MUNICIPALIDAD DE LA FLORIDA
REGION METROPOLITANA

De todas maneras

HOY SE DICTO LO QUE SIGUE:

DECRETO EXENTO Nº 2.950 .

LA FLORIDA, 17 SEP 2015

VISTOS:

El Ordinario N°21, de fecha 17 de septiembre de 2015, de Departamento de Informática, el Decreto Exento N°1612 de fecha 22 de mayo de 2015, que nombra al Encargado de Seguridad de la Información y designa a los funcionarios que integran al Comité de Gestión de Seguridad de la Información, el Decreto Exento N°2280 de fecha 24 de julio de 2015 que aprueba el Manual de Descripción de cargos del Departamento de Informática.

El Decreto N°372, de fecha 14 de agosto de 2015, que nombra a don Nicolás Fernando Alfonso Pizarro Juliá, como Administrador Municipal; el Reglamento N°83, de fecha 18 de febrero de 2013, que delega y asigna de modo general y permanente, las atribuciones y funciones específicas alcaldicias; el Reglamento N°84, de fecha 15 de abril de 2013, que modifica el Reglamento N°83, de fecha 18 de febrero de 2014.

Las facultades que me otorga el título II de la ley N°18695, Orgánica Constitucional de Municipalidades; y teniendo presente lo establecido en las leyes N°19.880 que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado y la Ley N°18.883, Estatuto Administrativo para funcionarios municipales.

CONSIDERANDO:

Lo requerido por el Jefe de informática subrogante en su Memorándum N°xxx de fecha 17 de septiembre de 2015, en donde señala la importancia de decretar la política de informática y el plan informático municipal con el propósito de regularizar, estandarizar y mejorar el impacto de la función de los sistemas y los recursos informáticos en las actividades propias de la Municipalidad de La Florida, en especial las que tienen impacto en la comunidad, con el propósito de aplicar de manera eficaz y eficientemente las tecnologías de información y comunicaciones en apoyo a los objetivos, políticas y estrategias de la gestión municipal.

Es necesario y relevante en todo estamento público describir las políticas de informática y comunicaciones para enunciar los principales lineamientos en relación con los aspectos generales de la informática y comunicaciones de la municipalidad de La Florida, con los sistemas de información municipal que apoyan la gestión administrativa, financiera y tecnológica, servicios de redes de datos, sistemas de telefonía y seguridad informática y seguridad de la información. Además con ello se da cumplimiento a los requisitos legales y fundamentación de procedimientos.

La Política de Informática estará dirigida a todos los empleados municipales, independientemente de la calidad jurídica de contratación que los regule, incluyendo al personal vinculado a empresas que prestan servicios al municipio y que laboran en instalaciones y que utilicen tecnologías de información y comunicaciones de propiedad del municipio. Estas políticas se aplicarán a todo equipamiento tecnológico que se vincule a la red municipal, al equipamiento propio o arrendado que tenga la Municipalidad de La Florida con el objetivo de brindar un adecuado servicio a la comunidad floridana.

De todas maneras

Esta Política de Informática se relaciona principalmente con las siguientes materias:

- Políticas de Seguridad Generales
- Políticas de Seguridad para Computadores y Respaldos de Información
- Políticas de Seguridad para las Comunicaciones
- Políticas de Seguridad para Redes
- Cuentas de los Usuarios
- Contraseñas y el Control de Acceso

De igual forma se consideran dos etapas para la implementación del Plan Informático Municipal, labor que corresponde al Comité de Gestión de Seguridad de la Información, designados de acuerdo al Decreto Exento N°1612 de fecha 22 de mayo de 2015 representados por el Encargado de Seguridad y el Jefe de Informática.

DECRETO:

1. **APRUÉBASE LA POLÍTICA DE INFORMÁTICA**, que a continuación se indica:

I. PROPÓSITO

Regularizar, estandarizar y mejorar el impacto de la función de los sistemas y los recursos informáticos en las actividades propias de la Municipalidad de La Florida, en especial las que tienen impacto en la comunidad, con el propósito de aplicar de manera eficaz y eficientemente las tecnologías de información y comunicaciones en apoyo a los objetivos, políticas y estrategias de la gestión municipal.

