I. MUNICIPALIDAD
LIMACHE

DECRETO N° 1.493.-

LIMACHE, 29 de Abril de 2022.-

VISTOS;

1. Los Ords. N° 33/2021 de f/31.12.2021 y N° 09/2022 de f/22.03.2022, del Sr. Director de Control, sobre Reglamento de Políticas y Estándares de Seguridad Informática, visado por el Sr. Administrador Municipal;
2. Las atribuciones que me confiere la Ley N°18.695 de 1988, Orgánica Constitucional de Municipalidades, cuyo texto refundido, coordinado y sistematizado fue fijado por el DFL. N°1, del Ministerio del Interior, publicado en el D.O. de f/26.07.2006,

D E C R E T O :

1°.- Apruébase el **REGLAMENTO DE POLITICAS Y ESTANDARES DE SEGURIDAD INFORMATICA",** cuyo texto será el siguiente:

I- OBIETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de seguridad de la información en la Municipalidad tiene como principales objetivos:

- El resguardo de los activos de información mediante controles de seguridad aplicables a partir del análisis, evaluación y tratamiento de los riesgos que afecten su confidencialidad, integridad y disponibilidad:
- Confidencialidad: aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello;
- Integridad: salvaguardar que la información y los métodos de procesamiento sean exactos y completos;
- Disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.
- Asimismo persigue el aseguramiento de la continuidad operacional a través de acciones tendientes a gestionar los incidentes y a revertir y resolver eventuales contingencias.
  Para los efectos indicados, en el presente documento se establecen las políticas, prácticas y procedimientos dirigidos al cumplimiento de los objetivos precedentemente señalados.

II- ÁMBITO DE APLICACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

De los roles y responsabilidades: para el Sistema de Seguridad de la Información el municipio deberá nombrar mediante decreto alcaldicio:
Un Encargado de Seguridad de la Información. Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá tener, a lo menos, las siguientes funciones:

a) Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación y velar por su correcta aplicación.
b) Coordinar la respuesta a incidentes computacionales.
c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
   • Un comité de Seguridad de la Información formado por un equipo multidisciplinario que tendrá injerencia en las decisiones estratégicas relativas a la seguridad de la información.
d) La política de seguridad deberá incluir, como mínimo, lo siguiente:
   • Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia.
   • La difusión de sus contenidos al interior de la organización.
   Su reevaluación en forma periódica, a lo menos cada 3 años.
   Las políticas de seguridad deberán documentarse y explicitar la periodicidad con que su cumplimiento será revisado.
   La seguridad del documento electrónico se logra garantizando los siguientes atributos esenciales del documento: (Decreto 83, Art. 6)

a) Confidencialidad;
b) Integridad;
c) Factibilidad de autenticación, y
d) Disponibilidad.

III.- SANCIONES APLICABLES

a) Los funcionarios incurrirán en responsabilidad administrativa cuando infrinjan los deberes y obligaciones contemplados en este reglamento la que deberá ser acreditada mediante investigación sumaria o sumario administrativo sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.
b) La ley N°19.223 Tipifica las siguientes figuras penales relativas a la informática:
Artículo 1 °. - El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.
Artículo 2°. - El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de esta, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
Artículo 3°. - El que maliciosamente altere, dañe o destruya los datos o contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
Artículo 4°. - El que maliciosamente revele o difunda los datos contenidos en un sistema de información, Sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."

IV. NORMAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

PREMISAS:

Los equipos, infraestructura y aplicaciones de propiedad del municipio dispuestos para el uso y goce de los usuarios, bajo cualquier modalidad, sólo podrán utilizarse y destinarse al desarrollo de las tareas propias del ámbito laboral. Todos los datos procesados por medio de los elementos anteriormente mencionados son propiedad de la Municipalidad y, por tanto, poseen carácter confidencial.

DEFINICIONES:

a) Información: Grupo de datos ya supervisados y ordenados que sirven para la toma de decisiones simples o estratégicas dentro de la institución.
b) Usuarios: Persona (externa, funcionario público, personal contratado a cualquier título y bajo cualquier régimen legal por el Municipio, practicantes y cualquier colaborador) que utilice algún recurso tecnológico institucional ya sea un computador, notebook, Tablet, smartphone, etc. o acceda a los servicios de red corporativos.
c) Incidente de Seguridad de la Información: Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información.
d) Encargado de Seguridad de la Información: Es el responsable de planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información de la municipalidad, debidamente designado por la autoridad correspondiente.
e) Información o datos personales: Son aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificadles, como por ejemplo el RUT, dirección, etc.
f) Información o datos sensibles: Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
g) Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
h) Información confidencial: Propiedad de la información, la cual pretende garantizar el acceso sólo a las personas autorizadas.
i) Nombre de usuario o Login: Cadena de caracteres que se utiliza para identificar a un Usuario en la entrada a un sistema operativo, software, servicio tecnológico (Aplicación Web, Portales Web, Correo electrónico, Etc.) o redes privadas entre otros servicios.
j) Encargado o responsable del software: Es la persona, jefe o director de área que se relaciona directamente con la funcionalidad específica del módulo de software que utiliza. Por ejemplo,

el módulo de tesorería cuyo responsable es el Tesorero Municipal.

