



CERTIFICACIÓN

El Infrascrito **SECRETARIO MUNICIPAL** de este Término **CERTIFICA** El preámbulo **Punto No. 4.3** y parte Final del **Acta No.026/18.-** De la Sesión Celebrada por La **HONORABLE CORPORACIÓN MUNICIPAL**, y que Literalmente Dice: **ACTA NUMERO VEINTISEIS** En la Ciudad de Lima, Departamento de Cortés a los Trece días del Mes de Julio del Año Dos Mil Dieciocho.- Siendo las: 8:30 AM. en Sesión **ORDINARIA** celebrada por la **HONORABLE CORPORACION MUNICIPAL** en Sala de Regidores presidió EL Señor **JOSE SANTIAGO MOTIÑO LOPEZ** Alcalde Municipal, con La Asistencia de la Señora Vice Alcaldesa **KARLA JANETH ENAMORADO SAGASTUME** presentes los señores Regidores: **ROBERTO RENE AYESTAS AVILA, ASTOR ADOLFO AMAYA FUENTES, JESUS AMADEO HERNANDEZ ROMERO, ANA DEL CARMEN MURILLO MENDOZA, JOSE LEONARDO VIERA ZAVALA, ROSA EVA CASTILLO MADRID, OSWALDO MARTINEZ ALVAREZ** y **HERIBERTO ESPINAL** y el Secretario del Despacho que da fe Señor **ALEX DAGOBERTO CABRERA ALVAREZ** se procedió de la siguiente manera:

PUNTO No. 4.3.- El señor **FRANKLIN BROWN** Encargado de informática, remite a la **HONORABLE CORPORACION MUNICIPAL** notificación haciendo de conocimiento que El Tribunal Superior de Cuentas se encuentra instalado en la Alcaldía Municipal, por lo que le solicitaron el punto de acta del reglamento aprobado para el departamento de informática, en la correspondencia que les fue enviada el 15 de febrero de 2018, donde se les envió copia del "Reglamento Municipal Política de Seguridad Informática" para su conocimiento y aprobación en vista por el tiempo transcurrido y considero que fue leído y estudiado, les solicito la aprobación del mismo para que forme parte de los reglamentos municipales oficiales, el reglamento antes mencionado fue creado para el uso adecuado del equipo de computo y sus políticas de seguridad, por lo cual el reglamento subsana todas las recomendaciones realizadas por el Tribunal Superior de Cuentas en tema de seguridad que se hizo ver en su momento al departamento de informática en su auditoria anterior.-**Notificación que es del conocimiento y Ampliamente Discutido y analizado el presente Reglamento LA HONORABLE CORPORACION MUNICIPAL En uso de las Facultades que La ley le confiere por unanimidad de votos ACUERDA:**

1.- Aprobado el Reglamento Municipal Políticas de Seguridad Informática el cual se Adjunta para que sea implementado en la presente Administración Municipal.-

FIRMA Y SELLO - JOSE SANTIAGO MOTIÑO LOPEZ.- ALCALDE MUNICIPAL.- FIRMA Y SELLO.- ALEX DAGOBERTO CABRERA ALVAREZ.- SECRETARIO MUNICIPAL.-

Se extiende la presente En la Ciudad de La Lima, Departamento de Cortes, a los Treinta y Un días del mes de Julio del año Dos Mil Dieciocho.



