LoBarnechea
NATURALMENTE LO MEJOR

ALCALDIA
SECRETARÍA COMUNAL DE PLANIFICACIÓN
DEPTO. DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

IDSGD:006221

DECRETO APRUEBA MANUAL DE SEGURIDAD DE LA INFORMACIÓN, DESIGNA ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN, ESTABLECE COMITÉ Y DESIGNA RESPONSABLES QUE INDICA.

DECRETO DAL N°0543/2020

LO BARNECHEA, 26-05-2020

VISTOS: lo dispuesto en el D.S. N°81, de 2005 del Ministerio Secretaría General de la Presidencia (SEGPRES), que aprueba norma técnica para los órganos de la Administración del Estado sobre la seguridad y confidencialidad de los documentos electrónicos, la norma chilena NCh-ISO 27001:2013, sobre sistema de gestión de seguridad de la información; y, en uso de las facultades que me confiere el artículo 56 y 63° letra i) de la citada Ley N°18.695, Orgánica Constitucional de Municipalidades, y;

TENIENDO PRESENTE:

a) Que toda organización que maneja sistemas tecnológicos debe resguardar y proteger su información y la de las personas y entidades con que se relaciona, de lo que se deriva la necesidad de establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información electrónica.

b) Que, para el establecimiento de dicho sistema de gestión de la información, resulta necesario contar con un Manual de Seguridad de la Información, que fije las pautas generales para el correcto uso de la información, permitiendo establecer las directrices que garanticen la seguridad y el correcto uso de los activos de información de la Municipalidad.

c) Que el D.S. N°83, de 2005, de SEGPRES, en sus artículos 7, 9 y 11 dispone la obligatoriedad de elaborar políticas de seguridad, y establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, con la finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos y la ciudadanía y el sector privado en general; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

d) Que, de acuerdo con lo establecido en el decreto referido anteriormente, los documentos electrónicos constituyen un activo para la entidad que los genera y obtiene, ya que la información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.

e) Que, de acuerdo con lo dispuesto en el artículo 12 del D.S. N°83, de 2005, de SEGPRES, debe designarse a un Encargado de Seguridad, que actuará como asesor del jefe de servicio en las materias relativas a seguridad de los documentos electrónicos;

f) Que, asimismo, con miras al establecimiento de un sistema de gestión de seguridad de la información que permita evaluar los riesgos existentes en el municipio en esta materia y adoptar los controles que se estimen imprescindibles para lograr mitigarlos o eliminarlos, se estima conveniente establecer un comité que apruebe la política de seguridad de la información para el Municipio de Lo Barnechea e imparta lineamientos generales en la materia.

DECRETO

1. **APRUÉBASE** el Manual de Seguridad de la Información, que se transcribe a continuación:

MANUAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

LoBarnechea JUNTOS HACEMOS UNA COMUNA MEJOR	**SGSI-CSI MANUAL DE SEGURIDAD DE LA INFORMACIÓN**		
	MUNICIPALIDAD DE LO BARNECHEA	Versión	1.0
		Fecha	11-05-2020

I. INTRODUCCIÓN

El objetivo de este manual es establecer las pautas generales que permitan el correcto uso de la información, sus repositorios y los medios de comunicación de manera integrada y coordinada con los requerimientos propios de la Municipalidad de Lo Barnechea (en adelante indistintamente “el Municipio” o “la Municipalidad”), las leyes que en su caso apliquen y la normativa interna.

Este manual puede ser complementado con normativas específicas en aquellos aspectos del servicio en los que sea necesario establecer normas concretas de actuación, las que deberán ser comunicadas oportunamente a todos los funcionarios y colaboradores del Municipio a los cuales se apliquen. En caso de contradicción, este manual prevalecerá sobre ellas.

Este documento debe ser constantemente actualizado de acuerdo con los avances y cambios en las tecnologías empleadas en nuestra organización.

Las normas establecidas en el presente manual tienen carácter obligatorio para toda persona que utilice recursos tecnológicos de la red de la Municipalidad.

II. NORMAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Premisas

El dominio, uso y goce de todos los equipos, infraestructura y aplicaciones dispuestos al servicio de los Usuarios por el Municipio, bajo cualquier modalidad, son propiedad de la Municipalidad y sólo se permite su utilización para desarrollar las tareas establecidas en el 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 utiliza algún recurso tecnológico institucional, tal como computador, notebook, tablet, smartphone, etc. o accede 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 personal o datos personales**: Son aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables, como por ejemplo el RUT o la dirección.
f) **Información sensible 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 contabilidad gubernamental, su responsable directo es el Jefe del Departamento de Contabilidad, el módulo de tesorería, su 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, Edonkey y Emule.

Uso apropiado de los recursos

El equipamiento informático, software e infraestructura de red que la Municipalidad pone a disposición de los Usuarios, debe utilizarse para los propósitos para los que ha sido concebido. Además, la información que procesan estos recursos debe ser tratada de manera confidencial. Debido a ello, queda 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 precise la instalación de componentes adicionales, deberá comunicarlo a su superior directo, el cual, tras valorar la petición, remitirá una solicitud formal al Departamento de Tecnologías de Información y Comunicación. No está permitido bajo ningún concepto la instalación de software que no vaya acompañado de su correspondiente licencia.
c) Conectarse a la red corporativa por medios distintos a los establecidos por la Municipalidad.
d) Emplear Internet con fines que no guarden en modo alguno, relación con las tareas y obligaciones estipuladas en el ámbito laboral. Esta premisa se hace extensible al uso del correo electrónico y aplicaciones informáticas.
e) 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 componentes potencialmente dañinos (malware), o con contenido amenazante, ofensivo u obsceno.
g) Intentar destruir, alterar, inutilizar o divulgar los datos e información que son propiedad de La Municipalidad.

El incumplimiento de cualquiera de las reglas establecidas en este manual puede dar lugar a responsabilidad administrativa, sin perjuicio de las responsabilidades penales y civiles que podrán también perseguirse. La Municipalidad desplegará los mecanismos que estime oportunos para velar por el uso apropiado de sus recursos.

III. ROL DE LA MUNICIPALIDAD

La Municipalidad, por medio del Departamento de Tecnologías de Información y Comunicación, es responsable de desplegar los medios técnicos y humanos que estén a su alcance, con el fin de garantizar la confidencialidad, integridad y disponibilidad de sus datos. Para ello colaborará de manera activa en la definición de las políticas, normativas, procesos y procedimientos que sean requeridos.

Es responsabilidad de La Municipalidad, por medio del Departamento de Tecnologías de Información y Comunicación, 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. Adicionalmente, siempre que sea de obligado cumplimiento, se tratará cualquier elemento introducido en los sistemas de información gestionados por la Municipalidad, según los requisitos establecidos por la normativa vigente sobre Propiedad Intelectual, Protección de Datos de Carácter Personal y Seguridad de la Información para Órganos del Estado.

El Departamento de Tecnologías de Información y Comunicación, será el responsable de brindar servicio directo de apoyo al Usuario con el equipamiento, instalación, alteración, cambio de lugar, configuración, etc. Además, se encargará de proveer, administrar y desarrollar recursos tecnológicos para la Municipalidad, con el propósito de facilitar el cumplimiento de la misión institucional a través de la mejora en sus procesos.

Seguridad física

Todos los equipos de computación (equipos portátiles, estaciones de trabajo, servidores, y equipos accesorios), que estén o sean conectados a la red de la Municipalidad, o aquel que en forma autónoma se tenga o que no sea propiedad del Municipio, debe de sujetarse a la revisión y supervisión del Departamento de Tecnologías de Información y Comunicación.