k) Programas P2P: Las aplicaciones P2P (peer to peer) son programas que permiten el intercambio de archivos entre internautas. Los más conocidos son LimeWire, Kazaa, Edonkeyy Emule.

V.- USO APROPIADO DE LOS RECURSOS

El equipamiento informático, software e infraestructura de red que la municipalidad ponga a disposición de los usuarios, deberá utilizarse solamente para los propósitos para los que ha sido concebido. La información que procesen estos recursos deberá ser tratada de manera confidencial, quedando expresamente prohibido:

a) Hacer uso del equipamiento con fines no relacionados con la actividad laboral;
b) Modificar, alterar, cambiar de ubicación física o dañar la configuración de los dispositivos de hardware, software y comunicaciones habilitados por la municipalidad para el desempeño de las funciones propias de cada usuario. En caso de que algún usuario requiera la instalación de componentes adicionales deberá comunicarlo su superior directo, el cual, en el evento de estimarlo pertinente, remitirá una solicitud formal a la Unidad de Informática. No se permitirá bajo ningún concepto la instalación de un software que no vaya acompañado de su correspondiente licencia;
c) Conectarse a la red corporativa a través de medios distintos a los establecidos por la Municipalidad;
d) Emplear Internet con fines ajenos a las tareas y obligaciones estipuladas en el ámbito laboral. Esta premisa se hace extensible al uso del correo electrónico y aplicaciones informáticas.
e) Acceder o intentar acceder sin autorización a los elementos y contenidos restringidos de los sistemas; así como leer, modificar o eliminar el correo electrónico personal de otros Usuarios.
f) Introducir intencionadamente en los Sistemas de Información de la Municipalidad programas potencialmente dañinos (malware), o con contenido amenazante, ofensivo u obsceno.
g) Intentar destruir, alterar, inutilizar o divulgar los datos e información de propiedad del municipio.

VI.- ROL DE LA UNIDAD DE INFORMÁTICA

La Unidad de Informática tendrá como función primordial dar soporte computacional a los distintos departamentos y direcciones municipales.

La Unidad de Informática realizará mantenciones preventivas, correctivas y proactivas a los equipos, programas, sistemas y software pertenecientes al municipio y que sean de su responsabilidad.

El jefe de Informática programará, elaborará calendarios de planificación de mantenciones computacionales al día.

Será de responsabilidad de la Unidad de Informática prestar ayuda y asesoría sólo cuando se trate de temas que competan al municipio.

Todo software que no haya sido instalado sin previa autorización podrá ser eliminado por el personal de Informática.

El personal de Informática procederá a verificar la integridad, configuración y estado de los equipos, y que estos se encuentren en el lugar que fue asignado o autorizado.

A la Unidad de Informática del municipio le corresponderá preocuparse permanentemente por la tecnología informática (software, hardware, equipos computacionales en general) y velar por el buen funcionamiento de los servicios que se entregan al usuario, brindando el soporte necesario y adecuado para que se puedan realizar las labores diarias en forma eficiente, controlando que se cumpla con la normativa vigente sobre Propiedad Intelectual, Protección de Datos de Carácter Personal y Seguridad de la Información para Órganos del Estado.

La Municipalidad, por medio de la Unidad de Informática deberá establecer y revisar periódicamente los diferentes controles de acceso a los sistemas de información que sostienen el servicio. Para ello determinará perfiles de usuario y limitará los accesos al sistema en función de las necesidades requeridas por cada funcionario para el desarrollo de sus actividades laborales.

VII-SEGURIDAD FÍSICA

Todos los equipos de computación (equipos portátiles, estaciones de trabajo, servidores, y equipos accesorios) conectados a la red de la municipalidad, aun cuando no sean de propiedad del municipio, estarán sujetos a la revisión y supervisión de la Unidad de Informática.

