MUNICIPALIDAD PROVINCIAL DE AREQUIPA

RESOLUCIÓN GERENCIAL

N°49 -2011-MPA/GM

Arequipa, 02 de febrero, 2011

VISTO: El Expediente Administrativo Nº 2752-2011 a través del cual la Sub Gerencia de Informática con proveído Nº 06 solicita la modificación de la resolución Gerencial Nº 03 -2011-MPA/GM, a fin de que se rectifique de la parte resolutiva en cuanto a la denominación de la directiva Nº 020-2010-MPA/GPPR/SGR, y;

CONSIDERANDO:

Que, la Municipalidad Provincial de Arequipa, de acuerdo al artículo 194 de la Constitución Política del Estado concordante con el artículo I y II del Título Preliminar de la Ley Orgánica de Municipalidades, Ley N° 27972, es una entidad de Derecho Público con autonomía política, económica y administrativa en asuntos de su competencia;

Que, de conformidad con el Art. IV del Título Preliminar de la Ley Nº 27972, los Gobiernos Locales representan al vecindario, y como tal promueven la adecuada prestación de los servicios públicos locales y el desarrollo integral, sostenible y armónico de su jurisdicción, en concordancia con lo previsto en el Art. 195 de la Constitución Política del Estado;

Que, el artículo 27 de la Ley Orgánica de Municipalidades, dispone que la Administración está Bajo la dirección y responsabilidad del Gerente Municipal, cuyas funciones específicas se encuentran debidamente establecidas en el manual de Organización y Funciones de la Municipalidad;

Que, con fecha 10 de enero del 2011, la Administración Municipal expidió la Resolución Gerencial Nº03-2011-MPA-GM, el cual resuelve aprobar la directiva denominada "Normas y Proyectos de Seguridad de la Información de los Medios Informáticos en la Municipalidad Provincial de Arequipa" remitida por la sub Gerencia de Informática , configurándose un error en su redacción , debiendo decir: NORMAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION DE LOS MEDIOS INFORMATICOS EN LA MUNICIPALIDAD PROVINCIAL DE AREQUIPA" , observándose claramente un error de carácter material de naturaleza subsanable, la misma que debe corregirse a fin de que no exista problemas en su identificación y ejecución;

Que, el artículo 201° de la Ley 27444 Ley del Procedimiento Administrativo General, establece que el error material o aritmético en los Actos Administrativos pueden ser rectificados con efecto retroactivo, en cualquier momento de Oficio o Instancia de los Administrados, siempre que no se altere lo sustancial de su contenido ni el sentido de la decisión;

Que, existiendo un error material y de acuerdo a lo dispuesto por el dispositivo citado debe procederse a la rectificación de la resolución expedida;

Que, la Gerencia General Municipal, de conformidad a las facultades otorgadas en la resolución de Alcaldía Nro.210-2007-MPA, de fecha 18 de mayo del 2007;

RESUELVE:

ARTICULO PRIMERO.- RECTIFICAR la parte resolutiva de la Resolución Gerencial Nº03-2011-MPA-GM, específicamente en su Artículo 1º que aprueba la Directiva 020-2010-MPA/GPPR/SGR, la misma que quedara redactada de la siguiente manera:

ARTICULO PRIMERO.- APROBAR *la directiva* 020-2010-MPA/GPPR/SGR *denominada* **"NORMAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACION DE LOS MEDIOS INFORMATICOS EN LA MUNICIPALIDAD PROVINCIAL DE AREQUIPA"**, remitida por la Sub Gerencia de Informática.

ARTICULO SEGUNDO.- RATIFICAR los demás extremos de la Resolución Gerencial Nº03-2011-MPA-GM, en virtud a las consideraciones expuestas.

Regístrese, comuníquese y cúmplase.

GA. Financiera.
GPP. Racionalización.
SG. Contabilidad.
SGR. Humanos.