Todos los Usuarios deberán conocer y respetar las siguientes reglas:

a) Está absolutamente prohibido conectar a la red institucional, cualquier equipo ajeno a la Municipalidad sin la aprobación y revisión del Departamento de Tecnologías de Información y Comunicación.
b) La protección física de los equipos corresponde a quienes en un principio se les ha asignado, y corresponde notificar la necesidad de moverlos a los encargados y jefaturas correspondientes, y estos al Departamento de Tecnologías de Información y Comunicación. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de ellos. El Departamento de Tecnologías de Información y Comunicación llevará un registro actualizado de todos los responsables de los equipos municipales.
c) La reubicación de algún equipo de computación será responsabilidad de la Municipalidad o de personal externo contratado, y se hará únicamente bajo la autorización del responsable, siempre y cuando el lugar donde se materializará la ubicación cuente con los medios necesarios, y las condiciones de uso adecuadas, para la instalación del equipo.
d) La Municipalidad, a través de su Departamento de Tecnologías de Información y Comunicación, es la responsable de la realización del mantenimiento preventivo y correctivo de los equipos, además de la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. El Departamento de Tecnologías de Información y Comunicación, realizará una mantención preventiva de cada estación de trabajo una vez al año, llevando un cronograma de acuerdo con cada Usuario.
e) Los Usuarios no podrán compartir carpetas, impresoras o cualquier dispositivo, sin la autorización del Departamento de Tecnologías de Información. En caso de que se requiera compartir información o un dispositivo, se deberá canalizar una solicitud fundada al Departamento de Tecnologías de Información y Comunicación.
f) La Municipalidad a través de su Departamento de Tecnologías de Información y Comunicación, realizará una mantención preventiva al equipamiento de la red anualmente. Está se efectuará previo aviso a los Usuarios involucrados en el proceso.

Seguridad Lógica

- El acceso lógico a equipo especializado de computación (servidores, Switchs, Firewalls, bases de datos, etc.) conectado a la red es administrado únicamente por personal autorizado por La Municipalidad.
- Todo el equipo de computación que esté o sea conectado a la Red, o aquellos que en forma autónoma se tengan o que no sean propiedad de la institución, deben sujetarse a los procedimientos de acceso que emita la Municipalidad.
- La Municipalidad es el responsable de proporcionar el servicio de acceso remoto cuando corresponda y las normas de acceso 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 el Departamento de Tecnologías de Información y Comunicación.
- 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 de departamento o unidad responsable de generar y procesar los datos involucrados.
- La instalación y uso de los sistemas de información serán provistos únicamente por el Departamento de Tecnologías de Información y Comunicación.
- Los servidores de bases de datos administrativos son de uso exclusivo para esta función, por lo que se prohíben los accesos de cualquiera, excepto para el personal de La Municipalidad. El uso de estos, o quien se determine sea necesario, deberá ser autorizado por el Departamento de Tecnologías de Información y Comunicación.
- La Municipalidad es la responsable de instalar y administrar el o los servidores. Es decir, sólo se permiten servidores autorizados por la Municipalidad.
- Los accesos a las páginas web a través de los navegadores se sujetarán a las normas y restricciones de acceso por el servidor 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.
- El material que se publique en la página web institucional deberá ser aprobado por La Municipalidad, respetando la ley de propiedad intelectual (derechos de autor, permisos y protección, como los que se aplican a cualquier material impreso).
- La Municipalidad tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información y conservar información del tráfico emanado de cada equipo conectado a la red de la Municipalidad.
- Los recursos disponibles a través de la red serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la Municipalidad donde corresponde solo al Departamento de Tecnologías de Información y Comunicación administrar, mantener y actualizar la infraestructura de la red.
- El correo de la Municipalidad será respaldado periódicamente de forma automática. Todo correo enviado o recibido en el sistema de correo de La Municipalidad se asume como parte de la información relevante al trabajo del funcionario. Se permitirá el uso de correos externos para usos personales y se prohíbe el uso de correo personal para asuntos de la Municipalidad, así como él envió o recepción de información relevante para el trabajo del funcionario por correos personales.
- En los computadores de escritorio únicamente se permitirá la instalación de software autorizado por el Departamento de Tecnologías de Información y Comunicación.

Este departamento es el único autorizado y responsable de brindar asesoría, supervisión y soporte en la instalación de software informático en equipos de propiedad de La Municipalidad o que ésta entregue a su personal para el cumplimiento de sus labores.