Vo.Bo. JOSE SANTIAGO MOTIÑO LOPEZ
ALCALDE MUNICIPAL

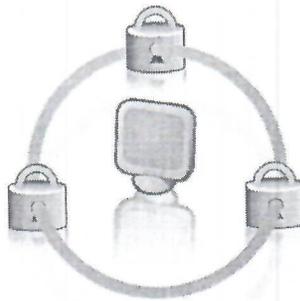


ALEX DAGOBERTO CABRERA ALVAREZ
SECRETARIO MUNICIPAL

MUNICIPALIDAD DE LA LIMA, CORTES



REGLAMENTO MUNICIPAL POLITICAS DE SEGURIDAD INFORMATICA



La Lima, Cortés - 2014



MUNICIPALIDAD DE LA LIMA, CORTES	1
REGLAMENTO MUNICIPAL	1
POLITICAS DE SEGURIDAD INFORMATICA	1
Justificación	5
Introducción	5
Objetivos	5
Sanciones por incumplimiento	5
Beneficios	5
Solicitudes de adquisición de equipo de cómputo	6
Responsabilidades	6
Responsabilidades del Departamento de Informática:	6
El Departamento de Informática consta de tres tipos de mantenimiento:	6
Preventivo	7
Proactivo	7
Correctivo	7
CAPITULO I	8
NORMAS DE SEGURIDAD DEL PERSONAL	8
Artículo 1. POLÍTICAS Y SEGURIDAD DEL PERSONAL.	8
1.1) Usuarios:	8
1.2) Obligaciones de los usuarios:	8
1.3) Acuerdos de uso y confidencialidad:	8
1.4) Capacitación en seguridad informática:	8
1.5) Medidas disciplinarias:	8
CAPITULO 2	9
NORMAS DE SEGURIDAD FISICA Y HARDWARE	9
Artículo 2. POLÍTICAS Y SEGURIDAD FÍSICA Y HARDWARE.	9
2.1) Usuario:	9
2.2) Cuidado y Protección de la información:	9



Franklin

2.3) Control de ingreso físico:	9
2.4) Seguridad en áreas de trabajo:	10
2.5) Reubicación y Protección de los equipos:	10
2.6) Mantenimiento de Equipo de cómputo:	11
2.7) Pérdida o transferencia de equipo:	11
2.8) Uso de Grabadores de DVDs y otros :	11
2.9) Daño al Equipo de Computo:	12
CAPITULO 3	12
NORMAS DE SEGURIDAD Y ADMINISTRACION DE OPERACIONES DE CÓMPUTO	12
Artículo 3. POLÍTICAS SEGURIDAD Y ADMINISTRACION DE CÓMPUTO	12
3.1) Política:	12
3.2) Uso de medios de almacenamiento:	12
3.3) Instalación de Software:	13
3.4) Identificando problemas:	13
3.5) Administración de la Configuración :	14
3.6) Seguridad de la Red:	14
3.7) Uso del correo electrónico:	14
3.8) Prevención Contra Código Malicioso:	15
3.9) Permisos Uso de Internet :	16
NIVELES DE ACCESO	18
NIVEL 1:	18
NIVEL 2:	18
NIVEL 4:	18
CATEGORIZACION DE NIVELES	18
CAPITULO 4	19
NORMAS DE SEGURIDAD Y CONTROL DE USUARIO	19
Artículo 4. POLÍTICAS SEGURIDAD Y CONTROL DE USUARIO	19

4.1) Política:	19
4.2) acceso a Usuario:	19
4.3) Administración de privilegios:	20
4.4) Equipo desatendido:	20
4.5) Administración y uso de contraseñas:	20
4.6) Control de accesos remotos:	21
CAPITULO 5	22
NORMAS DE SEGURIDAD CUMPLIMIENTO DE SEGURIDAD	22
Artículo 5. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA	22
5.1) Derechos de Propiedad Intelectual:	22
5.2) Revisiones del cumplimiento:	22
5.3) Violaciones de seguridad informática:	22



Justificación

El presente documento tiene como finalidad dar a conocer el reglamento municipal de Seguridad de Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la Municipalidad de la Lima, Cortes.

Introducción

La base de un buen plan para cualquier entidad pública que le permita operar de una forma confiable en materia de Seguridad Informática comienza con la definición de las políticas de seguridad.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas de seguridad que cubran las necesidades de la municipalidad de la lima en materia de seguridad.

En este Reglamento se encuentran las cinco políticas generales de seguridad para los empleados o usuarios de la municipalidad se consideran los siguientes puntos:

- Seguridad de Personal
- Seguridad Física y Ambiental
- Administración de Operaciones de Cómputo
- Controles de Acceso de usuarios
- Cumplimiento de la Norma de seguridad

Objetivos

Poder difundir las medidas y las Políticas de Seguridad Informática a todo el personal de la Municipalidad de la Lima Cortes, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados en marcado en la ley.

Sanciones por incumplimiento

El incumplimiento al presente reglamento podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Beneficios

El reglamento municipal de seguridad Informática es la base para la protección de los activos tecnológicos e información de la Municipalidad de la Lima.

Solicitudes de adquisición de equipo de cómputo

Las solicitudes para la adquisición de cualquier equipo de cómputo (impresora, escaner, Monitor, Software y demás recursos informáticos) deben ser enviadas por cada jefe de departamento al departamento de informática para su evaluación. Sera analizadas dependiendo de las necesidades y requerimiento del usuario, así como los procedimientos de compra de dicho bien.

Será responsabilidad del departamento de información proveer las especificaciones técnicas del equipo para la función que desempeña el usuario.

Responsabilidades

El departamento de informática es responsable de seguridad informática de la municipalidad de la lima.