MUNICIPALIDAD PROVINCIAL DE AREQUIPA
CPCC. Luis Rodríguez Pauca
Gerente Municipal

RECIBIDO
Siglas:
Fecha: 07 FEB 2011
Hora: 14:30 Horas
Reg. Nº: 041

MUNICIPALIDAD PROVINCIAL DE AREQUIPA
03 FEB. 2011
TRAMITE DOCUMENTARIO Y ARCHIVO

MUNICIPALIDAD PROVINCIAL DE AREQUIPA

RESOLUCIÓN GERENCIAL
N° 03 - 2011-MPA/GM

Arequipa, 10 de enero, 2011.

VISTO: El Informe N°1378-2010-MPA/GPPR de la Gerencia de Planificación Presupuesto y Racionalización, a través del cual remite el proyecto de directiva N°020-2010- MPA/GPPR/SGR denominado "**Normas y Procedimientos de Seguridad de la Información de los Medios Informáticos en la Municipalidad Provincial de Arequipa"** ,para su aprobación y;

CONSIDERANDO:

Que, la Municipalidad Provincial de Arequipa, de acuerdo al artículo 194 de la Constitución Política del Estado concordante con el artículo I y II del Título Preliminar de la Ley Orgánica de Municipalidades, Ley N° 27972, es una entidad de Derecho Publico con autonomía política, económica y administrativa en asuntos de su competencia;

Que, de conformidad con el Art. IV del Título Preliminar de la Ley Nº 27972, los Gobiernos Locales representan al vecindario, y como tal promueven la adecuada prestación de los servicios públicos locales y el desarrollo integral, sostenible y armónico de su jurisdicción, en concordancia con lo previsto en el Art. 195 de la Constitución Política del Estado;

Que el articulo 27º de la Ley Orgánica de Municipalidades, dispone que la Administración esta Bajo la dirección y responsabilidad del Gerente Municipal, cuyas funciones especificas se encuentran debidamente establecidas en el Manual de Organización y Funciones de la Municipalidad;

Que, las autoridades administrativas deben actuar con respeto a la Constitución, la Ley y el Derecho, dentro de las facultades que le estén atribuidas y de acuerdo a los fines para los que fueron conferidas, así como también deberán dirigir e impulsar de oficio el Procedimiento y ordenar la realización o practica de los Actos que resulten convenientes para el esclarecimiento y resolución de las cuestiones necesarias, ello en virtud de los Principios de Legalidad e Impulso de Oficio establecidos en el Artículo IV de la Ley del Procedimiento Administrativo General, Ley 27444;

Que, la Gerencia Municipal, de conformidad con los informes técnicos de los vistos y las facultades otorgadas en la resolución de Alcaldía Nro.210-2007-MPA, de fecha 18 de mayo del 2007;

RESUELVE:

ARTICULO PRIMERO.- APROBAR la Directiva Nº020-2010 MPA/GPPR/SGR, denominada "**Normas y Procedimientos de Seguridad de la Información de los Medios Informáticos en la Municipalidad Provincial de Arequipa"** ,remitida por la Sub Gerencia de Informática;

ARTICULO SEGUNDO.- ENCARGAR a la Sub Gerencia de Informática, hacer los requerimientos necesarios mediante la Sub Gerencia de Logística para su atención, de acuerdo al proyecto aprobad;

ARTICULO TERCERO.- ENCARGAR.- a la Gerencia de Administración Financiera en coordinación con la Sub Gerencia de Informática y la Sub Gerencia de Logística, realizar las acciones Administrativas complementarias conducentes al cumplimiento de la presente resolución;

ARTICULO CUARTO.- NOTIFICAR la presente Resolución Gerencial al interesado.

Regístrese, comuníquese y cúmplase.

GA. Financiera.
GA Tributaria
SG Logística
SG. Contabilidad.
SG Informática
SG Racionalización

Econ. FELIPE POCCO HUAMAN
Gerente
V°B°
Gerencia de Planificación, Presupuesto y Racionalización

GERENCIA DE RACIONALIZACIÓN
RECIBIDO
17 ENE. 2011
Firma:
Siglas:
Fecha:
Hora:
Reg. N°: 11:30 Hrs
Folios:
014
MUNICIPALIDAD PROVINCIAL DE AREQUIPA