II. OBJETIVOS ESPECÍFICOS

Es necesario y relevante en todo estamento público describir las políticas de informática y comunicaciones para enunciar los principales lineamientos en relación con los aspectos generales de la informática y comunicaciones de la municipalidad de La Florida, con los sistemas de información municipal que apoyan la gestión administrativa, financiera y tecnológica, servicios de redes de datos, sistemas de telefonía y seguridad informática y seguridad de la información. Además con ello se da cumplimiento a los requisitos legales y fundamentación de procedimientos.

III. ALCANCE

La Política de Informática estará dirigida a todos los empleados municipales, independientemente de la calidad jurídica de contratación que los regule, incluyendo al personal vinculado a empresas que prestan servicios al municipio y que laboran en instalaciones y que utilicen tecnologías de información y comunicaciones de propiedad del municipio. Estas políticas se aplicarán a todo equipamiento tecnológico que se vincule a la red municipal, al equipamiento propio o arrendado que tenga la Municipalidad de La Florida con el objetivo de brindar un adecuado servicio a la comunidad floridana.

IV. RESPONSABLES

El Departamento de Informática y el Comité de Gestión de Seguridad de la Información designado por Decreto Exento N°1612 de fecha 22 de mayo de 2015, serán los responsables de la mantención, revisión y actualización de este documento anualmente, de tal forma que se consideren los cambios tecnológicos que influyan en el funcionamiento municipal o normas

De todas maneras

jurídicas que impliquen modificación de las políticas de informática.

Este documento es fruto del esfuerzo constante de la gestión municipal en búsqueda del mejoramiento continuo de los sistemas de información y comunicación apoyando la creciente modernización del Estado, e inducir la investigación y la incorporación de tecnología informática para contribuir al aumento de la calidad de los servicios al usuario y la eficiencia en los procesos propios de la gestión pública del sector municipal.

En el último tiempo, las tecnologías de información y comunicaciones han alcanzado un grado importante de desarrollo, consolidándose como una herramienta imprescindible de apoyo en la solución de algunos de los muchos problemas que enfrenta diariamente la compleja administración en el ámbito municipal a nivel nacional.

Las inversiones realizadas en esta área han sido resueltas para apoyar la gestión operativa de las unidades involucradas a través de una mejora escalada y sustancial en la calidad y oportunidad de la información, contribuyendo a facilitar el proceso de toma de decisiones y han permitido también automatizar integralmente una parte importante de las funciones que desarrollan las diferentes Direcciones de la Municipalidad.

Durante la formulación del presupuesto municipal, las Direcciones Municipales, Departamentos o Secciones deberán presentar al Departamento de Informática los antecedentes de todos los proyectos de desarrollo tecnológico que requieran, así como las necesidades de software y de hardware, los cuales serán evaluados por el Departamento de Informática, esta información será imprescindible para la presentación de la cartera de proyectos y adquisiciones Municipal y se incluirán los proyectos sancionados dentro del Plan Informático y del Plan de Compras de la Municipalidad.

El Departamento de Informática deberá asegurar la interconexión y compatibilidad de los servicios y sistemas Informáticos en los proyectos propuestos.

Las soluciones computacionales implementadas en la Municipalidad de La Florida, implementadas tanto con recursos propios, han contribuido a mejorar el acceso a la información, la calidad de la atención otorgada y maximizar la eficiencia de la red Municipal y de la gestión técnico-administrativa.

Con el objetivo de velar por el buen funcionamiento y el óptimo desempeño que puedan generar los "Equipos y Sistemas Informáticos" de la Municipalidad de La Florida, se trabajara día a día con la implementación e implantación de políticas que definan y marquen las directrices que todos los colaboradores del ente municipal deben seguir, para lograr avanzar juntos en una misma dirección, siempre con el fin de mejorar y sacar adelante sus labores cotidianas en pro de brindar un servicio de calidad a toda la ciudadanía.