Todos los Usuarios deberán conocer y respetar las siguientes normas:

a) Prohíbase conectar a la red institucional, cualquier equipo ajeno a la Municipalidad sin la aprobación y revisión de la Unidad de Informática.

b) La protección física de los equipos corresponderá a los encargados y/o jefaturas correspondientes y a los funcionarios que hagan uso de estos.
c) Cuando se requiera trasladar o reubicar equipos, el jefe de la unidad respectiva deberá comunicarlo a la Unidad de Informática con el fin que ésta verifique previamente acaso el lugar al que pretenden ser trasladados cumpla con los requisitos técnicos y de seguridad necesarios y provea, en caso de ser necesario, los medios y condiciones que sea menester para tales efectos.
d) La Unidad de Informática llevará un registro actualizado de la ubicación de los equipos municipales, debiendo practicar una actualización de la ubicación del equipamiento al menos cada tres meses.
e) Corresponderá a Unidad de Informática realizar el mantenimiento preventivo y correctivo de los equipos, la verificación de la seguridad física y el acondicionamiento específico que corresponda, debiendo practicar una mantención preventiva de cada estación de trabajo al menos una vez al año debiendo coordinarse con cada departamento o Dirección;
f) Los usuarios no podrán compartir carpetas, impresoras o cualquier dispositivo sin la autorización de la Unidad de Informática. En caso de que se requiera compartir información o un dispositivo, se deberá canalizar una solicitud fundada a dicha unidad;
g) Queda estrictamente prohibido consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos. (D.S. 83 Art. 18).
h) Deberá evitarse que los equipos queden expuestos a temperaturas extremas puesto que ello altera su normal funcionamiento. (D.S. 83 Art. 18).
i) Prohíbase copiar o "piratear" sistemas programados a menos que ellos sean de dominio público (Shareware, Freeware); ya que ello puede implicar que municipio sea sancionado;
j) El usuario no podrá alterar los softwares y/o sistemas que se encuentren a su disposición.
k) ProhíbesE la instalación y uso de software de juegos de cualquier tipo;
l) Prohíbese cambiar la configuración de los equipos que ha sido determinada por la Unidad de Informática.
m) Ningún programa podrá ser instalado en otro sistema o computador diferente de aquél donde fueron instalados y licenciados.
n) Prohíbese la instalación individual de programas, (excepto previa autorización de la Unidad de Informática) como por ejemplo:
   - Demostraciones de proveedores.
   - Instalación de nuevas versiones para un software ya adquirido.
   - Utilización de programas de diagnóstico.

VIII.- SEGURIDAD LÓGICA

a) El acceso lógico al equipo especializado de computación (servidores, Switch, Firewalls, bases de datos, etc.) conectado a la red será administrado únicamente por personal autorizado de la Unidad de Informática del municipio;
b) Todo el equipo de computación que esté o sea conectado a la red incluso aquellos que no sean de propiedad municipal deberán sujetarse a los procedimientos de acceso establecidos por la unidad referida;
e) La Municipalidad, cuando corresponda, proveerá el servicio de acceso remoto a los recursos informáticos disponibles. El usuario deberá hacer uso de estos servicios en concordancia con los lineamientos generales de uso de Internet y los procedimientos que establezca la Unidad de Informática;
d) El manejo de información administrativa que se considere de uso restringido deberá tener acceso de Usuario y Contraseña con el objeto de garantizar su integridad. El control de acceso a cada sistema de información será determinado por la jefatura del departamento o unidad responsable de generar y procesar los datos respectivos;
e) La instalación y uso de los sistemas de información serán provistos únicamente por la Unidad de Informática;
f) Los servidores de bases de datos administrativos serán de uso exclusivo para esta función, por lo que sólo podrá acceder personal de la municipalidad autorizado por la Unidad de Informática.
g) La Unidad de Informática será la única responsable de instalar y administrar el o los servidores que se requieran;
h) Los accesos a las páginas web a través de los navegadores se sujetarán a las normas y restricciones de acceso del servidor de control de navegación de la Municipalidad. Quedarán restringidos a modo general los accesos a páginas de descargas de programas con contenido malicioso, videos no atingentes al ámbito laboral, herramientas de Chat distintas a las que proporcione la municipalidad, música, radios, sitios de contenido erótico, que inciten al odio o la discriminación por razones étnicas, raciales, religiosas o de orientación sexual o política;

