y éste será enviado al jefe de departamento, de la misma forma.

El Formulario de Solicitud de Cuenta de Acceso, deberá identificar claramente al usuario y al sistema para el cual se está solicitando cuenta. Por lo tanto, deberá contener los datos: Nombre completo, RUN, Sistema, Fecha de inicio/fin de acceso. Además, deberá contener la individualización y firma del Jefe de departamento y funcionario solicitante. Además, contendrá todas las funcionalidades o tareas del sistema, en donde el jefe de departamento deberá señalar claramente qué tipo de permiso o privilegio tendrá su funcionario en dicha funcionalidad. También, el Formulario de Solicitud de Cuenta de Acceso, en su parte final, contendrá a modo de instrucción para el funcionario o usuario final, las indicaciones señaladas en el Decreto 83 de 2004 “Norma Técnica para los Órganos de la Administración del estado sobre seguridad y confidencialidad de los documentos electrónicos”, en su Art. 28 letras a) a la j), y lo señalado en su Art. N°31 letras a) a la c).

Finalmente, esta solicitud de cuenta será entregada por la Unidad de Informática, al Jefe del sistema, para su revisión y así, autorizar/modificar/rechazar los privilegios finales del usuario. En caso de existir rechazo o modificación de privilegios, el Jefe de sistema deberá indicar el motivo de tal decisión. Si ésta no fuera autorizada, será imposible la creación de la cuenta de acceso y en el caso de ser aprobada con modificaciones, la creación de la cuenta se realizará de acuerdo a los privilegios estipulados por el Jefe de Sistema.

Los jefes de Sistemas, serán los responsables finales de la administración de un sistema computacional, y serán nombrados mediante Decreto Alcaldicio.

Los Formularios de Solicitud de Cuenta de Acceso finales, deberán ser archivadas en un Archivo especialmente destinado para el registro de éstas, en la Unidad de Informática.

A continuación se incluye un Formulario de Solicitud de Cuenta de Acceso TIPO, ya que la zona de privilegios dependerá de cada sistema a autorizar:

FORMULARIO DE SOLICITUD DE CUENTA DE ACCESO

Pucón, ____ de _____ de 201__

IDENTIFICACIÓN DEL JEFE DE DEPARTAMENTO SOLICITANTE

Nombre completo : _____

Departamento Municipal : _____

Sistema Computacional: _____ Municipal ☐ Educación ☐ Salud ☐

Firma Jefe Departamento : _____

IDENTIFICACIÓN DEL FUNCIONARIO PARA QUIEN SE SOLICITA ACCESO

Nombre completo : _____ R.U.N. : _____ - ___

Periodo por el cual se solicita la cuenta : Desde ___ /___ /201__ hasta ___ /___ /201__

Labores a realizar con el acceso : _____

_____

_____

Firma Funcionario : _____

IDENTIFICACIÓN DEL JEFE DE SISTEMA

Nombre completo : _____

Fecha de Recepción del Formulario para revisión de privilegios de acceso : ___ /___ /201__

Periodo por el cual se le autoriza la cuenta : Desde ___ /___ /201__ hasta ___/___/201__

Firma Jefe de Sistema : _____

PRIVILEGIOS DE ACCESO AL SISTEMA

(Indicar "**Sí**" o "**No**" en cada opción)	**Nuevo**	**Modificar**	**Eliminar**	**Consultar**	**Listar**	**Imprimir**	**Observaciones Jefe Sist.**
Funcionalidad 1	☐	☐	☐	☐	☐	☐	_____
Funcionalidad 2	☐	☐	☐	☐	☐	☐	_____
Funcionalidad 3	☐	☐	☐	☐	☐	☐	_____
Funcionalidad 4	☐	☐	☐	☐	☐	☐	_____
Funcionalidad 5	☐	☐	☐	☐	☐	☐	_____
Funcionalidad 6	☐	☐	☐	☐	☐	☐	_____
Funcionalidad 7	☐	☐	☐	☐	☐	☐	_____
Funcionalidad 8	☐	☐	☐	☐	☐	☐	_____

USO EXCLUSIVO UNIDAD DE INFORMÁTICA

Con fecha : ___ /___ /201__ , _____ recibe Formulario de Jefe de Departamento

Con fecha : ___ /___ /201__ , _____ recibe Formulario revisado por el Jefe de Sistema

---------- **INDICACIONES DE USO A SEGUIR** ----------

* Identificadores : Claves o contraseñas. Son de carácter personal y reservado.

Los usuarios deberán cumplir con las obligaciones señaladas en el Decreto 83 de 2004 "Norma Técnica para los Órganos de la Administración del estado sobre seguridad y confidencialidad de los documentos electrónicos", en su Art. 28 letras a) a la j), y lo señalado en su Art. N°31 letras a) a la c), que indican lo siguiente:

Artículo 28.- La asignación de los identificadores se deberá controlar mediante un proceso formal de gestión, en que el jefe directo del usuario peticionario será el responsable de la respectiva solicitud.