Los usuarios son responsables de cumplir con todas las políticas de la Municipalidad de La Florida relativas a la Seguridad Informática y en particular a las Políticas de Seguridad.

V. POLÍTICAS DE SEGURIDAD GENERALES

a) Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los Sistemas Informáticos.
b) No divulgar información confidencial de la municipalidad a personas no autorizadas.
c) Mantener información municipal en equipos computacionales propios (Notebook, Netbook o Pc's) sin autorización escrita de la jefatura directa, así como también

De todas maneras

mantener bases de datos u otra información de propiedad municipal o generada con fines exclusivos de las funciones que se desempeñan en el municipio en dispositivos removibles o discos externos

d) No permitir ni facilitar el uso de los sistemas informáticos de la municipalidad a personas no autorizadas.
e) No se permite la interconexión a la red interna del edificio Municipal a toda aquella persona que no sea funcionario de la institución, con la salvedad de funcionarios externos que provengan de Instituciones y que estén debidamente autorizados y validados por la Administración Municipal.
f) No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Municipalidad de La Florida.
g) No se permite el uso de dispositivos de banda ancha móvil dentro del recinto municipal.
h) Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
i) Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas. Al asignársele cuenta de usuario se debe cambiar en el primer acceso la contraseña por una de las características señaladas
j) Reportar inmediatamente a su jefe inmediato y al Jefe del Departamento de Informática cualquier evento que pueda comprometer la seguridad de la Municipalidad de La Florida y sus recursos informáticos, como por ejemplo problemas eléctricos, virus informático, intrusos, modificación o pérdida de datos, daño por eventos de la naturaleza, falla por vida útil o maltrato y otras que comprometan el normal funcionamiento de los recursos puestos a disposición para la realización de las labores propias del cargo.

VI. POLÍTICAS DE SEGURIDAD PARA COMPUTADORES Y RESPALDOS DE INFORMACIÓN

a) Los computadores de la Municipalidad de La Florida sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
b) Es responsabilidad de los usuarios, velar por el aseo y protección de los equipos de trabajo; esto incluye limpieza de las zonas donde se encuentran instalados los equipos, utilizar medios de protección contra el polvo, agua, incendio, etc.
c) Los equipos de la Municipalidad de La Florida sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
d) Está prohibido a los usuarios modificar la configuración de hardware y software establecida por el Departamento de Informática.
e) Como medida de higiene y de seguridad del equipo físico informático (Hardware), queda totalmente prohibido sin excepción alguna el fumar, ingerir bebidas o alimentos mientras se estén utilizando las estaciones de trabajo, impresoras y cualquier otro equipo que tenga que ver con la infraestructura informática, ya que este tipo de práctica pone en riesgo el buen funcionamiento de los dispositivos.
f) Será responsabilidad del encargado del equipo de trabajo; el velar por el buen funcionamiento y cuidado del computador; por lo tanto si este último llegase a quebrantar negligentemente la política "referida a la higiene y seguridad del equipo físico informático", recaerán sobre este todas las acciones pertinentes, para lograr que la estación de trabajo se mantenga funcionando en su estado normal entre las acciones

De todas maneras

están:

- El reemplazo total o parcial del equipo afectado en un periodo que no sobrepase los 30 días; a partir del día en que ocurrió el accidente.
- En caso de pérdida de información estratégica e indispensable para la Municipalidad, sobre el encargado del computador recaerán las medidas administrativas que imponga la Administración Municipal.
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente al Jefe del Departamento de Informática ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción y mal uso. Las medidas que se deben de implantar, incluyen el uso de cerradura con llave y reforzar la vigilancia.
- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- No pueden moverse los equipos o reubicarlos sin conocimiento y autorización del Departamento de Informática, quien informará a la Administración Municipal en caso de ser necesario.
  Para llevar un equipo fuera de la Municipalidad se requiere una autorización escrita del Jefe del Departamento de Informática con previa aprobación de la Administración Municipal.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente al Jefe del Departamento de Informática y al Administrador Municipal.
- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 10 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben ocultar de la pantalla.
- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Municipalidad de La Florida está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales. Es responsabilidad de cada usuario hacer entrega de todos los discos referentes a las licencias que posea la estación de trabajo que está bajo su cargo al Jefe del Departamento de Informática; en el caso de pérdida de los discos por parte del usuario, este último debe de justificar por escrito ante el Jefe del Departamento de Informática y ante la Administración Municipal bajo que situaciones se generó la pérdida. Estos últimos se encargarán de aplicar la sanción administrativa correspondiente.
- Los usuarios no deben copiar a un medio removible (como un diskette, CD-ROM, dispositivos de almacenamiento masivo), el software o los datos residentes en las computadoras de la Municipalidad de La Florida, para ser trasladados fuera de las instalaciones, sin la aprobación previa del Jefe del Departamento de Informática.
- No pueden extraerse datos fuera de la sede de la Municipalidad de La Florida sin la

De todas maneras

aprobación previa de la Administración Municipal y del Jefe del Departamento de Informática. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como internet.

- El municipio cuenta con un antivirus corporativo que es el que se utiliza en el equipamiento municipal, no está permitida la instalación de otras aplicaciones con este fin. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe del Departamento de Informática para que se tomen las medidas correspondientes y poner la PC en cuarentena hasta que el problema sea resuelto.
- Debe utilizarse el programa antivirus para examinar todo software que venga de afuera (Internet) o inclusive de otros departamentos de la Municipalidad de La Florida.
- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.
- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. No se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el Departamento de Informática.
- No deben usarse diskettes, pendrive u otros medios de almacenamiento en cualquier computadora de la Municipalidad de La Florida a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Municipalidad de La Florida deben entregarse al Departamento de informática para su debido resguardo.
- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Departamento de Informática es responsable de hacer copias de respaldo periódicas. Los Directores de las distintas dependencias son responsables de definir qué información debe respaldarse, así como la frecuencia y el método de respaldo (por ejemplo: incremental, total).
- La empresa o las empresas proveedoras de Sistemas de Gestión Municipal (en caso que existan contratos de esa naturaleza) deben entregar respaldos mensuales de la información de las bases de datos y son dichos proveedores los responsables de mantener los sistemas en funcionamiento regular y dar cuenta al Departamento de Informática cuando se presenten fallas que tengan relación con el funcionamiento de la red municipal.
- Los usuarios deben de vigilar cautelosamente las impresoras, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Municipalidad de La Florida.
- El personal que utiliza un computador portátil que contenga información confidencial de la Municipalidad de La Florida, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar debidamente respaldada y protegida.

VII. POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES

Los sistemas de comunicación de la Municipalidad de La Florida generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la

productividad del empleado ni con las actividades propias de la Municipalidad de La Florida.

a) Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

b) La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Municipalidad de La Florida y en tal sentido deben usarse las horas no laborables.

c) Uso correcto del correo electrónico

- Los buzones de correo del municipio se rigen por una política que regula, el tamaño del buzón de correo, el tamaño de los archivos adjuntos y la cantidad de destinatarios, según detalla la siguiente Tabla:

Tipo de Usuario	Límite de envío (adjuntos)	Límite de recepción (adjuntos)	Cantidad de destinatarios	Tamaño del Buzón
Normal	7 Mb	7 Mb	10	120 Mb
Directivo	10 Mb	10 Mb	50	500 Mb

VIII. POLÍTICAS DE SEGURIDAD PARA REDES

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Información concerniente a la Municipalidad de La Florida; al estar conectada a redes de computadoras.

a) Es política de la Municipalidad de La Florida prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria.

b) Todos los cambios en los servidores y equipos de red de la Municipalidad de La Florida, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia debidamente autorizado por el Administrador Municipal y con el conocimiento del Jefe del Departamento de Informática. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial. Además, se deberá informar al oficial de Seguridad el cual deberá verificar que los cambios se realicen de acuerdo a lo protocolizado.