i) El material que se publique en la página web institucional deberá respetar la ley de propiedad intelectual (derechos de autor, permisos y protección, como los que se aplican a cualquier material impreso);
j) La Municipalidad tendrá la facultad de revisar periódicamente el tráfico emanado de cada equipo conectado a la red municipal;
k) Los recursos disponibles a través de la red serán de uso exclusivo para asuntos relacionados con las funciones propias de la municipalidad y corresponderá solo a la Unidad de Informática administrar, mantener y actualizar la infraestructura de la red;
i) El correo de la Municipalidad será respaldado periódicamente de forma automática. Todo correo enviado o recibido en el sistema de correo municipal se considerará como parte de la información relativa al trabajo del funcionario. Se permitirá el uso de correos externos para uso personal estando prohibido el uso del correo personal para materias propias de la municipalidad, así como el envío o recepción de información relevante para el trabajo del funcionario a través de correos personales;
m) En los equipos informáticos se permitirá solamente la instalación de software autorizados por la Unidad de Informática, única autorizada y responsable de brindar asesoría, supervisión y soporte en la instalación de software informáticos en los equipos municipales que sean proporcionados a los funcionarios para el cumplimiento de sus funciones;
n) La adquisición y actualización de software para los equipos se llevará a cabo de acuerdo con una calendarización propuesta por La Unidad de Informática. Cualquier programa requerido por algún Usuario deberá ser solicitado y autorizado por el jefe del departamento al que pertenece el funcionario, este requerimiento deberá ser comunicado al Unidad de Informática, el cual realizará la evaluación técnica y económica del licenciamiento requerido. Corresponderá al Unidad de Informática autorizar cualquier adquisición o actualización de software.
o) La Unidad de Informática efectuará revisiones periódicas sin previo aviso al usuario para asegurar que sólo se estén utilizando software con licencia en los equipos de la municipalidad.
p) La información generada por los sistemas centralizados (bases de datos, correos, archivos en general) de la municipalidad será resguardada por la Unidad de Informática.
q) Cualquier software que requiera ser instalado para trabajar sobre la Red deberá ser evaluado previamente por la Unidad de Informática.
r) La Unidad de Informática realizará un monitoreo constante sobre todos y cada uno de los servicios, que estime necesario, que las tecnologías de Internet disponen en los sistemas considerados críticos, donde estos estarán bajo monitoreo permanente.
s) La Unidad de Informática analizará periódicamente el tráfico de datos en la red por medio de la revisión de conexión del servidor Proxy.

IX .- Seguridad de Redes

Deberán crearse VLAN para segmentar la Red Municipal, para optimizar el tráfico y seguridad.

La transmisión de Redes Wí-Fi y Alámbricas será mediante Certificados Digitales y su uso es exclusivo para Computadores que cumplan los requisitos de Seguridad para estar dentro de la Red Municipal.

En lo que se refiere a los Puertos de Salida, deberán sólo habilitarse los standard (80, 443), sólo previa solicitud fundada podrán habilitarse nuevos puertos.

En cuanto a los puertos de Entrada, adicionalmente al 1723 correspondiente a VPN, no deberá abrirse ninguno más; excepto que se necesite publicar algún servicio.

Los Servicios Publicados tales como FTP y Web deberán estar en la DMZ (Zona Desmilitarizada).

X .- RESPONSABILIDAD DE LOS USUARIOS

Cada usuario será responsable del equipamiento que la Municipalidad le ha confiado para el desarrollo de sus funciones laborales. Por ello, sólo podrá extraer de las dependencias de la Municipalidad, aquellos equipos y dispositivos autorizados por su jefe directo y previa autorización de la Administración Municipal, quien confiará dicha labor al Unidad de Informática para su ejecución y registro.

El usuario será responsable de proteger y cuidar diligentemente dicho equipamiento, así como la confidencialidad de la información perteneciente o confiada al municipio y deberá contribuir de manera activa al resguardo de ésta.

El usuario será responsable de sus contraseñas y en ninguna circunstancia deberá divulgarlas o cederlas a otra persona. Las contraseñas de usuario deberán ser robustas y difícilmente adivinables por terceros no autorizados.

En caso de detectar algún Incidente de Seguridad, de aquellos definidos como tal en esta política, o cualquier otro evento que haga presumir razonablemente que se pone en peligro la seguridad

del equipamiento o de la información confiada, el usuario deberá comunicarlo inmediatamente a su jefatura.