Para los efectos del referido control, en cada institución se impartirán instrucciones sobre la forma de asignación de identificadores que se aplicará. Dichas instrucciones deberán incluir a lo menos, lo siguiente:

a) La obligación de mantener en forma confidencial de los identificadores que se asignen;
b) La obligación de no registrar los identificadores en papel;
c) La prohibición de almacenar identificadores en un computador de manera desprotegida;
d) El deber de no compartir los identificadores de usuarios individuales;
e) El mandato de no incluir el identificador en cualquier proceso de inicio de sesión automatizado, por ejemplo, almacenado en una macro;
f) La indicación de cambiar los identificadores cuando hayan indicios de un posible compromiso del identificador o del sistema;
g) La recomendación de elegir identificadores 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 consecutivos o grupos completamente numéricos o alfabéticos; y no sean palabras de diccionario o nombres comunes;
h) La indicación de cambiar los identificadores a intervalos regulares. Las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que los identificadores normales;
i) Normas para evitar el reciclaje de identificadores viejos, y
j) La indicación de cambiar el identificador temporal al iniciar la primera sesión.

Artículo 31.- Para reducir el riesgo de acceso no autorizado a documentos electrónicos o sistemas informáticos, se deberá promover buenas prácticas, como las de pantalla limpia.

En particular, se incentivará a los usuarios o configurar los sistemas de manera que se dé cumplimiento a los siguientes estándares:

a) Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que éstas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con protector de pantalla con una contraseña protegida;
b) Cerrar las sesiones de los computadores principales cuando la sesión finaliza, lo que no significa, necesariamente, apagar el terminal o los equipos, y
c) Asegurar los terminales o equipos frente al uso no autorizado, mediante una contraseña de traba o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.

---------- **FIN INDICACIONES DE USO A SEGUIR** ----------

PROCESO DE CREACIÓN DE CUENTA Y ENTREGA DE CLAVE DE ACCESO PARA SISTEMAS COMPUTACIONALES

La Unidad de Informática al recibir el Formulario de Solicitud de Cuenta de Acceso firmada por el Jefe de Sistema, procederá en los casos de:

- Rechazo: informar por escrito o electrónicamente, al jefe de departamento y al usuario solicitante, del rechazo de la creación de cuenta de acceso, para lo cual adjuntará copia del Formulario de Solicitud de Cuenta de Acceso final.
- Aprobación con modificaciones: crear la cuenta de acceso de acuerdo a los privilegios estipulados por el Jefe de Sistema, y creará una clave temporal de acuerdo a lo establecido por el Decreto 83 de 2004 "Norma Técnica para los Órganos de la Administración del estado sobre seguridad y confidencialidad de los documentos electrónicos" en su Art. N°28 letras g) e i). Luego deberá informar por escrito o electrónicamente, al jefe de departamento y al usuario solicitante, la modificación de los privilegios de acceso al sistema, para lo cual adjuntará copia del Formulario de Solicitud de Cuenta de Acceso final. Además, se le solicitará al usuario solicitante, su presencia en la Unidad de Informática, en donde se le entregará de manera personal el "Acta de Recepción de Clave de Acceso Temporal", la cual deberá firmar como acuso recibo de dicha clave de acceso.
- Aprobación sin modificaciones: crear la cuenta de acceso de acuerdo a los privilegios estipulados por el Jefe de Sistema, y creará una clave temporal de acuerdo a lo establecido por el Decreto 83 de 2004 "Norma Técnica para los Órganos de la Administración del estado sobre seguridad y confidencialidad de los documentos electrónicos" en su Art. N°28 letras g) e i). Luego deberá informar por escrito o electrónicamente, al jefe de departamento y al usuario solicitante, la aprobación sin observaciones de la clave de acceso al sistema. Además, se le solicitará al usuario solicitante, su presencia en la Unidad de Informática, en donde se le entregará de manera personal el "Acta de Recepción de Clave de Acceso Temporal", la cual deberá firmar como acuso recibo de dicha clave de acceso.

El Acta de Recepción de Clave de Acceso Temporal, deberá identificar claramente al usuario y al sistema para el cual se está solicitando cuenta. Por lo tanto, deberá contener los datos: Nombre completo, RUN, Sistema, Fecha de inicio/fin de acceso, Nombre del Jefe de departamento y Jefe del sistema autorizante. También contendrá todas las funcionalidades o tareas del sistema a las cuales se les permitió privilegios y su clave temporal. Adicionalmente, en su parte final, contendrá a modo de instrucción para el funcionario o usuario final, las indicaciones señaladas en el Decreto 83 de 2004 "Norma Técnica para los Órganos de la Administración del estado sobre seguridad y confidencialidad de los documentos electrónicos", en su Art. 28 letras a) a la j), y lo señalado en su Art.N°31 letras a) a la c).

Una copia del Acta de Recepción de Clave de Acceso Temporal, firmada por el usuario y por el personal de la Unidad de Informática que hace entrega del acta, quedará archivada en un Archivo especialmente destinado para el registro de éstas, en la Unidad de Informática.