- La adquisición y actualización de software para los equipos se llevará a cabo de acuerdo con una calendarización propuesta por el Departamento de Tecnologías de Información y Comunicación. 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 Departamento de Tecnologías de Información y Comunicación, el cual realizará la evaluación técnica y económica junto al Departamento de Planificación estratégica de la posible adquisición del licenciamiento requerido. Corresponderá al Departamento de Tecnologías de Información y Comunicación autorizar cualquier adquisición o actualización del software.
- El Departamento de Tecnologías de Información y Comunicación efectuará revisiones periódicas sin previo aviso al Usuario para asegurar que sólo exista software con licencia en los equipos de la Municipalidad.
- La información generada por los sistemas centralizados (bases de datos, correos, archivos en general) de la Municipalidad será resguardada por el Departamento de Tecnologías de Información y Comunicación.
- Cualquier software que requiera ser instalado para trabajar sobre la Red deberá ser evaluado previamente por el Departamento de Tecnologías de Información y Comunicación.
- El Departamento de Tecnologías de Información y Comunicación realizará un monitoreo constante sobre todos y cada uno de los servicios, que estime necesario, que las tecnologías de Internet e Intranet disponen en los sistemas considerados críticos, donde estos estarán bajo monitoreo permanente.
- El Departamento de Tecnologías de Información y Comunicación analizará periódicamente el tráfico de datos en la red por medio de la revisión de conexión del servidor Proxy o control de navegación de propiedad de La Municipalidad.

IV. RESPONSABILIDAD DE LOS USUARIOS

Cada Usuario es 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 o director de área y que sea informado para su autorización y registro por el Departamento de Tecnologías de Información y Comunicación. El Usuario es responsable de proteger y cuidar diligentemente dicho equipamiento, así como la confidencialidad de la información perteneciente o confiada a La Municipalidad, y deberá contribuir de manera activa al resguardo de ésta.

El Usuario se hace responsable de sus contraseñas y en ninguna circunstancia debe divulgarlas o cederlas a otra persona. Las contraseñas de Usuario deben ser robustas y difícilmente adivinables por terceros no autorizados.

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

la seguridad del equipamiento o la información confiados, el Usuario deberá comunicarlo inmediatamente a su jefatura.

Tendrá acceso a los sistemas administrativos, solo el personal de la Municipalidad que tenga la autorización del Usuario responsable del sistema aún si se trata de personal de apoyo administrativo o técnico.

Puesto de trabajo seguro y escritorio limpio

Es 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. Se establecen como normas de obligado cumplimiento:

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 o la oficina está vacía.
b) Todos los terminales y 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 Control+Alt+Supr, 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 debe ser recogida inmediatamente de las impresoras, una vez haya sido enviada a las mismas y liberada con su dispositivo de identificación.
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.
g) Con carácter general, nunca deben quedar a la vista: nombres de Usuario, contraseñas, direcciones IP, directorios, contratos, números de cuenta, datos de funcionarios, etc.

Como regla generar, los Usuarios deberán notificar a su jefatura directa, cualquier Incidente de Seguridad que detecten en relación con estas normas.

Recomendaciones del uso y cambio de contraseñas

El nombre de usuario o login están directamente relacionados 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 el Departamento de Tecnologías de Información y Comunicación. 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 clave secreta a ninguna persona, incluyendo a sus superiores jerárquicos o personal del Departamento de Tecnologías de Información y Comunicación.
b) No entregar ni solicitar el nombre de usuario o contraseña a nadie de la organización, o de terceros que pudiera conocer, a ninguna persona, incluyendo a sus superiores jerárquicos o personal del Departamento de Tecnologías de Información y Comunicación.
c) Los Usuarios deberán hacer cambio de sus contraseñas como mínimo mensualmente y como máximo trimestral y especialmente cuando sospeche que

alguien pueda haberla conocido (Por defecto Active Directory forzará el cambio de contraseña a los 90 días). No deberá repetir los Usuarios y contraseña en servicios en internet.