XL-PUESTO DE TRABAIO SEGURO Y ESCRITORIO LIMPIO

Será responsabilidad de los funcionarios de la Municipalidad cumplir con los requisitos y procedimientos de seguridad definidos para proteger el equipamiento desatendido y evitar así los accesos no autorizados a la información propiedad de la municipalidad. Para tales efectos se establecen como normas de obligado cumplimiento las siguientes:

a) Los documentos que contengan información sensible o confidencial permanecerán guardados bajo llave cuando no estén siendo utilizados, especialmente si el usuario no se encuentra en su puesto de trabajo.
b) Todas las estaciones de trabajo dispondrán de control de acceso mediante Usuario y contraseña, y mecanismos de bloqueo automático tras un período de inactividad del sistema.
c) Cuando el Usuario se ausente de su puesto de trabajo, deberá bloquear su terminal mediante Windows + L, o bien apagarlo directamente.
d) Los buzones de correo convencional, y fotocopiadoras nunca deben quedar desatendidos si no poseen algún tipo de protección.
e) La información impresa deberá ser recogida inmediatamente de las impresoras, una vez haya sido enviada a las mismas.
f) Al terminar la jornada laboral, el usuario deberá recopilar y asegurar el material confidencial, cerrar con llave cajones y oficinas, y desconectar todos los dispositivos y terminales que no vayan a ser utilizados, el equipo computacional deberá quedar siempre apagado al finalizar la jornada laboral.
g) No deberán quedar a la vista: nombres de Usuario, contraseñas, direcciones IP, directorios, contratos, números de cuenta, datos de funcionarios, impresiones y, en general, todo aquello que contenga información municipal.
h) Deberá promoverse la práctica de escritorio limpio. (D.S. 83 Art. 18).

XII .- RECOMENDACIONES DEL USO YCAMBIO DE CONTRASEÑAS

El nombre de usuario o Login estará directamente relacionado con la identidad del funcionario, trabajador o colaborador y con los atributos que sirve al cargo en la municipalidad. El nombre de usuario y la contraseña inicial serán asignados únicamente por la Unidad de Informática. El funcionario deberá hacer uso con respeto, cuidado y responsabilidad de las credenciales entregadas considerando siempre las siguientes obligaciones:

a) No entregar nombre de usuario ni contraseña a ninguna persona, incluyendo a sus superiores jerárquicos o personal de la Unidad de Informática.
b) Los usuarios deberán hacer cambio de sus contraseñas como mínimo mensualmente y como máximo trimestral y especialmente cuando sospeche que alguien pueda haberla conocido.

XIII .- RECOMENDACIONES PARA LA SELECCIÓN DE CONTRASEÑAS SEGURAS

a) Sustituir las contraseñas que le han sido asignadas por defecto por contraseñas difíciles de adivinar, de acuerdo con los criterios de robustez recomendados por la Unidad de Informática;
b) Mantener estricta reserva de sus contraseñas y no hacer uso de cuentas ajenas, ni siquiera con el permiso expreso del titular. Las cuentas de Usuario y sus contraseñas son personales e intransferibles.
e) Las contraseñas, deberán contener al menos ocho caracteres, y en una mezcla de cuatro diferentes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales como: ¡Mn1! @#$%A&*;" Sí sólo hay una letra o carácter especial, no debe ser el primero ni el último en la contraseña.
d) La contraseña no deberá ser un nombre propio, un vocablo soez o vulgar, o una parte del nombre de la persona o su dirección de correo electrónico.
e) La contraseña deberá ser robusta para los sitios en donde se almacena información cuya privacidad sea importante. Se deberán utilizar contraseñas diferentes para todos los sitios.

XIV .- NORMATIVA PARA EL USO DE COMPUTADORES PERSONALES Y ORDENADORES PORTÁTILES

Los computadores, equipos portátiles y teléfonos móviles que la Municipalidad pone a disposición de sus funcionarios y el personal, sólo deberán ser utilizados para desarrollar las actividades propias del municipio.
Cada usuario dispondrá de una cuenta personalizada, dotada de los accesos y aplicaciones

exclusivamente necesarios para el correcto desarrollo de sus labores profesionales. El usuario no deberá modificar ni vulnerar los permisos procurados por la organización ni podrá instalar aplicaciones no relacionadas con el trabajo. En caso de que el usuario estime necesaria la extensión de sus permisos o la instalación de una aplicación específica para llevar a cabo su labor, deberá consultarlo con su superior directo, el cual lo solicitará al Unidad de Informática para en caso de ser necesario, validar los accesos que correspondan.
No se aprobará la instalación de ningún software sin su correspondiente licencia.
El usuario deberá velar por la seguridad y confidencialidad de la información contenida en sus equipos, especialmente cuando se encuentre fuera de las dependencias de la municipalidad.
Los usuarios deberán, asimismo:

a) Bloquear su equipo al ausentarse de su puesto de trabajo. Se aconseja mantener activado un salvapantallas protegido con contraseña.
b) Asegurarse de que se realicen copias de seguridad de información confidencial o relevante para la municipalidad.