Responsabilidades del Departamento de Informática:

- 1) Elaborar y Actualizar las políticas, normas, pautas y procedimiento relativo a seguridad informática.
- 2) Coordinar el análisis de riesgos, planes de contingencia y prevención de desastres
- 3) Efectuar la evaluación y revisión de la situación de la municipalidad de la lima en cuanto a seguridad informática
- 4) Implementar y velar por el cumplimiento de las políticas ,normas y procedimiento de seguridad de toda la municipalidad
- 5) Evaluar e implementar productos de seguridad informática y realizar las demás actividades necesarias para garantizar un ambiente informático seguro ,eficiente y eficaz
- 6) Proporcionar apoyo técnico relacionado a la seguridad informática, en caso de intrusión , virus, fraudes y acceso no autorizados , ataque de hackers y otros percance.
- 7) Establecer controles de acceso apropiados para cada usuario.

El Departamento de Informática consta de tres tipos de mantenimiento:

CAPITULO I

NORMAS DE SEGURIDAD DEL PERSONAL

Artículo 1. POLÍTICAS Y SEGURIDAD DEL PERSONAL.

1.1) Usuarios:

todo usuario se comprometen a cumplir los principios de confidencialidad de la información cuando esta sea de carácter Reservada y de uso de la Municipalidad de La Lima, así como el estricto apego al reglamento de Políticas Seguridad Informática.

1.2) Obligaciones de los usuarios:

Es responsabilidad de los usuarios cumplir las Políticas de Seguridad Informática del presente manual.

1.3) Acuerdos de uso y confidencialidad:

Todos los usuarios informáticos de la municipalidad de la lima , deberán apegarse a los principios de confidencialidad y el uso adecuado de los recursos informáticos y de información de la Municipalidad de la lima, así como comprometerse a cumplir con lo establecido en el Reglamento de usuario política de seguridad informática.

1.4) Capacitación en seguridad informática:

Todo empleado de la Municipalidad de la lima y entidades Municipales descentralizadas Deberá: Leer el reglamento de Políticas de Seguridad Informática para los Usuarios de la Municipalidad de la lima, y las entidades Municipales descentralizadas el cual se encuentra disponible en digital o impreso para su lectura, donde se dan a conocer las obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento y deberá firma el acuerdo de cumplimiento de las normas vigente.

1.5) Medidas disciplinarias:

En los casos que exista incumplimiento por parte de los usuarios de las normas establecidas en este reglamento estará sujeto a las sanciones correspondiente, misma que serán implementada por la gerencia de personal.

CAPITULO 2

NORMAS DE SEGURIDAD FISICA Y HARDWARE

Artículo 2. POLÍTICAS Y SEGURIDAD FÍSICA Y HARDWARE.

2.1) Usuario:

Está prohibido el ingreso de personas ajenas a las áreas de trabajo e instalaciones y a las áreas restringidas de la Municipalidad de la Lima mismas deberán ser Rotuladas, (sólo personal autorizado) no podrán ingresar a las áreas clasificada como sensible para poder salvaguardar los equipos de cómputo y de comunicaciones, de la Municipalidad de la Lima.

2.2) Cuidado y Protección de la información:

- a) El usuario deberá reportar de forma inmediata al departamento de informática, cuando se detecte o que existan riesgos reales o potenciales para el equipos de cómputo, como pueda ser fugas de agua, conatos de incendio u otros.
- b) El usuario tiene la obligación de proteger los CD-ROM, DVD, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su cuidado, aun cuando no se utilice y contengan información reservada o confidencial.
- c) Es responsabilidad del usuario evitar en todo momento fuga de la información de la municipalidad de la lima que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.
- d) Es responsabilidad del departamento de Bienes Municipales registrar las asignación oficial de los equipos de informática y se enviara copia al departamento de informática

2.3) Control de ingreso físico:

- a) Cualquier persona que tenga acceso a las instalaciones de la municipalidad de La Lima, deberá registrarse con el personal de seguridad (cuando este traiga equipo y herramienta de cómputo), y si permanece un día podrán retirar en el mismo momento, sin necesidad de trámite alguno.



b) En caso de que el equipo no sea propiedad de la Municipalidad de la Lima, y permanezca dentro de la institución más de un día hábil, es necesario que el responsable de la organización en la que trabaja o propietario del equipo, elabore y firme un oficio de autorización de entrada y salida.

2.4) Seguridad en áreas de trabajo:

Los Data Center (Centro de Computo) de la municipalidad de la Lima son áreas restringidas, por lo que sólo el personal autorizado por el departamento de informática, podrá ingresar en ellas, para las estaciones de trabajo solo los empleados municipales tendrá acceso a la mismas no podrá prestar el equipo a personas ajenas de la municipalidad.