A continuación se incluye un Acta de Recepción de Clave de Acceso Temporal TIPO, ya que la zona de privilegios dependerá de cada sistema a autorizar:

POLITICAS Y NORMAS

ACTA DE RECEPCIÓN DE CLAVE DE ACCESO TEMPORAL

IDENTIFICACIÓN DEL FUNCIONARIO A QUIEN SE AUTORIZA EL ACCESO

Nombre completo Usuario: _____ R.U.N. : _____ - ___

Nombre completo Jefe de Departamento: _____

Departamento Municipal: _____

Sistema Computacional: _____ Municipal ☐ Educación ☐ Salud ☐

Nombre completo Jefe de Sistema: _____

Periodo por el cual se le autoriza el acceso: Desde ___ /___ /201__ hasta ___ /___ /201__

PRIVILEGIOS DE ACCESO AL SISTEMA

(Indicar "**Sí**" o "**No**" en cada opción)	**Nuevo**	**Modificar**	**Eliminar**	**Consultar**	**Listar**	**Imprimir**	**Observaciones Jefe Sist.**
Funcionalidad 1							_____
Funcionalidad 2							_____
Funcionalidad 3							_____
Funcionalidad 4							_____
Funcionalidad 5							_____
Funcionalidad 6							_____
Funcionalidad 7							_____
Funcionalidad 8							_____

---------- **INDICACIONES DE USO A SEGUIR** ----------

* Identificadores : Claves o contraseñas. Son de carácter personal y reservado.

Los usuarios deberán cumplir con las obligaciones señaladas en el Decreto 83 de 2004 "Norma Técnica para los Órganos de la Administración del estado sobre seguridad y confidencialidad de los documentos electrónicos", en su Art. 28 letras a) a la j), y lo señalado en su Art. N°31 letras a) a la c), que indican lo siguiente:

Artículo 28.- La asignación de los identificadores se deberá controlar mediante un proceso formal de gestión, en que el jefe directo del usuario peticionario será el responsable de la respectiva solicitud.
Para los efectos del referido control, en cada institución se impartirán instrucciones sobre la forma de asignación de identificadores que se aplicará. Dichas instrucciones deberán incluir a lo menos, lo siguiente:

a) La obligación de mantener en forma confidencial de los identificadores que se asignen;
b) La obligación de no registrar los identificadores en papel;
c) La prohibición de almacenar identificadores en un computador de manera desprotegida;
d) El deber de no compartir los identificadores de usuarios individuales;
e) El mandato de no incluir el identificador en cualquier proceso de inicio de sesión automatizado, por ejemplo, almacenado en una macro;
f) La indicación de cambiar los identificadores cuando hayan indicios de un posible compromiso del identificador o del sistema;
g) La recomendación de elegir identificadores 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 consecutivos o grupos completamente numéricos o alfabéticos; y no sean palabras de diccionario o nombres comunes;
h) La indicación de cambiar los identificadores a intervalos regulares. Las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que los identificadores normales;

i) Normas para evitar el reciclaje de identificadores viejos, y
j) La indicación de cambiar el identificador temporal al iniciar la primera sesión.

Artículo 31.- Para reducir el riesgo de acceso no autorizado a documentos electrónicos o sistemas informáticos, se deberá promover buenas prácticas, como las de pantalla limpia.
En particular, se incentivará a los usuarios o configurar los sistemas de manera que se dé cumplimiento a los siguientes estándares:

a) Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que éstas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con protector de pantalla con una contraseña protegida;
b) Cerrar las sesiones de los computadores principales cuando la sesión finaliza, lo que no significa, necesariamente, apagar el terminal o los equipos, y
c) Asegurar los terminales o equipos frente al uso no autorizado, mediante una contraseña de traba o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.

---------- **FIN INDICACIONES DE USO A SEGUIR** ----------

CONSTANCIA DE ENTREGA DATOS DE ACCESO

Nombre Usuario: _____ Clave Temporal: _____

El Usuario deberá cambiar su clave temporal, al iniciar la primera sesión.

Con fecha: ___ /___ /201__ , se creó la cuenta de acceso con los privilegios autorizados.

Con fecha: ___ /___ /201__ , el funcionario recibió su nombre de usuario y clave temporal.

Para constancia, firman:

Firma Funcionario: _____ Nombre y Firma Informático: _____

PROCESO DE REVISIÓN DE CUENTAS DE ACCESO PARA SISTEMAS COMPUTACIONALES

La Unidad de Informática, cada año y al menos una vez, durante el mes de enero, procederá a la revisión de las cuentas de acceso para todos los sistemas computacionales. Opcionalmente, y dependiendo de la necesidad que manifestare el Jefe de departamento o el Jefe de sistema, podrá realizarse una revisión de cuentas de acceso para sistemas, total (todos los sistemas o cuentas de acceso) o parcial (un sistema o cuenta de acceso en particular).