Además, en el caso de ordenadores portátiles, deberán observarse las siguientes normas generales:

a) En caso de tener que viajar con el equipo, éste nunca deberá ser enviado con el equipaje.
b) Nunca se deberá dejar el portátil desatendido y a la vista del público, especialmente en situaciones que puedan aumentar el riesgo de robo. En los hoteles u otros lugares de alojamiento o permanencia, el equipo deberá guardarse en un espacio cerrado bajo llave o en una caja fuerte.
c) En caso de pérdida del dispositivo informático portátil, el funcionario deberá notificar inmediatamente a su jefe directo y a la Unidad de Informática y denunciar el hecho a las autoridades policiales o judiciales.

Los equipos deberán ser entregados al usuario en perfecto estado y funcionamiento. Si el usuario detecta algún desperfecto, mal funcionamiento o contenido inadecuado al recibir el equipo, deberá poner inmediatamente esta circunstancia en conocimiento de su jefe directo con el fin de quedar exonerado de toda responsabilidad.

XV .- DE LOS RESPALDOS

Los respaldos de la Información es uno de los puntos más importantes que permitirán a la municipalidad el funcionamiento después de un desastre.
El objetivo de esta política es otorgar un medio por el cual poder recuperar información importante para no paralizar el funcionamiento normal del municipio.
Todos los documentos deberán ser almacenados obligatoriamente en la Carpeta Mis Documentos del usuario. Además, estará totalmente prohibido trabajar directamente sobre dispositivos externos.

6.1. Respaldo Documentos Desktop y Notebook
Este proceso será ejecutado automáticamente en las fechas programadas y/o cuando el usuario lo estime conveniente.
6.2. Respaldo Documentos Servidores
Este proceso programado por la Unidad de Informática en los Servidores y en los tiempos definidos por esta.
6.3. Seguridad de los Respaldos
Los respaldos, tanto Servidores, Desktops y Notebooks serán realizados con clave de encriptación, independiente para cada tipo de respaldo.
6.4. Periodicidad de los Respaldos
Los respaldos Desktop y Notebook críticos serán realizados al menos 1 vez al mes cuando se trate de un respaldo completo y/o diario cuando sea Incremental.
Los servidores tendrán un respaldo diario incremental y un respaldo completo semanal.
6.5. Ubicación de los Respaldos
Desktop y Notebook, serán Respaldos en Discos ÑAS en ubicaciones opuestos de la Municipalidad.

El respaldo principal de los servidores será realizado vía VPN con empresa externa (se entregará un DVD con respaldos diarios al mes), también se realizará un respaldo en Disco Externo el cual quedará almacenado en la Caja Fuerte Principal de la municipalidad. Deberá dejarse un registro firmado por la persona que realizó el proceso de respaldo, indicando fecha, hora, archivos respaldados de Servidores además del Nombre y Firma del funcionario.

XVI .- NORMATIVA DE USO RESPONSABLE DE INTERNET

Internet es un servicio que la Municipalidad pondrá a disposición de su personal para uso estrictamente profesional. Considerando que este recurso en el ámbito laboral aumenta las amenazas a la seguridad de la red pudiendo afectar la productividad de sus usuarios éstos

deberán cumplir con las siguientes obligaciones:

a) Los Usuarios serán los únicos responsables de las sesiones iniciadas en Internet desde sus terminales de trabajo y se comprometen a acatar las reglas y normas de funcionamiento establecidas en la presente normativa.
b) El acceso a Internet por personal externo requerirá la autorización previa y por escrito del encargado de la dirección o jefe de departamento respectivo.
c) Los usuarios deberán identificarse y autenticarse individualmente antes de obtener acceso a Internet.
d) La municipalidad se reserva el derecho a filtrar el contenido al que el usuario podrá acceder a través de internet desde los recursos y servicios de propiedad de la organización, así como a monitorear y registrar los accesos realizados desde los mismos.
e) En ningún caso, un usuario podrá modificar las configuraciones de los navegadores (opciones de Internet), de los equipos ni la activación de servidores o puertos sin la autorización correspondiente.
f) Prohíbase expresamente el acceso, la descarga y/o el almacenamiento en cualquier dispositivo de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenido que incumpla las normas éticas y de cortesía del municipio.
g) Prohíbase, asimismo, el almacenamiento en los equipos de archivos y contenidos que violen la legislación vigente relativa a Propiedad Intelectual. Los Usuarios deberán respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual de cualquier información visualizada u obtenida mediante Internet haciendo uso de los recursos informáticos y de la red municipal.
h) Bajo ningún concepto los usuarios podrán utilizar programas de descarga de archivos P2P o similares.
i) Prohíbase el uso de Internet mediante los recursos informáticos o de red de la municipalidad con fines recreativos, así como para obtener o distribuir material violento, pornográfico, que atente contra la dignidad de las personas o incompatible con los valores de la municipalidad.
j) El uso de chat o programa de conversación en tiempo real estará permitido solo a través de las plataformas que disponga la Unidad de Informática. Si un director, jefe de departamento o sección necesita autorizar a su personal para el uso de una plataforma distinta a las autorizadas, deberá justificar y solicitar de manera escrita la aprobación del uso de esta plataforma a la Unidad de Informática.
k) No se deberá buscar, hacer uso o apoderarse de información personal, ni se deberán obtener copias del software, archivos, datos ni contraseñas pertenecientes a usuarios de internet. No se deberá llevar a cabo, en ningún caso, la suplantación de forma voluntaria o consciente de otro usuario.
l) Cualquier Incidente de Seguridad relacionado con la navegación por Internet, deberá ser comunicado sin demora al jefe inmediato y a la Unidad de Informática.
m) Prohíbase la descarga de software ejecutables desde Internet sin autorización, especialmente la utilización de imágenes (como los formatos GIF, JPG, BMP o TIFF entre otros), sonido (formatos WAV y MP3 principalmente) y video (MPG, DivX, AVI, RAW o similares) para fines ajenos a la actividad laboral.