Recomendaciones para la selección de contraseñas seguras:

- Sustituir las contraseñas que le han sido asignadas por defecto por contraseñas difíciles de adivinar, de acuerdo con los criterios de robustez recomendados por Departamento de Tecnologías de Información y Comunicación.
- Mantener estricta reserva de sus contraseñas ni hacer uso de cuentas ajenas, ni siquiera con el permiso expreso del propietario de la cuenta. Las cuentas de Usuario y sus contraseñas son personales e intransferibles.
- Las contraseñas, deben contener al menos ocho caracteres, y en una mezcla de cuatro diferentes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales tales como !@#$%^&*,;" Si sólo hay una letra o carácter especial, no debe ser el primero ni el último en la contraseña.
- 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.
- La contraseña debe ser robusta para los sitios en donde almacena información cuya privacidad es importante. Se deben utilizar contraseñas diferentes para todos los sitios. Incluso en los que la privacidad no es un problema.
- Nunca confíe a un tercero sus contraseñas importantes (correo electrónico, banca, servicios médicos, etc.).

Normativa para el uso de PC’s y ordenadores portátiles

Los PC´s y equipos portátiles que la Municipalidad pone a disposición de sus funcionarios y el personal, sólo deben ser utilizados para desarrollar las actividades propias del Municipio. La petición de los equipos informáticos deberá ser formalizada por el responsable de cada área, empleando para ello una solicitud a modo de formulario que deberá ser revisada y autorizada por el Departamento de Tecnologías de Información y Comunicación. El uso de los equipos por personal externo se solicitará directamente al Departamento de Tecnologías de Información y Comunicación y requerirá previa autorización por escrito del jefe de departamento o el director de área donde se encuentra asignado el dispositivo.

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, especialmente con intención de instalar aplicaciones no relacionadas con el trabajo. En caso de que el Usuario estime oportuna 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 Departamento de Tecnologías de Información y Comunicación para en caso de ser necesario, validar los accesos solicitados con el encargado o responsable del software.

No se aprobará la instalación de 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. Para ello, cada Usuario:

a) Debe bloquear su equipo cuando vaya a ausentarse de su puesto de trabajo. Se aconseja mantener activado un salvapantallas protegido con contraseña.

b) Aunque no es recomendable almacenar en el equipo información confidencial o relevante para la Municipalidad, dado el caso, deberá asegurarse de que se realizan copias de seguridad de ésta.
c) Es obligación de todos los Usuarios que manejen información mantener el respaldo correspondiente de la misma, ya que se considera como un activo de la Organización que debe preservarse. Para ello cada Usuario dispone de una carpeta (repositorio) donde deberá guardar copia de los archivos digitales necesarios de respaldar como información del Municipio. Estos se almacenan físicamente en el servidor institucional de archivos el cual es copiado en horario nocturno no productivo y en donde los archivos serán resguardados físicamente en un sitio interno de la organización.
d) Todo el software propiedad de la Municipalidad deberá ser usado exclusivamente para asuntos relacionados con las actividades de la institución.
e) Todos y cada uno de los equipos de la red dispondrán de softwares de seguridad (antivirus, actualizaciones, privilegios de acceso, y otros que se apliquen) por tanto ningún Usuario está autorizado a desinstalar software de los equipos.

Además, en el caso de ordenadores portátiles, se hacen extensibles las siguientes normas generales:

f) En caso de tener que viajar con el equipo, nunca se debe enviar éste con el equipaje.
g) Nunca se debe dejar el portátil desatendido y a la vista del público, especialmente en situaciones que puedan aumentar el riesgo de robo. En los hoteles, el portátil deberá guardarse en un espacio cerrado bajo llave o en una caja fuerte.
h) En caso de pérdida del dispositivo informático portátil, el funcionario deberá notificar inmediatamente a su jefe directo y al Departamento de tecnologías de información y Comunicación.

Antes de introducir o descargar información en los equipos desde cualquier dispositivo móvil de almacenamiento, éste debe ser examinado por las herramientas de antivirus. Para verificar el cumplimiento de estas obligaciones, así como el correcto funcionamiento de los equipos y el buen uso de estos, el Departamento de Tecnologías de Información y Comunicación, realizará inspecciones periódicas con el objeto de examinar los siguientes aspectos: Aplicaciones instaladas, registro del sistema operativo, y estado del antivirus.