2.5) Reubicación y Protección de los equipos:

a) Los usuarios no deben mover o reubicar los equipos de cómputo o instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del departamento de informática, debiéndose solicitar a la misma en caso de requerir este servicio.

b) El área del departamento de informática será la encargada de llevar un control de usuario responsable de los activos físicos que se le asignen y de conservarlos en la ubicación autorizada por el departamento de informática.

c) El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario de la Municipalidad de la Lima.

d) Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por el mal uso y poder aprovechar al máximo las mismas.

e) Es responsabilidad de los usuarios almacenar su información únicamente en la unidad de red que se le asigne, ya que las otras unidades están destinadas para archivos de programas y sistemas operativo, solo se almacenara información municipal, no podrá guardar música, videos, juegos en la unidad de red asignada.

f) Cuando se esté trabajando con el equipo de cómputo, no se deberá consumir alimentos o ingerir líquidos, en el área de trabajo.

g) Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

h) Se debe mantener el equipo de cómputo en un entorno limpio y sin humedad el usuario deberá limpiar la parte física del CPU.

i) El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

Preventivo

El departamento de informática dispone de un cronograma de mantenimiento preventivo para anticiparse a problemas o situaciones riesgosas que perjudiquen el buen funcionamiento de los servicios existentes.

Proactivo

En caso de Fallas permanentes de un equipo o sistema computacional, el departamento de informática encontrara la causa de la falla y procederá a su eliminación mediante la implementación o incorporación de nuevas tecnologías.

Correctivo

El departamento de informática dispondrá de personal calificado para solucionar y corregir problemas computacionales que presente el usuario.

j) Cuando se requiera mover varios equipos de cómputo de lugar, éstos deberán ser notificados con una semana de anticipación al departamento de informática a través de una notificación firmada por encargado de bienes municipales y el Jefe del departamento del área que corresponda.

k) Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo solamente el departamento de informática está autorizado a tal efecto.

2.6) Mantenimiento de Equipo de cómputo:

a) Solamente el personal autorizado por el departamento de informática podrá llevar a cabo las reparaciones del equipo de cómputo, por lo cual los usuarios no deberán de permitir que personas ajenas no podrá tocar, reparar, diagnosticar el equipo de cómputo al no aceptar esta disposición se estará violentando en el reglamento de seguridad dando lugar a la sustracción de información sin autorización.

b) Los usuarios deberán asegurarse de respaldar la información que considere de suma importancia previendo así la pérdida involuntaria de información, cuando el equipo estuviera en reparación podrá solicitar asistencia para asegurar el correcto respaldo al departamento de informática.

2.7) Pérdida o transferencia de equipo:

a) El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable del uso y custodia del mismo; en consecuencia, responderá por el en casos de robo, extravío o pérdida del mismo.

El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

b) El usuario deberá dar aviso de inmediato al departamento de informática del hurto o la desaparición, del equipo de cómputo o accesorios bajo su resguardo deberá presentar un nota de las autoridades competentes de la DGIC que deberá adjuntar a la notificación del caso a la Gerencia Municipal y a Bienes Municipales.

2.8) Uso de Grabadores de DVDs y otros :

a) El uso de los grabadores de discos compactos es exclusivo para hacer respaldos de información por su cantidad de volumen de datos.

c) La asignación de esta quemadora será previa justificación por escrito y autorizado por el jefe inmediato correspondiente.

d) El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

c) Los módems internos o externos esta prohibidos para el uso en cualquier equipo de cómputo, excepto cuando lo autorice el departamento de informática.



Franklin Brown

2.9) Daño al Equipo de Computo:

a) El equipo de cómputo o cualquier recurso asignado que sufra algún daño por maltrato, descuido o negligencia por parte del usuario, el responsable deberá cubrir el valor de la Pieza o reposición del equipo o accesorios afectados. Para tal caso se determinará la causa de dicho daño.

b) No será responsabilidad del usuario si el equipo por daños eléctricos o por rayos se dañara, o por su vida útil en componentes.

CAPITULO 3

NORMAS DE SEGURIDAD Y ADMINISTRACION DE OPERACIONES DE CÓMPUTO

Artículo 3. POLÍTICAS SEGURIDAD Y ADMINISTRACION DE CÓMPUTO

3.1) Política:

a) Los usuarios deberán utilizar métodos adecuados para proteger la información que se mantiene y se utiliza en las instalaciones de la municipalidad de la lima. de tal forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la municipalidad de la lima o hacia redes externas como internet.

b) Los usuarios de la municipalidad de la lima que hagan uso de equipo de cómputo, deberán tener cuidado para prevenir código malicioso conocido como virus, malware o spyware. Puede pedir asesoría al departamento de informática.