XVII .- NORMATIVA DE USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

El servicio de correo electrónico es una plataforma de comunicación brindada por el municipio que permite a los usuarios enviar y recibir mensajes electrónicos a todo el mundo. Este servicio se utiliza para mejorar la comunicación entre los funcionarios y entre entidades públicas o privadas. El acceso y uso de estos servicios por parte de los usuarios, así como los privilegios asociados a dicho acceso, deberán limitarse al ejercicio de sus obligaciones profesionales.
Los usuarios serán responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la municipalidad. Asimismo, los usuarios deberán considerar los riesgos y responsabilidades que implica el uso indebido de las direcciones de correo electrónico suministradas por el municipio.
Los Usuarios deberán tener presente lo siguiente:

a) No podrán utilizar la herramienta de correo electrónico con fines ajenos al cumplimiento de las funciones propias del cargo o al desarrollo de actividades ajenas al ámbito municipal;
b) La forma y contenidos de los correos enviados por el usuario deberán estar en consonancia con las normas éticas y de cortesía a que están obligados los funcionarios públicos, quedando prohibido el envío de correos ofensivos, amenazantes o que atenten contra la dignidad de las personas.
c) Los archivos adjuntos recibidos serán analizados por las herramientas antivirus antes de ser abiertos o ejecutados. Los correos sospechosos y sus adjuntos de dudosa procedencia no deberán ser abiertos y deberán eliminarse inmediatamente.

d) Informar a la Unidad de Informática sobre cualquier anomalía que detecten en su correo, así como de la apertura de un correo sospechoso o cualquier alerta generada por el antivirus.
e) En particular, están estrictamente prohibidas las siguientes prácticas catalogadas como abuso del correo electrónico:
   e)1) La difusión de contenido ilegal; como por ejemplo amenazas, código malicioso, apología del terrorismo, pornografía infantil, software pirata, o de cualquier otra naturaleza delictiva.
   e2) El uso no autorizado de servidores propiedad de la municipalidad para el envío de correos personales.
   e3) El envío indiscriminado de correos con intención de imposibilitar o dificultar el servicio de correo de la Municipalidad o de personas o entidades externas.
f) Deberán abstenerse de participar en cadenas de correo y responder o reenviar correos con contenido de advertencias de seguridad, ayuda solidaria y otros de índole similar.
g) Deberán mantener ordenados y clasificados todos sus buzones y carpetas. Los correos inservibles deben ser eliminados y todos los archivos adjuntos almacenados en el equipo o unidad de disco habilitada.
h) Los archivos adjuntos de elevado tamaño de bytes se deberán comprimir antes de ser enviados.
i) Al responder o reenviar un correo, se procederá a eliminar toda la información irrelevante, tal como direcciones, firmas, encabezados, etc.
J) No utilizar el correo electrónico institucional en sitios web asociados al retail, bancos, sitios pornográficos o aquellos que promuevan la violencia.
   El uso inapropiado de las herramientas informáticas en general, y del correo electrónico en particular, que provea la Municipalidad, deberá ser denunciado por todo usuario que tenga conocimiento de ello tanto a su superior jerárquico como a la Unidad de Informática y puede dar lugar a la instrucción de un proceso disciplinario respecto del infractor.