Estas revisiones podrán realizarse de forma aleatoria entre todo el personal tantas veces como la organización estime oportuno. Una vez examinado el equipo del Usuario, en caso de encontrar contenido no autorizado, se informará de manera inmediata y por escrito a su jefatura directa y director de área, los cuales deberán definir, comunicar y ejecutar las medidas oportunas consecuentes de no respetar las directrices

Los equipos deberán ser entregados al Usuario en perfecto estado y funcionamiento. Si el Usuario detectase 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 solucionar el incidente y que el Usuario quede exonerado de toda responsabilidad.

Los equipos de escritorio y ordenadores portátiles (a través de su docking), serán instalados y asegurados con candados anclados a cada escritorio, de manera de dificultar el hurto de estos. En caso de que un Usuario detecte la no existencia de este candado, deberá informarlo al Departamento de tecnologías de información y Comunicación y solicitar su instalación. Las llaves de los candados se encuentran administradas por el Departamento de tecnologías de información y Comunicación.

LoBarnechea
NATURALMENTE LO MEJOR
ALCALDIA
SECRETARÍA COMUNAL DE PLANIFICACIÓN
DEPTO. DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Normativa de uso responsable de internet

Internet es un servicio que la Municipalidad pone 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, se establecen las siguientes obligaciones:

a) Los Usuarios son 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 requiere 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 puede 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. En caso de que un Usuario considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, notificará a su responsable directo para que éste solicite al Departamento de Tecnologías de Información y Comunicación el acceso correspondiente.
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. Todos los equipos en que así lo estime la Municipalidad están configurados para su acceso a Internet.
f) Se prohíbe 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 de La Municipalidad.
g) Tampoco se permite 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 o de red de la Municipalidad.
h) Bajo ningún concepto los Usuarios podrán utilizar programas de descarga de archivos P2P o similares.
i) Se prohíbe 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 está permitido solo a través de la plataforma de Microsoft Teams, Whatsapp y Whatsapp Web. Si un director, jefe de departamento o sección necesita autorizar a su personal, para el uso de una plataforma distinta a las mencionadas, deberá justificar y solicitar de manera escrita la aprobación del uso de esta plataforma al Departamento de Tecnologías de Información y Comunicación.
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 Encargado de Seguridad.

m) Queda prohibida la descarga de software ejecutable 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.

Normativa de uso del correo electrónico

El correo electrónico es una herramienta que la Municipalidad habilita para aquellas comunicaciones requeridas como consecuencia del desarrollo de la actividad propia de la institución, con otras entidades, con la ciudadanía o con otros Usuarios. 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 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 ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por la Municipalidad. Los mensajes de correo transmiten información en sus encabezados (en principio ocultas) que indican datos adicionales del emisor, por lo que deben tenerse en cuenta posibles repercusiones (como daños a la imagen institucional y otros) que podría ocasionar una mala utilización de este recurso.

La utilización del correo electrónico por personal externo requiere la autorización previa y por escrito del director o jefe de departamento del área solicitante.

Los Usuarios deberán acatar las siguientes reglas:

a) No podrán utilizar la herramienta de correo electrónico con fines ajenos al propio desarrollo de las actividades encomendadas por la Municipalidad.
b) La forma y contenidos de los correos enviados por el Usuario deberán alinearse con las normas éticas y de cortesía marcadas por La Municipalidad, quedando prohibido, el envío de correos ofensivos, amenazantes, que atenten contra la dignidad de las personas o de mal gusto.
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 su eliminación debe ser inmediata.
d) Deberán comunicar a sus responsables directos 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.
   e.2) El uso no autorizado de servidores propiedad de la Municipalidad para el envío de correo personal.
   e.3) 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) Deben 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) Deben 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) A la hora de responder o reenviar un correo, se procederá a eliminar toda la información irrelevante, tal como direcciones, firmas, encabezados, etc.

El uso inapropiado de las herramientas informáticas en general, y del correo electrónico en particular, que provee la Municipalidad, debe ser denunciado por todo Usuario que tenga conocimiento de ello a su superior jerárquico y puede dar lugar a un proceso disciplinario y/o a la toma de las medidas disciplinarias correspondientes por parte de la Municipalidad.

Normativa de uso de impresoras y otro equipamiento
Las impresoras y scanners 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 profesionales.