3.2) Uso de medios de almacenamiento:

a) Deberá hacer una solicitud por escrito para poder utilizar una carpeta compartida, para que el departamento de informática la analice y la apruebe. La contravención de esta norma se considerara una falta grave.

b) Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, dicho documento se presentará con sello y firma del Jefe del departamento o de unidad.

c) Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, en la unidad de red asignada. Puede pedir asesoría al departamento de informática.

d) En caso de que el volumen de información sea demasiado grande y se requiera algún respaldo en CD, DVD, deberá acudir al departamento de informática.

c) Los empleados de La municipalidad de la lima deben conservar los registros de los contribuyentes o información valiosa que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita el departamento de Acceso a la Información Pública de la Municipalidad de la lima, en los términos de Ley de Acceso a la Información.

d) Las actividades que realicen los usuarios de la municipalidad de la lima en la infraestructura tecnológica de la municipalidad de la lima son registradas y susceptibles de auditoría.

3.3) Instalación de Software:

a) Los usuarios que requieran la instalación de algún software que no sea propiedad de la municipalidad de la lima, deberán justificar su uso y solicitar su autorización al departamento de informática, a través de un oficio firmado por el jefe del departamento, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software o si fuera el caso que es software gratuito indicar la fuente o Empresa que lo distribuye para hacer la investigación.

b) Si el dueño del software no presenta la factura de compra del mismo, el departamento de informática procederá de manera inmediata a desinstalar dicho software.

c) Se considera una falta grave a los usuarios que instalen cualquier tipo de programa (software) en sus computadoras estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Municipalidad de la lima, que no esté autorizado por el departamento de informática.

d) Todo equipo de cómputo será entregado con el software básico y respectiva licencia de uso

3.4) Identificando problemas:

a) El usuario que sospeche o tenga conocimiento de la ocurrencia de un problema de seguridad informática deberá reportarlo al departamento de informática, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

b) Cuando tenga conocimiento o sospecha de que la información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las áreas administrativas, el usuario deberá notificar al departamento de informática con copia al departamento de Recurso Humano sobre lo sucedido.

c) Cualquier problema generado durante la utilización u operación de los procesos de los usos del sistema de información de la municipalidad de la lima, debe ser reportado al departamento de informática por escrito de acuerdo al formato que el departamento de informática.

d) Cuando se requiera de un módulo o algún cambio en general deberán reportarlo por escrito al Departamento de Informática

3.5) Administración de la Configuración :

Los usuarios de los diferente departamentos de la municipalidad de la lima no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la municipalidad de la lima , sin la autorización por escrito del departamento de informática.

3.6) Seguridad de la Red:

a) Será considerada como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el departamento de informática en la cual, los usuarios realicen la exploración de los recursos informáticos en la red de la municipalidad de la lima, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad como ser sniffer, envenenamiento de arp ,ingeniería inversa.

b) Queda totalmente prohibido el uso de internet de otra empresa que no sea la que está actualmente vigente ya que violenta en el reglamento de política de seguridad.

c) Se considera Falta grave si se conecta una computadora o portátil a la estructura de la red y querer tratar de averiguar las configuración de la misma, es considerado una violación al reglamento la seguridad por lo cual será remitido al departamento de recurso humano.

3.7) Uso del correo electrónico:

a) Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros salvo con la autorización del departamento de informática.



Franklin B

b) Los usuarios deben tratar los mensajes de correo electrónico no personales y archivos adjuntos como información que es propiedad de la municipalidad de la lima.

c) Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó el departamento de informática.

d) La municipalidad de la lima, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática de la municipalidad de la lima o realizado acciones no autorizadas.

e) Como el correo electrónico institucional de la municipalidad de la lima es privado, la única forma en la que puede ser revelada es mediante una orden judicial.

f) El usuario debe de utilizar el correo electrónico de la municipalidad de la lima única y exclusivamente para los recursos que tenga asignado, quedando prohibido cualquier otro uso distinto.

h) La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito al departamento de informática, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área que corresponda. Una vez creado y asignado las cuentas oficiales.

i) Queda prohibido engañar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico el robo de identidad es penado por la ley.

j) Todo usuario es responsable por los datos/documentos adjunto que envíe.

k) Cada usuario es responsable de las acciones efectuadas desde su cuenta de correo , la Municipalidad de la lima no hace responsable de las opiniones emitidas