IX. CUENTAS DE LOS USUARIOS

a) Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
b) La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada por el Jefe del Departamento de Informática.
c) No debe concederse una cuenta a personas que no sean empleados de la Municipalidad de La Florida a menos que estén debidamente autorizados por la Administración Municipal.

De todas maneras

d) Es responsabilidad de cada Jefe de Departamento, el emitir la solicitud de creación, actualización o eliminación (ya sea temporal o definitiva, por causas como vacaciones, incapacidades, despido, u otra) de una cuenta de usuario de la red municipal para cada uno de los demás colaboradores del departamento.
e) Es responsabilidad del Jefe del Departamento de Recursos Humanos suministrar al Jefe del Departamento de Informática las respectivas acciones de personal de todo aquel funcionario que posee una cuenta de acceso a la red municipal. Esto con el objetivo de que este último realice las labores de mantenimiento al módulo de usuarios del sistema y así mismo adjunte la respectiva justificación.
f) Es responsabilidad del Jefe de Departamento de Informática emitir un documento oficial en el cual se estipule explícitamente el nivel de acceso a la red municipal si así lo solicita el Director de la dependencia. Dicho documento contara con la firma tanto del Jefe de Departamento de Informática como del nuevo usuario de la cuenta.
g) El Jefe del Departamento de Informática es el único funcionario de la institución que autoriza la creación, actualización o eliminación de las cuentas de los usuarios de la red municipal.
h) Como medida de seguridad y control cada cuatro meses (cuatrimestral), se cambiarán todas las claves de los usuarios de la red municipal, esto con el objetivo de prevenir cualquier acceso indebido al sistema por parte de un usuario que conozca la clave de otro.
i) Con respecto al formato de las claves de usuario, se establece que estas últimas deben:
   - Combinar letras (Incluir mayúsculas) y números.
   - Tener un tamaño de siete caracteres.
   - Como medida de seguridad se le especificará a cada usuario que su clave no debe de tener ninguna relación directa con ellos, para evitar que cualquier otra persona fácilmente descubra la clave que utilizan para ingresar a la red municipal.
   - Es responsabilidad del Encargado de Redes y Servidores de la Municipalidad de La Florida revisar periódicamente el listado de usuarios activos en la red municipal, además de verificar si el nivel de acceso con que cuentan corresponde a las labores que realizan. También es responsabilidad del Encargado de Redes y Servidores de la Municipalidad de La Florida monitorear las transacciones realizadas por cada uno de los usuarios de la red municipal, esto con el objetivo de llevar un control de los datos y la información manipulada por los usuarios dentro del sistema
j) No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Jefe del Departamento de Informática determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el período de tiempo requerido para efectuar el trabajo.
k) Se prohíbe el uso de cuentas anónimas o de invitado y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.
l) Cuando un funcionario es despedido o renuncia a la Municipalidad de La Florida, debe desactivarse su cuenta antes de que deje el cargo y debe avisarse de dicha situación con la debida anticipación al Departamento de Informática.

X. CONTRASEÑAS Y EL CONTROL DE ACCESO

a) El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
b) Nunca debe compartirse la contraseña o revelarla a otros. Compartir la contraseña expone al usuario a las consecuencias de las acciones que los otros hagan con esa

De todas maneras

contraseña.

c) Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
d) Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
e) Si no ha habido ninguna actividad en una Terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 10 minutos. El restablecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña.
f) Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Municipalidad de La Florida, pudiendo provocar eventuales responsabilidades administrativas, civiles, penales, etc.
g) Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos. Esta acción se llevará a cabo en el Departamento de Informática cuando sea necesario o cuando el Administrador Municipal así lo disponga.
h) Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los puedan leer las personas autorizadas.
i) Los servidores de red y los equipos de comunicación deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de comunicación a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.
j) Se deberá contar con sistema de registro de todo el personal que ingrese a la sala de servidores, tanto para personal en tránsito, como para personal externo.
k) En el registro mencionado en el punto anterior, este deberá considerar:
    - Nombre Completo
    - Rut
    - Hora de entrada
    - Hora de Salida
    - Trabajo a realizar
    - Firma de quien autoriza
    - Firma de solicitante
    - Tipo de usuario (Interno - Externo)

l) Como parte de las buenas practicas, queda prohibido para toda persona que ingrese al data center, utilizar equipos fotográficos, de grabación de audio o video y lo relativo a no comer, beber o fumar.

m) Los accesos deberán ser autorizado por el jefe del departamento de Informática o los administradores de red, previo registro a la solicitud de acceso, el cual debe contener la información requerida en el punto X. letra k.