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 scanners u otros dispositivos de análoga funcionalidad.

Normativa de uso de la telefonía
La Municipalidad, con objeto de optimizar y facilitar el trabajo de sus funcionarios ofrece soluciones de telefonía a los Usuarios que, por sus funciones, así lo necesiten. Sin embargo, el uso fraudulento del teléfono, fijo o móvil puede poner en peligro la integridad de la información de la Municipalidad o de las personas o entidades con que se relaciona, así como, lesionar sus intereses. Esto puede acontecer mediante la práctica de actividades consideradas ilícitas, que atenten contra la moral o la dignidad de las personas, que puedan resultar ofensivas o incluso como consecuencia del uso abusivo del mismo.

El uso personal de las comunicaciones telefónicas estará permitido si es fortuito o insignificante y no interfiere con las actividades laborales habituales ni perjudica el rendimiento de éstas. 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.

Los equipos telefónicos son propiedad de la Municipalidad y, por tanto, se reserva el derecho de revisar la lista de llamadas realizadas, con el objeto de verificar el cumplimiento de estas normas ante cualquier sospecha fundada o evidencia de uso fraudulento o abusivo del servicio.”

2. **DÉJASE SIN EFECTO** el decreto DAS N° 950 de fecha 13 de marzo de 2019, a través del cual se designó Encargado de Seguridad de la Información de la

Municipalidad de Lo Barnechea al Jefe de Tecnología e Información y Comunicación.

3. **DESÍGNASE** como Encargado de Seguridad de la Información, de acuerdo con lo dispuesto en el artículo 12 del D.S. N°83, de 2005, de SEGPRES, para que actúe como asesor del jefe de servicio en las materias relativas a seguridad de los documentos electrónicos, a don Ricardo Fabian Mendoza Leyton, R.U.T. 13.070.996-6, funcionario a contrata, grado 8, del Departamento de Tecnologías de Información.

4. **ESTABLECESE** un **Comité de Seguridad de la Información (CSI)**, que tendrá por misión validar y aprobar las políticas de seguridad de la información y los controles tendientes a regular el uso y manejo de la información que proponga el Encargado de Seguridad de la Información. Las funciones específicas del CSI son las siguientes:

   a) Responsable del ciclo de vida de las políticas de seguridad de la información.
   b) Validar y difundir las políticas a través de los medios de comunicación establecidos dentro de la Municipalidad de Lo Barnechea.
   c) Velar por la implementación de los controles de seguridad en la plataforma tecnológica de la Municipalidad.
   d) Promover la realización de cursos de seguridad de la información para todos los funcionarios.
   e) Revisar al menos una vez al año el funcionamiento del Sistema de Seguridad de la Información (SGSI).

5. **DESÍGNASE** a los siguientes funcionarios como integrantes del CSI:
   1. Administrador Municipal o quien éste designe;
   2. Director de Control Interno o quien éste designe;
   3. Director Jurídico o quien éste designe;
   4. Director de la Secretaría Comunal de Planificación o quien éste designe;
   5. Director de Gestión de Personas o quien éste designe;
   6. Jefe del Departamento de Tecnologías de Información y Comunicaciones; y,
   7. Encargado de Seguridad de la Información.

6. **PÚBLIQUESE** el Manual de Seguridad de la Información en la página web de la Municipalidad.

7. **INSTRÚYASE** a la Dirección de Gestión de Personas y al Departamento de Comunicaciones de informar permanentemente a todos los funcionarios y colaboradores del Municipio, por todos los medios pertinentes, acerca del manual que este decreto aprueba, así como la designación del Encargado de Seguridad de la Información y del CSI.

ALCALDIA
SECRETARÍA COMUNAL DE PLANIFICACIÓN
DEPTO. DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

VIVIAN BARRA PEÑALOZA	**JUAN CRISTOBAL LIRA IBAÑEZ**
SECRETARIO MUNICIPAL	**ALCALDE**
MUNICIPALIDAD DE LO BARNECHEA	**MUNICIPALIDAD DE LO BARNECHEA**

Este documento incorpora Firma(s) Electrónica(s) Avanzada(s)