Para la revisión general del mes de enero, la Unidad de Informática digitalizará los Formularios de Solicitud de Cuenta de Acceso finales del año anterior, y las enviará electrónicamente vía email a cada jefe de departamento, solicitando su revisión. Éste deberá revisar la continuidad de los usuarios y sus privilegios. En el caso de que la Cuenta de Acceso a sistemas, deba:

- Seguir en igualdad de condiciones: El jefe de departamento, devolverá el Formulario digitalizado, a la Unidad de Informática vía email con copia al Jefe de Sistema, indicando que ratifica la continuidad de la cuenta de acceso sin observaciones por un periodo que deberá indicar claramente, el cual no podrá ser superior a enero del siguiente año.
- Ser modificada en sus privilegios: El jefe de departamento, devolverá el Formulario digitalizado, a la Unidad de Informática vía email con copia al Jefe de Sistema, indicando que los privilegios deben ser modificados y solicitará un nuevo Formulario de Solicitud de Cuenta de Acceso, para ser completado. El procedimiento a seguir, será el mismo indicado en "PROCEDIMIENTO DE SOLICITUD DE CUENTA DE ACCESO PARA SISTEMAS COMPUTACIONALES" y luego en "PROCESO DE CREACIÓN DE CUENTA Y ENTREGA DE CLAVE DE ACCESO PARA SISTEMAS COMPUTACIONALES".
- Ser eliminada: El jefe de departamento deberá imprimir el Formulario digitalizad y escribir en ella con su puño y letra: "DEBE SER ELIMINADA POR (indicar motivo)". Luego, de igual forma escribir su nombre completo y firmarla para constancia. Después, deberá hacerla llegar en original a la Unidad de Informática, para que se proceda a la eliminación, y hacer llegar una copia al Jefe de Sistema y al usuario propietario de la cuenta, para su conocimiento. Finalmente, la Unidad de Informática realizará la eliminación de la cuenta e informará del acto al jefe de departamento, al Jefe de Sistema y al usuario, vía email, quienes deberán acusar recibo de la misma forma.

Para el caso de una revisión opcional, a petición de un Jefe de departamento o Jefe de sistema, la cual podrá solicitarse en la fecha que consideren necesario, deberá solicitar formalmente vía email a la Unidad de Informática la revisión del o los sistemas, o la revisión del o los usuarios en particular, individualizándolos claramente.

Para esta revisión opcional, la Unidad de Informática digitalizará los Formularios de Solicitud de Cuenta de Acceso finales, para el(los) sistema(s) o del(os) usuario(s) solicitado(s), y las enviará electrónicamente vía email al jefe de departamento o Jefe de Sistema que lo haya solicitado, para que procedan a su revisión. Éste deberá revisar la continuidad de los usuarios y sus privilegios. En el caso de que la Cuenta de Acceso a sistemas, deba:

- Seguir en igualdad de condiciones: El jefe de departamento o Jefe de Sistema que haya solicitado la revisión, devolverá el Formulario digitalizado a la Unidad de Informática vía email, indicando que ratifica la continuidad de la cuenta de acceso sin observaciones por un periodo que deberá indicar claramente, el cual no podrá ser superior a enero del siguiente año.
- Ser modificada en sus privilegios: El jefe de departamento o Jefe de Sistema que haya

solicitado la revisión, devolverá el Formulario digitalizado, a la Unidad de Informática vía email, indicando que los privilegios deben ser modificados y solicitará un nuevo formulario de Solicitud de Cuenta de Acceso, para ser completado. Si la modificación de privilegios la solicita el Jefe de sistema, éste deberá informar su modificación al Jefe de departamento, para que éste complete el nuevo formulario de Solicitud de Cuenta de Acceso y proceda a su tramitación. El procedimiento a seguir, será el mismo indicado en "PROCEDIMIENTO DE SOLICITUD DE CUENTA DE ACCESO PARA SISTEMAS COMPUTACIONALES" y luego en "PROCESO DE CREACIÓN DE CUENTA Y ENTREGA DE CLAVE DE ACCESO PARA SISTEMAS COMPUTACIONALES".

- Ser eliminada: El jefe de departamento o Jefe de Sistema que haya solicitado la revisión, deberá imprimir el Formulario digitalizado y escribir en ella con su puño y letra: "DEBE SER ELIMINADA POR (indicar motivo)". Luego, de igual forma escribir su nombre completo y firmarla para constancia. Después, deberá hacerla llegar en original a la Unidad de Informática, para que se proceda a la eliminación, y en el caso de que la eliminación la solicite el Jefe de Sistema, éste también deberá hacer llegar una copia al Jefe de departamento para que tome conocimiento de la medida. Finalmente, la Unidad de Informática realizará la eliminación de la cuenta e informará del acto al jefe de departamento, al Jefe de Sistema y al usuario, vía email, quienes deberán acusar recibo de la misma forma.

5.5. SOBRE LA INSTALACIÓN Y USO DE SOFTWARE Y APLICACIONES

El software y las aplicaciones que serán instalados en los equipos informáticos de la Plataforma Tecnológica serán aquellos que previamente hayan sido estandarizados por la Unidad de Informática y/o autorizado por la Municipalidad de Pucón y para los cuales se disponga de las licencias respectivas.

No deberá instalarse ningún tipo de software que no se encuentre autorizado por la Unidad de Informática en los equipos de la Plataforma Tecnológica Municipal. El usuario interno o el custodio son responsables ante la Municipalidad de Pucón y/o ante terceros (por ej. ADS, Microsoft, Autodesk, etc.), por la instalación y uso de cualquier software no autorizado que haya sido colocado en el equipo informático de su uso y responsabilidad.