MUNICIPALIDAD PROVINCIAL DE AREQUIPA

CPCc. Luis Rodríguez Pauca
Gerente Municipal

MUNICIPALIDAD PROVINCIAL DE AREQUIPA
13 ENE. 2011
TRÁMITE DOCUMENTARIO

MUNICIPALIDAD PROVINCIAL DE AREQUIPA

DIRECTIVA Nº 020-2010-MPA/GPPR/SGR

"Normas y Procedimientos de Seguridad de la Información de los medios Informáticos en la Municipalidad Provincial de Arequipa"

Elaborado por: Sub Gerencia de Informática

01. OBJETIVO

Garantizar la protección y seguridad de la información en los medios informáticos, asegurando su confidencialidad, integridad, disponibilidad y confiabilidad en la Municipalidad Provincial de Arequipa (en adelante Municipalidad).

02. FINALIDAD

Establecer obligaciones y responsabilidades respecto de la seguridad de la información en los medios informáticos de la Municipalidad.

03. BASE LEGAL

a) Ley Nº 27972, Ley Orgánica de Municipalidades;

b) Ley Nº 27444, Ley del Procedimiento Administrativo General;

c) Ley Nº 27309, Ley que incorpora los delitos informáticos al Código Penal;

d) Resolución de Contraloría Nº 072-98-CG;

e) Resolución Ministerial Nº 246-2004-PCM., que aprueba el uso obligatorio de la NTP-ISO/IEC-17799:2007 de Tecnología de la Información. Código de buenas prácticas para la gestión de la Seguridad de la Información;

f) Lineamientos de Política Nacional de Seguridad de la Información en el Estado Peruano.

04. ALCANCE

Las disposiciones de la presente Directiva son de cumplimiento obligatorio por todas las Gerencias y Sub Gerencias, así como de todo el personal que labore en la Municipalidad.

05. NORMAS GENERALES

5.1 Las normas y procedimientos de seguridad de la información en los medios informáticos valoran los riesgos, priorizan el valor de la información y estandarizan los controles y revisiones de los sistemas de información.

5.2 Establecer las bases referenciales para el desarrollo de estrategias y planes referidos a la seguridad de la información.

5.3 Brindar un entorno de trabajo seguro a los servidores de la Municipalidad, los mismos que deberán cumplir con las disposiciones contenidas en la presente directiva.

06. NORMAS ESPECÍFICAS

A) Administración de Usuarios

6.1 La Sub Gerencia de Informática es la encargada de administrar los usuarios y además deberá asegurar que la información existente en los medios informáticos de la Municipalidad no sea modificada, variada o manipulada por terceros para cuyo efecto deberán de cumplir con proporcionar al servidor usuario la siguiente información:

a) El usuario será determinado por la inicial de su primer nombre, seguido de su apellido, en caso de que exista coincidencia de usuario, al segundo en crear se le adicionará la inicial de su segundo apellido, de persistir la similitud se deberá insertar antes del primer apellido la inicial de su segundo nombre y en último de los casos, el que mejor determine el administrador del sistema o red o quien haga sus veces en la Sub Gerencia de Informática.

b) Los usuarios estarán debidamente autorizados e identificados a través de un password, clave o contraseña. Está prohibido el uso de usuarios genéricos, anónimos u otros que no hayan sido otorgados por la Sub Gerencia de Informática.

c) Para la asignación del password, clave o contraseña, los mismos deberán cumplir con los siguientes requisitos:

c.1) Su longitud debe ser como mínimo de cinco (05) caracteres;
c.2) Debe contener al menos un número y una letra;
c.3) No debe ser igual al nombre de otro usuario;
c.4) Debe permitir la utilización de caracteres especiales;
c.5) Se deberá bloquear al usuario en caso de que se den tres (03) intentos errados de autenticación, debiendo registrar dichos eventos (errores y bloqueos);
c.6) Permitir al usuario cambiar su password periódicamente e implementar su cambio como máximo cada ciento ochenta (180) días, al respecto se deberá hacer excepciones con los usuarios administradores del sistema y/o red;
c.7) No deben ser mostrados ni impresos en el momento en que son solicitados, bajo responsabilidad de los usuarios.

d) Los recursos de las estaciones de trabajo, deben protegerse con password, clave o contraseña, de manera que su uso sea personal e indelegable, si el uso se da en duplicado, será de responsabilidad del servidor o de quien esté a cargo del password y del equipo informático.