3.8) Prevención Contra Código Malicioso:

a) Para prevenir infecciones por virus informáticos, los usuarios de la municipalidad de la lima, no debe hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el departamento de informática.

b) Los empleados de la municipalidad de la lima, deberán verificar que la información de las, memorias USB, discos flexibles, CD's, estén libres de cualquier tipo de código malicioso, por lo cual deberán ejecutar el software antivirus, autorizado por el departamento de informática para su escaneo e eliminación.

c) Ningún empleado de la municipalidad de la lima deberá escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento del computadora, archivos de sistema o software. ni probarlos en cualquiera de los ambientes o



Franklin Brown

plataformas de la municipalidad de la lima. El incumplimiento de este será considerado una falta grave.

d) Ningún empleado de la municipalidad de la lima o personal externo podrá bajar o descargar software varios, mensajería instantánea, sin la debida autorización del departamento de informática.

e) Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo e informar al departamento de informática para la detección y eliminación del virus.

f) Cada usuario que tenga bajo su cuidado algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica al departamento de informática las actualizaciones del software de antivirus.

g) Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el departamento de informática en programas tales como:

- Antivirus;
- Correo electrónico;
- Paquetes Office;
- Navegadores;
- Otros programas
- Software Municipal (SAFT) ,Aguas de la lima (Simafi)

Nota: Debido a que algunos virus son difíciles de eliminar ningún usuario de la municipalidad de la lima debe intentar eliminarlo, corre el riesgo de eliminar archivos importantes y dejar inutilizado el sistema operativo o pérdida importante de la información, lo indicado será llamar al departamento de informática para solucionarlo.

3.9) Permisos Uso de Internet :

a) El departamento de informática tiene la autoridad para controlar y negar el acceso a cualquiera que viole las políticas o interfiere con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.

b) El acceso a internet provisto a los usuarios de la municipalidad de la lima es exclusivamente para las actividades relacionadas con las necesidades del puesto y su función.

c) El uso de internet es personal e intransferible no permitiéndose que terceras personas hagan uso del servicio.

d) El Departamento de informática llevara un control de los usuarios que tenga el servicio de internet.

- e) El usuario no debe utilizar ninguna conexión privada a través de las estaciones de trabajo.
- f) Para las organizaciones que visitan la municipalidad o entidad sin fines de lucro se les autoriza solamente el periodo de tiempo que estará en la instalaciones, si sobrepasa lo autorizado deberá de llenar una solicitud en la cual indicara el motivo de la ampliación y la magnitud del tiempo para no violentar el reglamento de seguridad.
- g) Se prohíbe acceder a lugares obscenos, que distribuyan material pornográfico, o bien materiales ofensivos en perjuicio de terceros.
- h) La navegación en internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la institución.
- i) Está prohibido bajar aceleradores, o instalara programas que violen derecho de autor.
- j) Está prohibido ver o reproducir bajar archivos de música en línea o video desde internet o cualquier otro medio.
- k) Se prohíbe utilizar los servicios de red para juegos (en línea) a través del servicio de internet o intranet
- l) Se prohíben los juegos basados en sistema web.
- ll) Todo usuario que acceda a otra red por medio de la red de la institución debe acatar las reglas (Sami ,Sinap,Sinit,Renot,Sure).
- m) Cada usuario es el responsable de las acciones efectuadas a través de internet. Es política de la Municipalidad de la lima no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones pueden ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad y auditoria.
- n) Están prohibido el uso de redes sociales en horas laborales.
- ñ) Solamente las Redes Sociales Oficiales de la Municipalidad de la lima se podrán ingresar para su actualización.
- o) Se considera que las redes sociales creadas a nombre de la municipalidad de la lima son propiedad de ellas.
- p) Ninguna persona tendrá derecho a ella cuando se requiera usuario y clave se deberá proporcionar.
- q) El acceso y uso de módem ya se de cualquier empresa en la municipalidad de la lima tiene ser previamente autorizado por el departamento de informática ya que se considera como una Falta grave.

NIVELES DE ACCESO

Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

NIVEL 1:

Sin restricciones: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de Información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea, redes sociales. A excepción de contenido ofensivo o peligroso.

NIVEL 2:

Internet restringido y mensajería instantánea: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose el reglamento de seguridad en el uso de internet. A excepción de contenido ofensivo o peligroso.

NIVEL 3: Internet restringido, redes sociales: Los usuarios sólo podrán hacer uso de internet aplicándose el reglamento de seguridad en el uso de internet.

NIVEL 4:

El usuario no tendrá acceso a Internet ni a servicios de mensajería instantánea.