No está autorizada la incorporación de programas propios del usuario interno, a menos que se cuente con la autorización escrita de la Unidad de Informática.

No está permitido desinstalar software, aplicaciones, borrar archivos del sistema o cambiar configuraciones pre-establecidas para los equipos informáticos de la Plataforma Tecnológica sin supervisión o conocimiento del personal de la Unidad de Informática.

No está autorizada la copia o distribución, para fines personales o comerciales, de cualquier aplicación o software protegido legalmente o violar cualquier derecho de autor o términos de licenciamiento adquiridos por la Municipalidad de Pucón, sin la autorización escrita del propietario del software.

No está permitida la instalación o uso de software de espionaje, monitoreo de tráfico o programas maliciosos en la red de datos que originen violaciones a la seguridad, interrupciones de la comunicación en red, que eviten o intercepten la autenticación del usuario (inicio de sesión en el dominio por ej.) por cualquier método, o que busquen acceder a recursos a los que no se les ha permitido expresamente el acceso a excepción de los servicios de control utilizados por la Unidad de Informática.

Toda instalación, desinstalación o traslado de software incluyendo los de "dominio público" o de "distribución libre" desde y hacia un equipo informático de la Municipalidad de Pucón requiere autorización y coordinación previos con la Unidad de Informática.

El usuario es consciente y reconoce los derechos de la Municipalidad de Pucón a tomar todas las acciones legales pertinentes al usar una licencia de software adquirido por la institución.

Cualquier software o aplicación instalado en un equipo informático que no cumpla con lo estipulado anteriormente, será desinstalado sin aviso previo y sin que ello origine ninguna responsabilidad del personal de la Unidad de Informática o de la propia Municipalidad de Pucón.

5.6. SOBRE EL USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

La asignación de una cuenta de correo institucional, es exclusivamente para apoyar el desempeño de las labores municipales encomendadas. En ningún caso es para fines personales.

Está prohibido usar los equipos de Informática de la Municipalidad de Pucón para enviar mensajes de amenaza o acoso a los usuarios de la institución o externos desde las cuentas de correo electrónico institucionales, lo cual será comunicado a las autoridades correspondientes para la sanción inmediata del usuario y el seguimiento respectivo de la Unidad de Informática.

No está permitido el envío de correos de tipo spam o con comunicaciones fraudulentas desde las cuentas institucionales, que originen daños a la imagen de la Municipalidad de Pucón. Tampoco está permitido remitir correos con mensajes, imágenes o videos obscenos o inmorales desde o hacia la Municipalidad de Pucón.

No está permitido el envío masivo de correo electrónico ("broadcasts"), que incluyan todos los usuarios de la red. Sólo podrán ser trasmitidos para dar a conocer temas institucionales y de trabajo, responsabilizándose el emisor por su contenido y previa autorización del jefe de área o la Unidad de Informática.

No está permitido usar identidades falsas en mensajes de correo electrónico institucionales, ya sea con direcciones ficticias o con una identidad que no sea la propia asignada por la Municipalidad de Pucón.

No está permitido usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores, revelar información privada sin el permiso explícito del dueño, dañar o perjudicar de alguna manera los recursos disponibles electrónicamente, para apropiarse de los documentos de la Municipalidad de Pucón.

Todas las políticas incluidas en este documento son aplicables al correo electrónico institucional. El correo electrónico debe usarse de manera profesional y cuidadosa, tomando especial cuidado en evitar el envío a destinatarios dudosos o destinatarios colectivos. Las leyes de derechos de autor y licencias de software también aplican para el correo electrónico.

No está permitido el uso de correo institucional para participar en una cadena de correos y/o mensajes que no cumplan fines institucionales. Se debe borrar este tipo de mensajes en el momento de recepcionarlos.

En ningún caso es permitido suplantar cuentas de usuarios ajenos.

Si al emitir un correo institucional, recibe de regreso un mensaje de error o "rebote", el titular de la cuenta deberá enviar de inmediato dicho mensaje a la Unidad de Informática, para analizar el origen de ello y tomar las medidas pertinentes.

No está permitido abrir archivos comprimidos (rar, zip, etc.) o archivos desconocidos que sean recepcionados en la cuenta institucional.

Ante la duda de la procedencia de un correo electrónico o la pertinencia de un archivo desconocido que venga como adjunto, el titular de la cuenta en ningún caso estará facultado para abrir dicho archivo, ya que podría tratarse de un virus informático que podría dañar la información contenida en su equipo o la integridad del mismo. Por lo tanto, antes que todo, deberá consultar a la Unidad de Informática los pasos a seguir, antes de realizar cualquier acción que decida por su cuenta.

Ante el término de la relación laboral, el titular de la cuenta deberá dar aviso inmediato a la Unidad de Informática y no estará facultado para eliminar los correos institucionales. Todo correo generado y/o recibido en el periodo laboral, es propiedad del municipio.

Ante la eventualidad de ya no ser necesaria la utilización de una casilla electrónica institucional, el jefe de área deberá informarlo de inmediato a la Unidad de Informática para su desactivación y respaldo.

En caso de acceder a la cuenta de correo institucional desde un equipo informático externo al municipio, es exclusivamente bajo la responsabilidad del titular de la cuenta institucional, quien se tendrá que hacer cargo del buen uso y de la protección de contraseña e información correspondiente.