6.2 El usuario es responsable de las acciones que se realicen con su identificación personal; por tanto el password, clave o contraseña, debe cumplir con las siguientes características:

a) Confidencial; solo es para el manejo y uso exclusivo del usuario;

b) Personal; Está bajo la responsabilidad de una persona;

c) No trivial; Es complejo y difícil de adivinar por terceros.

6.3 Todo usuario en coordinación con su Jefe Inmediato y la Sub Gerencia de Informática, tienen la responsabilidad de cambiar periódicamente su password, clave o contraseña, debiendo memorizarlo y no guardarlo escrito, menos en un archivo de computadora, por ser susceptible de ser leído y usado por otra persona en caso de que existan razones sustentatorias de que su password, clave o contraseña ha sido comprometida, deberá promover su cambio inmediatamente.

6.4 Se califica como falta grave sujeta a sanción según el régimen laboral del servidor, las siguientes:

a) Difundir su password, clave o contraseña a otra persona sin autorización del

inmediato superior ni de la Sub Gerencia de Informática;

b) Copiar y hacer uso del password, clave o contraseña de otra persona;

c) Utilizar el password, clave o contraseña de otra persona para extraer información, enviar correos o acceder a datos confidenciales con fines particulares o irregulares.

B) Control de accesos:

6.5 Los Gerentes, Sub Gerentes y Jefes Inmediatos o los que hagan sus veces según corresponda, tienen la siguiente responsabilidad:

a) Evaluar y solicitar el acceso a los sistemas y aplicativos del personal a su cargo, señalando módulos, roles, niveles de acceso y horario, los mismos que deberán guardar relación con su cargo y funciones; así mismo con relación a las bajas o suspensión de usuarios de igual forma estos pedidos deberán realizarse por escrito.

b) Revisar permanentemente los niveles de autorización de uso de equipos, información y sistemas, debiendo informar obligatoriamente a la Sub Gerencia de Informática los desplazamientos de personal a otra dependencia o de aquellas rotaciones que se den dentro de la misma unidad orgánica, en el plazo más inmediato.

c) Identificar los reportes de la siguiente manera:

c.1) Estricta confidencialidad;

c.2) Confidencialidad con acceso a ciertos funcionarios;

c.3) De dominio del personal;

c.4) Públicos.

MUNICIPALIDAD PROVINCIAL DE AREQUIPA - Sub Gerencia de Informática

MUNICIPALIDAD PROVINCIAL DE AREQUIPA - GERENCIA DE PLANIFICACIÓN, PRESUPUESTO - Sub Gerencia de Racionalización

6.6 La Sub Gerencia de Recursos Humanos está obligada bajo responsabilidad a enviar a la Sub Gerencia de Informática y Estadística, por lo menos con quince (15) días de anticipación, la relación del personal que va a terminar su vínculo laboral, debiendo dicha Sub Gerencia en coordinación con la Unidad Orgánica donde se encuentre laborando el servidor a tomar las providencias que el caso requiere.

6.7 La Sub Gerencia de Informática y Estadística, para efecto de resguardar la información en los medios informáticos deberá de cumplir con las siguiente acciones:

a) Configurará accesos para:

a.1) Sistemas operativos;

a.2) Uno o varios dominios de red y/o Internet y/o correo electrónico;

a.3) Sistemas de información y/o aplicaciones de software y/o utilitarios;

a.4) Operaciones con base de datos;

a.5) Compartir recursos;

a.6) Espacio para almacenamiento de información en el servidor;

a.7) Espacios compartidos para grupos de trabajo.

b) Los usuarios deberán estar identificados con su correspondiente nivel de acceso, los mismos que pueden ser:

b.1) Consulta de información no restringida o reservada;

b.2) Mantenimiento de información no restringida o reservada;

b.3) Consulta de información restringida;

b.4) Mantenimiento de información restringida.