CATEGORIZACION DE NIVELES

Se describe a continuación quien será asignado a los niveles antes mencionados:

Nivel 1: Alcalde ,Vicealcalde ,Corporación Municipal, Gerentes Generales

Nivel 2: Jefes de Departamentos y sub gerente

Nivel 3: Empleados cuya funciones necesitan el uso internet (Secretaria ,Asistente) de gerencia y alcaldía

Nivel 4: Empleados que no están autorizados a utilizar ningún servicio de internet

CAPITULO 4

NORMAS DE SEGURIDAD Y CONTROL DE USUARIO

Artículo 4. POLÍTICAS SEGURIDAD Y CONTROL DE USUARIO

4.1) Política:

- a) Cada usuario es responsable del uso de acceso que se le a proporcionado; aceptando la responsabilidad del uso del nombre de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de la municipalidad de la lima, por lo cual deberá mantenerlo de forma confidencial.
- b) El departamento de informática, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica de la municipalidad de la lima, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones.

4.2) acceso a Usuario:

- a) El acceso a la infraestructura de red de la municipalidad de la lima para personal externo debe ser autorizado por el jefe de departamento, quien deberá notificarlo por oficio al departamento de informática, quien lo habilitará.
- b) Está prohibido que los usuarios utilicen la infraestructura de red de la Municipalidad de la Lima para obtener acceso no autorizado a la información u otros sistemas de información de la municipalidad de la lima.
- c) Todos los empleado que utilizan el sistema saft y validación en el servidor son responsables por su nombre de usuario y su contraseña asignada para al acceso de los recursos.
- d) Todos los usuarios deberán validarse por el departamento de informática para tener acceso provisto antes de poder usar la infraestructura tecnológica de la municipalidad de la lima.
- e) Los usuarios no deben proporcionar información a personal ajeno, de los proceso de acceso a los sistema e infraestructura de red de la municipalidad de la lima, excepto que se esté realizado una auditoria y y que se requiera conocer algunos proceso de cómo funciona los sistema, solamente podrá mostrar los procesos no deberá dar información de usuario y contraseña, ya que violenta el reglamento de seguridad.

f) Cualquier usuario que accede a la infraestructura de red de la municipalidad de la lima debe contar con un nombre de usuario único y personalizado, por lo cual no está permitido el uso de un mismo nombre de usuario por varios empleado.

g) Los usuarios tienen prohibido compartir su usuario y su contraseña, ya que todo lo que ocurra con ese usuario y contraseña será responsabilidad exclusiva al que pertenezcan, Existe en el módulo de seguridad de bitácora que registra todos los procesos que se hagan en el sistema Saft y en la estructura de la red.

4.3) Administración de privilegios:

a) Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura de la red de la municipalidad de la lima, deberán ser notificados por escrito al departamento de informática para realizar los ajuste adecuado.

b) Solamente el departamento de informática está facultado de otorga los privilegios del usuario.

c) El Departamento de informática designara al Jefe de departamento con derecho administrativo en el módulo que este asignado para poder hacer correcciones, cuando se requiera, ya sea un error en el módulo asignado.

d) Queda a decisión del Jefe de Departamento asignar a un empleado a llevar las funciones administrativa en el módulo que se esté asignado a dicha jefatura.

e) Cualquier error o mal uso de la cuenta administrativa designado por el jefe de departamento al empleado correrá con la misma suerte si se encontrara un mal uso de la misma dándole lugar a una falta grave de seguridad sobre la manipulación inadecuada del software.

4.4) Equipo desatendido:

a) Los usuarios deberán mantener sus equipos de cómputo con contraseñas y en los protectores de pantalla (previamente instalados y autorizados por el departamento de informática, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo determinado.

b) Todo usuario cuando deje su estación de trabajo deberá de bloquear su equipo y/o abocarse con el departamento de informática para el uso correcto del bloqueo.

4.5) Administración y uso de contraseñas:

La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

a) Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito al departamento de informática, indicando si es de acceso a la red o a módulos de sistemas desarrollados por el departamento de informática, para que se le proporcione una nueva contraseña.

b) La obtención de un usuario y contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante al departamento de informática como empleado de la municipalidad de la lima y su respectiva nota del jefe de departamento.

c) Está prohibido que los nombres de usuarios y contraseñas se encuentren de forma visible en cualquier forma impresa o escrita en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

d) Todos los usuarios deberán considerar los siguientes parámetros para la construcción de sus contraseñas:

e) No deben contener números consecutivos.

f) Deberán estar compuestos de al menos ocho (8) caracteres y máximo once (11). Estos caracteres deben ser alfanuméricos, o sea, números y letras.

g) Deberán ser difíciles de adivinar, no se deberán usar que se relacionen con el trabajo o la vida personal del usuario.

h) Deben ser diferentes a las contraseñas que se hayan usado previamente.

i) La contraseña podrá ser cambiada por requerimiento del usuario de la cuenta.

j) Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de reportarla al departamento de informática por escrito. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

k) Los cambios o desbloqueo de contraseñas solicitados por el usuario al departamento de informática serán solicitados mediante nota oficial sellado y firmado por el jefe inmediato del usuario que lo requiere.

l) Todo usuario que no informe sobre su contraseña que ha sido comprometida da lugar a una falta grave.