En caso de sospechar apropiación indebida de la clave del correo institucional a su cargo, el titular de la cuenta deberá realizar de inmediato el cambio de la clave. Para ello podrá solicitar ayuda técnica a la Unidad de Informática.

5.7. SOBRE EL ACCESO A INTERNET Y OTROS SERVICIOS WEB

El único sitio Web autorizado de la Municipalidad de Pucón, es el inscrito con la dirección y www.municipalidadpucon.cl, cuyo contenido es propiedad intelectual de la Municipalidad de Pucón.

El material que aparezca en el sitio Web de la Municipalidad de Pucón debe ser aprobado por el Administrador Municipal y/o Jefe Oficina de Comunicaciones, respetando la propiedad intelectual (derechos de autor, créditos, permisos, protección y todos los que se aplican a cualquier material de esta naturaleza)

El sitio Web Municipal será evaluado periódicamente por parte de un Comité Web presidido por el Administrador Municipal y será este comité quien determine los procedimientos y responsabilidades para la actualización de los contenidos del sitio.

Los jefes de las unidades generadoras de contenido autorizado, deberán hacer llegar oportuna y electrónicamente la información a la Oficina de Comunicaciones o a la Unidad de Informática, en los formatos convenidos, para su actualización.

El encargado operativo(Jefe Of. Comunicaciones) encargado del diseño y/o mantenimiento del sitio Web o WEBMASTER, que administre información referente a la Municipalidad de Pucón debe acogerse a las políticas del Municipio incluyendo derechos de autor, leyes sobre obscenidad, calumnia, difamación y piratería de software. El contenido debe ser revisado periódicamente para asegurar su veracidad.

No está permitido el uso indebido de los recursos de internet con fines personales no laborales, a excepción de los usuarios conectados en las zonas Wi-Fi públicas.

No está permitido acceder a internet con fines comerciales o recreativos (juegos, chat, radio por internet, blogs de música y video para descargar o escuchar en línea, conversación en tiempo real), a excepción de los usuarios conectados en las zonas Wi-Fi públicas.

No está permitido usar cualquier tipo de conversación en línea, sin el requerimiento respectivo y/o el permiso expreso de las autoridades, a excepción de los usuarios conectados en las zonas Wi-Fi públicas.

No está permitido degradar el ancho de banda de la conexión IP a Internet, debido a descargas de archivos de música, imágenes, videos, etc., o empleo de radio o video en línea, no autorizado.

El responsable de la Unidad de Informática acogiendo las directivas de la Municipalidad de Pucón determinará los estándares para los contenidos considerados como oficiales para el desempeño de la labor profesional, técnica y administrativa. Cualquier otra página o sitio Web puede ser bloqueado sin necesidad de comunicación al usuario.

Para mayor detalle en cuanto al acceso del servicio internet, debe remitirse al Reglamento Interno "Uso de Servicio de Internet".

5.8. SOBRE LA PRIVACIDAD DE LA INFORMACIÓN EN LOS RECURSOS INFORMÁTICOS

Cuando los equipos y sistemas informáticos funcionan correctamente, el usuario interno debe considerar que los datos generados en éstos son información propiedad de la Municipalidad de Pucón y debe cuida la privacidad de ellos. Los usuarios deben estar conscientes sin embargo que ningún sistema de información es completamente seguro, y que hay personas dentro y fuera de la institución que pueden encontrar formas de tener acceso a la información, y por ello debe extremar los cuidados para no desproteger la información municipal.

Es responsabilidad del usuario interno contribuir en la protección de la información contenida en el recurso informático asignado, evitado divulgar contraseñas, no dejar sesiones abiertas al ausentarse de su puesto de trabajo, etc.

Es responsabilidad del usuario interno realizar el respaldo de su información municipal, así como es responsabilidad de éste informarse sobre los detalles de los tipos de licencia, cobertura, transferibilidad y certificación mediante solicitud a la Unidad de Informática. Podrá pedir ayuda a la Unidad de Informática si lo requiere.

El personal de soporte técnico tiene la autoridad para acceder a archivos individuales o datos cada vez que deban realizar mantenimiento, reparación o chequeo de equipos de computación internos. También tiene autorización para eliminar archivos innecesarios que degradan el buen funcionamiento del equipo y que no estén autorizados (software no autorizado, archivos de música, video, etc.).

Cuando se sospeche de uso indebido de los recursos informáticos de la Plataforma Tecnológica Municipal, el personal de la Unidad de Informática, con la autorización respectiva del Administrador Municipal o Jefe de Área, puede acceder a cualquier cuenta, datos, archivos o servicios de información pertenecientes al usuario interno involucrado para investigar e informar a las autoridades respectivas.

El personal de la Unidad de Informática está autorizado a monitorear los sistemas de información de la Municipalidad de Pucón para salvaguardar la integridad, disponibilidad, seguridad y desempeño correcto de los mismos y ejecutar las acciones pertinentes como: negación, restricción de acceso de usuarios o sistemas, aislamiento y desconexión de equipos o servicios.