De todas maneras

2. **APRUÉBASE EL PLAN INFORMÁTICO MUNICIPAL,** que a continuación se indica:

El Plan Informático Municipal, considera las siguientes etapas, con sus respectivas tareas:

- **ETAPA 1**

a) Informe situación tecnológica municipal y necesidades.
b) Manual de Procedimientos sobre copias de respaldo en un sitio distinto al principal, registro de éstas en la sala de servidores, restauración de las mismas, examen y prueba regular de los dispositivos de respaldo, en virtud del Servicio de Virtualización de Servidores Municipales.
c) Informe sobre el registro de los cambios realizados a la configuración de los sistemas; recuperación de la condición inicial en caso de falla o error, evaluación del impacto potencial de los cambios realizados
d) Instructivo de análisis de impacto frente a posibles riesgos externos e internos de los sistemas de información.
e) Elaborar plan de continuidad del negocio y recuperación ante desastres.
f) Definición de procedimientos para la implementación a nivel municipal del SIG como modelo de Gestión Territorial Municipal
g) Informe de equipamiento (hardware y software)
h) Plan de Mantención equipamiento
i) Plan de Respaldo de la información
j) Plan de Renovación Equipamiento
k) Informe preliminar y propuesta del procedimiento para la presentación de proyectos tecnológicos

- **ETAPA 2**

a) Procedimientos del SIG
b) Procedimientos presentación de proyectos tecnológicos
c) Plan de Compras circunscrito al área tecnológica
d) Plan para revisión de procedimientos y validación de cumplimientos de protocolo de seguridad.

Los responsables de dar cumplimiento al Plan Informático Municipal serán el Comité de Gestión de Seguridad de la Información aprobados mediante Decreto Exento N°1612 de fecha 22 de mayo de 2015, representados por el Encargado de Seguridad y el Jefe de Informática.

Los plazos por parte del Comité de Seguridad de la Información para el desarrollo de las etapas, será para la primera etapa durante el año 2016 y para la segunda etapa durante el año 2017.

El cronograma de actividades será formulado por el Comité de Gestión de Seguridad de la Información y una vez sancionado se informará al Administrador Municipal sobre el mismo. El Encargado de Seguridad deberá velar el cumplimiento de lo dispuesto en el cronograma de actividades.

La persona que sienta afectado sus derechos con la dictación del presente decreto podrá interponer el recurso de legalidad para ante el órgano que dictó el acto administrativo que se impugnan dentro del plazo que señala la ley, sin perjuicio de los recursos que le franquea la justicia ordinaria.

De todas maneras

Anótese, comuníquese, transcríbase a Alcaldía, Secretaría Municipal, Dirección de Control, Departamento de Informática, Oficina de Partes, dése copia al interesado y hecho, archívese.

La Oficina de Partes y Reclamos, Sugerencias y Archivo mantendrá un ejemplar del presente acto administrativo a disposición de quien lo solicite.

Firmado por orden del Alcalde: **NICOLAS PIZARRO JULIÁ, ADMINISTRADOR MUNICIPAL; DINA CASTILLO GONZALEZ, SECRETARIA MUNICIPAL**– Hay Timbres respectivos.

Lo que transcribo para su conocimiento y fines que corresponda.

I. MUNICIPALIDAD DE LA FLORIDA
SECRETARIA MUNICIPAL

SECRETARIA MUNICIPAL

NPJ/DCG/MLSR/AOG/OMM/SCS