4.6) Control de accesos remotos:

a) Está prohibido el acceso a redes externas por vía de cualquier Dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno del departamento de informática.

b) a administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y control de acceso seguro autorizado por el Departamento de Informática.

CAPITULO 5

NORMAS DE SEGURIDAD CUMPLIMIENTO DE SEGURIDAD

Artículo 5. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

5.1) Derechos de Propiedad Intelectual:

- a) Está prohibido por las leyes de derechos de autor y por la Municipalidad de la lima, realizar copia no autorizadas de software, ya sea adquirido o desarrollado por la municipalidad de la lima.
- b) Los sistemas desarrollados por personal, interno o externo, que sea parte del departamento de informática, o sea coordinado por ésta, son propiedad intelectual de la municipalidad de la lima.
- c) En el caso de las instituciones que donen el software son ellos dueños del código fuente queda a la disposición de ellos si entregan el código fuente de dicho sistema.

5.2) Revisiones del cumplimiento:

- a) El departamento de informática realizará acciones de verificación de manera sistemática para el cumplimiento del reglamento de Políticas de Seguridad Informática para los usuarios.
- b) El departamento de informática podrá implementar formas de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar las actividades de procesos que se ejecuta en la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en el reglamento Política de Seguridad Informática.

5.3) Violaciones de seguridad informática:

- a) Está prohibido el uso de cual herramientas de hardware o software para poder violar los controles de seguridad informática. A menos que se autorice por el departamento de informática para poder detectar fallas en seguridad.



Franklin Brown

- b) Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información.
- c) Ninguna persona puede probar o intentar comprometer los controles internos a menos que cuente con la aprobación del departamento de informática, con excepción del Tribunal Superior de Cuentas.
- d) Ningún usuario de la municipalidad de la lima debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas.
- e) No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para autoreplicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información de la Municipalidad de La Lima.

Franklin Brown



La Lima, Cortés. a los veintitrés (23) días del mes de enero de dos mil catorce (2014).



ACUERDO Y COMPROMISO DEL USO DE CONTRASEÑA

DEL SISTEMA SAFT (SISTEMA ADMINISTRATIVO FINANCIERO TRIBUTARIO)

SIMAFI (SISTEMA INTEGRADO MUNICIPAL DE ADMINISTRACION)



Yo, _____, con número de identidad _____, Como parte de mis funciones en el Registro de datos, acepto el uso de CLAVES a fin de realizar mis labores y comprendo que la responsabilidad en el uso y custodia individual de cada clave, es de cada usuario al cual se le brinda acceso a los módulos municipales que se han asignado.

Manifiesto que las contraseñas que me han asignado, serán utilizadas solo para los propósitos de mis funciones, en el Sistema administrativo financiero Tributario (SAFT), Sistema Integrado Municipal de Administración (SIMAFI), como pueden ser las contraseñas de cuentas de usuario del sistema operativo, contraseñas del sistema SAFT, SIMAFI, Cuentas de correo electrónico, servicios web, etc.

Acepto que todas las contraseñas de cuentas que den acceso a recursos y servicios informáticos en el Sistema administrativo financiero Tributario (SAFT), Sistema Integrado Municipal de Administración (SIMAFI) seguirán las directrices generales señaladas por el departamento de Informática.

En caso de haber cedido o comprometido mi clave de acceso a los sistemas, me responsabilizo en comunicar por escrito el hecho al Departamento de informática, a fin de que se tomen los correctivos necesarios.

Me comprometo a no compartir mis claves de acceso y los recursos institucionales y administrar mi clave asignada, con el máximo cuidado y como información sensible y confidencial.

Dejo constancia por escrito a través de este documento, de mi aceptación a los términos y

Acepto haber leído y comprendido el alcance del documento denominado "REGLAMENTO MUNICIPAL POLITICAS DE SEGURIDAD INFORMATICA" y me comprometo a su estricto cumplimiento.

Usuario Final



Francisco Brown

Dpto. Informática