La Unidad de Informática monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes, recolectando estadísticas de utilización basado en las direcciones de red, protocolo de red y tipo de aplicación, restringiendo las actividades del usuario y el uso de las aplicaciones innecesarias que incida en la degradación del rendimiento del tráfico y se informará al Administrador Municipal y Jefe de Área respectivo.

5.9. RESPONSABILIDADES DE LA UNIDAD DE INFORMÁTICA

Es responsabilidad de la Unidad de Informática, administrar, supervisar y mantener la plataforma Tecnológica de la Municipalidad de Pucón.

Identificar, inventariar y almacenar en lugar de acceso restringido los soportes que contengan programas y datos.

Mantener un catastro actualizado de los recursos y tecnologías de información que se encuentren operando en dependencias de la institución.

Mantener actualizado un Registro de accesos y utilización del recurso Base de Datos, para registrar en forma consistente todo evento realizado en los sistemas de Información con los siguientes atributos mínimos de identificación : fecha y hora cierta , usuario , recurso accedido, tipo y origen del acceso .

Mantener y actualizar un Registro de Incidentes de seguridad en el que conste el tipo de incidente (anomalía de cualquier tipo que afecte o pudiera afectar el Sistema de Información), la fecha y hora de producido, a quien se informa, efectos derivados del incidentes y medidas adoptadas.

Proponer, mantener y actualizar un Plan de Operaciones de contingencia, en un conjunto de pautas generales a seguir cuando se producen situaciones anormales o inusuales que afectan el procedimiento normal de datos.

Se considera que el correo electrónico es una comunicación directa y confidencial entre el que envía y el (los) que recibe (n) y no debe ser observado o reproducido por nadie más que éstos. El personal técnico de apoyo informático que por razones de su trabajo tenga acceso al servicio de correo electrónico, deberá tratarlo confidencialmente y se sujeta a las normas y conducta ética que ese cargo requiere y las sanciones que se determinen.

Acatar las disposiciones dictadas en las políticas de seguridad respecto al implante de software administrativo de gestión y control municipal, ofimática licenciado o de acceso libre y otros de productividad necesarios.

Realizar cambios de equipos, ubicación, conectar o inicializar nodos y periféricos, realizar modificaciones en los equipos, instalar y modificar ductos y otros elementos de comunicación en la red, cuando sea necesario para reparar o mejorar el recurso informático.

Todo requerimiento o solicitud de servicios a la Unidad de Informática por parte de los usuarios internos de la Plataforma Tecnológica Municipal se realizará por escrito a través de un Memorándum Interno, Oficio o correo electrónico dirigido a su Jefe de Área, quien a su vez, si estimare pertinente el requerimiento, lo solicitará formalmente al Jefe de la Unidad de Informática, de la misma forma descrita anteriormente.

La Unidad de Informática será la responsable de dar el soporte inicial a todos los servicios licitados por la Unidad a empresas externas (Software de Gestión, Conexión a internet, etc.), sin perjuicio de ser el Contacto Técnico para la supervisión del cumplimiento de los servicios estipulados por

contrato y en la canalización de los requerimientos por las vías dispuestas por cada empresa para solicitar correcciones a fallas o modificaciones a los servicios.

El personal que necesite su incorporación a los Sistemas de Personal y Remuneraciones(Reloj control para sistema biométrico) deberá realizar la solicitud directamente en la Oficina de Personal donde se le indicará los detalles del procedimiento a seguir, siendo la Unidad de Informática la responsable de la mantención de las bases de datos asociadas al servicio y su correcta operación.

Será responsabilidad de esta Unidad de Informática, mantener operativo el servidor que aloja el sitio Web de la Municipalidad de Pucón. No así la actualización del sitio web, ya que el encargado operativo es la Oficina de Comunicaciones, dado que es una herramienta propia de esa función municipal.

Realizar el respaldo diario de las bases de datos que utilizan todos los sistemas computacionales, el cual se deberá realizar automáticamente en un servidor propio, 2 veces por día, una vez a las 14:20 hrs, cuando las funciones ya han concluido las de la jornada de la mañana, y otra vez por la noche a las 21hrs, cuando ya están concluidas las funciones del día completo, para asegurarse de que contengan hasta la última información que se pudo trabajar en el día.

Cada día siguiente a primera hora de la mañana, entre las 8 y 9hrs, deberá ser sacadas una copia de estos respaldos generadas el día anterior a las 21 hrs, y en la tarde entre las 15 y 16 hrs, deberá ser sacada una copia de los respaldos generados ese mismo día a las 14:20 hrs. En ambos casos, a un disco externo para Backup que posee la Unidad de informática para estos efectos en dependencias de dicho departamento.

Cada día se sacará una segunda copia, que se almacenará en una unidad de respaldo con la debida protección, para almacenar ahí la tercera zona de respaldo de información, la que está ubicada en el CESFAM del departamento de salud, dado que es un lugar externo al edificio consistorial seguro para custodia.

Lo mismo se deberá hacer cada viernes, con las copias de sistemas en cuando a las carpetas de instaladores, manuales y nuevos ejecutables. Donde el primer respaldo está en un equipo de la Unidad de Informática, la segunda copia está en el disco externo para Backup. Y la tercera copia, estará en la unidad de respaldo que se encuentra en las dependencias del CESFAM del departamento de salud, sitio externo seguro fuera del edificio consistorial.