XVIII .- NORMATIVA DE USO DE IMPRESORAS Y OTRO EQUIPAMIENTO

Las impresoras y scanner son una herramienta que la Municipalidad habilita para aquellas funciones requeridas como consecuencia del desarrollo de la actividad propia de la organización.
El acceso y uso de estos servicios por parte de los Usuarios, así como los privilegios asociados a dicho acceso, deben limitarse al ejercicio de sus obligaciones propias del cargo.
Cuando la Municipalidad detecte un uso excesivo e inadecuado de estos recursos por parte de un usuario, podrá adoptar las medidas disciplinarias pertinentes.
En todo caso, el usuario deberá asegurarse de que no queden documentos impresos en la bandeja de salida o retenidos en la cola de impresión que contengan datos confidenciales, así como de retirar los documentos conforme vayan siendo impresos. Este mismo compromiso es aplicable respecto de scanner u otros dispositivos de análoga funcionalidad.

XIX .- NORMATIVA DE USO DE LA TELEFONÍA

La municipalidad, con el objeto de optimizar y facilitar el trabajo de sus funcionarios podrá entregar soluciones de telefonía a los que lo requieran por la naturaleza de sus funciones, debiendo éstos adoptar los resguardos correspondientes para evitar poner en peligro la integridad de la información de la Municipalidad o de las personas o entidades con que se relaciona, quedando los funcionarios sujetos a las limitaciones y restricciones establecidas en este reglamento ya las responsabilidades consiguientes.
El uso personal de las comunicaciones telefónicas estará permitido si es fortuito o insignificante y en la medida que no interfiera con las actividades laborales habituales ni perjudique su rendimiento. El acceso de los usuarios y sus privilegios asociados se verán limitados exclusivamente a aquellos que resulten imprescindibles para desarrollar las funciones correspondientes a sus obligaciones profesionales para con la municipalidad.
Siendo los equipos telefónicos de propiedad de la municipalidad, ésta se reserva el derecho de revisar la lista de llamadas realizadas y su historial de navegación web, con el objeto de verificar el cumplimiento de la normativa ante cualquier sospecha fundada o evidencia de uso fraudulento o abusivo del servicio.

XX .-DEFINICIONES

a) Autenticación: proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.
b) Confidencialidad: aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.
c) Contenido del documento electrónico: información, ideas y conceptos que un documento

expresa.

d) Continuidad del negocio: continuidad de las operaciones de la institución.
e) Disponibilidad: aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.
f) Documento electrónico: toda representación de un hecho, imagen o ¡dea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
g) Documentos públicos: aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.
h) Documentos reservados: aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter.
i) Documentos secretos: los documentos que tienen tal carácter de conformidad al artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado y su Reglamento.
j) Identificador formal de autenticación: mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.
k) Incidentes de seguridad: situación adversa que amenaza o pone en riesgo un sistema informático.
l) Información: contenido de un documento electrónico.
m) Integridad: salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.
n) Política de seguridad: conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.
o) Repositorio: estructura electrónica donde se almacenan documentos electrónicos.
p) Riesgos: amenazas de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia.
q) Sistema informático: conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
r) Usuario: entidad o individuo que utiliza un sistema informático.

2°.- Publique el presente Reglamento, en la página Web de la Ilustre Municipalidad de Limache.

ANÓTESE, TRANSCRÍBASE Y DÉSE CUENTA.-
(FDO.-) DANIEL MORALES ESPINDOLA, Alcalde de la Comuna de Limache. José Fernández Gómez, Secretario Municipal".

ES COPIA FIEL DEL ORIGINAL

JOSE FERNANDEZ GOMEZ
Secretario Municipal
Ministro De Fe

DISTRIBUCION:

1. Juzgado de Policía Local.
2. Sr. Administrador Municipal.
3. Secretaría Municipal.
4. Dirección de Control.
5. Dirección Asesoría Jurídica.
6. Dirección de Administración y Finanzas.
7. Dirección M. Ambiente, Aseo y Ornato.
8. Dirección de Obras Municipales.
9. Dirección de Desarrollo Comunitario.
10. Dirección de Seguridad Pública.
11. Dirección de Tránsito.
12. Secretaría Comunal de Planificación.
13. Departamento de Salud Municipal.
14. Departamento Adm. de Educación.
15. Tesorería Municipal.
16. Área Operativa.
17. Of. Adquisiciones.
18. Of. Habilitación.
19. Personal Municipal
20. Página Web.
21. Portal Transparencia Activa.
22. Archivo.

DME/JFG.
C:\Users\msantander\Documents\REGLAMENTOS\1493-2022 POLITICAS Y ESTANDARES DE SEGURIDAD INFORMATICA\1493-2022 REGLAMENTO DE POLITICAS Y ESTANDARES DE SEGURIDAD INFORMATICA.docx