PROCEDIMIENTO DE RESTAURACIÓN DE BASES DE DATOS:
Después de conectarse a la instancia de SQL Server (Motor de base de datos de SQL Server), en el Explorador de objetos, hacer clic en el nombre del servidor para expandir el árbol.

1. Crear la **Base de Datos** con el nombre **original** respetando mayúsculas y minúsculas luego clic con el botón secundario en Base de datos recién creada, seleccionar **Tareas** luego **Restaurar** y, a continuación, hacer clic en **Base de datos**. Al hacer clic en Base de datos se abre el cuadro de diálogo **Restaurar base de datos**.
2. En la página **General**, aparece de manera predeterminada el nombre de la base de datos.
3. Posterior a ello se debe especificar el origen y la ubicación de los conjuntos de copias de seguridad que se deben restaurar, para ello se debe hacer clic en una de las opciones siguientes:

- **Desde base de datos**
  Escribir el nombre de base de datos en el cuadro de lista.
- **Desde dispositivo, que es nuestro caso ya que se utiliza la copia guardada en algún medio externo.**
  Hacer clic en el botón Examinar, se abrirá un cuadro de diálogo **Especificar copia de seguridad**, luego en la lista **Medio para copia de seguridad**, seleccionar uno de los tipos de dispositivo y seleccionar el respaldo que tendrá el mismo nombre de la base de datos a restaurar y finalmente hacer clic en **Aceptar** para volver a la página **General**.

4. En el cuadro **Seleccionar los conjuntos de copia de seguridad que se van a restaurar**, seleccione las copias de seguridad que desea restaurar.
5. Una vez seleccionada la copia a restaurar, hacer clic en Opciones en el panel **Seleccionar una página**.
6. En el panel **Opciones de restauración**, existen cuatro opciones:
   a. **Sobrescribir la base de datos existente**
   b. **Conservar la configuración de replicación**
   c. **Preguntar antes de restaurar cada copia de seguridad**
   d. **Restringir el acceso a la base de datos restaurada**

   En nuestro caso se debe seleccionar **sobrescribir la base de datos existente** ya que se necesita que la base de Datos se idéntica a la que originalmente existía conservando su diseño y contenido en forma íntegra.

   Para finalizar, una vez realizada la restauración de completa de todas las **Bases de Datos**, se realizan pruebas de las aplicaciones en estaciones de trabajo y se da cierre al proceso de **Restauración**.

Será responsabilidad de la Unidad de Informática, mantener operativo y administrar el servidor de correo institucional.

5.10. INCUMPLIMIENTO DE LAS POLITICAS

La Municipalidad de Pucón hará responsable al usuario de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento.

La Municipalidad de Pucón se reserva el derecho de evaluar periódicamente el cumplimiento de este reglamento. Cualquier acción disciplinaria derivada del incumplimiento de la misma, será considerada de acuerdo a la normativa legal vigente, a los procedimientos establecidos por la Municipalidad de Pucón y, en estricto acato a las directivas y reglamento interno de ésta.

El usuario que no cumpla con el uso correcto del software y hardware que componen la Plataforma Tecnológica Municipal, será directamente responsable de las sanciones legales derivadas de sus propios actos, y de los costos y gastos en que pudiera incurrir la Municipalidad de Pucón en defensa por el uso no autorizado o indebido de estos elementos.

6. NOTIFICACIÓN DEL REGLAMENTO

La Municipalidad de Pucón establecerá un Decreto aprobatorio del presente reglamento, el cual será distribuido inicialmente a la totalidad de los usuarios internos o funcionarios, a través de Oficio y correo electrónico, manteniendo copia en la página Web del Municipio para conocimiento de todo público.

La Oficina de Personal, entregará copia de este reglamento de manera electrónica o física, al personal nuevo que ingrese a desempeñar labores para el municipio, para su instrucción.

7. APLICACIÓN Y CUMPLIMIENTO

Esta política aplica a todos los integrantes de la Municipalidad de Pucón(áreas Municipal, Educación y Salud), sean Directivos, profesionales, técnicos, administrativos o personal auxiliar, en todas las formas de contrato vigentes: Personal de Planta, Contrata, Código del Trabajo o a Honorarios.

Cualquier usuario interno que viole este reglamento será objeto de la sanción disciplinaria pertinente.

También aplica a los usuarios de las zonas Wi-Fi públicas en las materias y puntos donde se señala sus responsabilidades, limitaciones, derechos y deberes. La Municipalidad de Pucón se reserva el derecho de denunciar a la justicia aquellos usuarios externos que incurran en ilícitos y se exime de responsabilidades por los actos de éstos que deriven en perjuicios a terceros.

Todo usuario que sea descubierto en la violación de estas normas, podrá ser suspendido del beneficio del uso del servicio, lo que implica la desconexión inmediata temporal o definitiva de la autorización de Acceso y, la solicitud de sanción quedando sujeto a la Ley Nº 19223 de fecha 28 de Mayo de 1993.