c) La computadora de trabajo que no tenga ninguna actividad durante un cierto periodo de tiempo, se le deberá suspender su sesión de manera automática, para su posterior operatividad el usuario tendrá que volver a registrar su contraseña teniendo en cuenta el numeral 6.5 de la presente.

d) Restringir el acceso a los sistemas aplicativos y equipos sólo a las computadoras de trabajo que pertenecen a la dependencia y en caso de terceros, que sean de otras dependencias ubicadas al interior o exterior de la Municipalidad, previa autorización de la Sub Gerencia de Informática, la misma que indicará los módulos, niveles de acceso, horario y lapso de tiempo.

e) Diferenciar a los usuarios que solo tienen acceso al equipo más no a los sistemas o base de datos y de igual manera a las personas ajenas a la Municipalidad.

f) Además de restringir el acceso por usuario y password optar por dirección IP y dirección MAC.

C) Protección de la Información

La Sub Gerencia de Informática deberá tener en cuenta lo siguiente:

6.8 Respaldar debidamente toda aquella información que la Municipalidad catalogue como sensible, debiendo tener en cuenta los parámetros de su ejecución a continuación señalados:

a) Volumen de información a copiar:

a.1) Copiar solo los datos; poco recomendable;

a.2) Copia completa; recomendable si el soporte, tiempo de copia y frecuencia lo permiten;

a.3) Copia incremental; solamente se almacenan las modificaciones realizadas desde la última copia completa. Utilizan un mínimo espacio de almacenamiento;

a.4) Copia diferencial; se almacenan los ficheros completos que han sido modificados, al igual que el anterior se necesita la copia completa original.

b) Tiempo disponible para efectuar la copia que no suponga un contratiempo con el funcionamiento habitual del sistema de información.

c) Soporte utilizado como cintas magnéticas, discos compactos, grabadoras de CD-ROM's o cualquier otro dispositivo capaz de almacenar datos.

d) Frecuencia de realización de copias de seguridad en forma diaria y oportuna.

e) Planificación de la copia definiendo hora, día, semana y mes y en lo posible en forma automática a través de tareas programadas.

f) Mecanismos de comprobación de la copia.

g) Establecer estándares en la codificación y etiquetado de los dispositivos de almacenamiento externo a utilizar.

h) Responsabilidad del proceso asignado a una persona.

6.9 Las copias de seguridad, son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia a otro local debidamente acondicionado).

6.10 Mantener controlado el uso de los datos de la Municipalidad, haciendo que la información se muestre ininteligible para aquellas personas sin acceso autorizado y ello por medio de técnicas criptográficas.

6.11 Proteger la integridad de la información publicada electrónicamente a fin de evitar la modificación no autorizada. Su publicación deberá estar autorizada por el órgano competente.

D) Administración de Programas de Aplicación

La Sub Gerencia de Informática es responsable de:

6.12 Los programas de aplicación como activos, deberán tener control rígido sobre sus modificaciones, deberán estar documentadas, para estar seguros que los cambios no causen daños accidentales o intencionados a los datos o su uso no autorizado. Estas modificaciones deben responder a:

a) Fallas de programación;

b) Cambio de políticas normativas internas o externas;

c) Cambio de operatividad;

d) Incremento de facilidades;

e) Control de versiones.

MUNICIPALIDAD PROVINCIAL DE AREQUIPA - Sub Gerencia de Informática

6.13 Las tareas de desarrollo y mantenimiento de sistemas, deben seguir el ciclo de desarrollo del software y contemplar medidas de seguridad en cada una de sus fases, además de exigir su cumplimiento, en caso de que estas tareas sean realizadas por terceros. Para ello, la documentación correspondiente a los sistemas que se desarrollen, deben estar correctamente terminados asignando la debida seguridad para su resguardo y acceso a ésta información.

MUNICIPALIDAD PROVINCIAL - GERENCIA DE PLANIFICACIÓN, PRESUPUESTO Y RACIONALIZACIÓN - Sub Gerencia de Racionalización - DE AREQUIPA

6.14 Desarrollar como sistema de seguridad un software de control de todas las actividades de la Municipalidad.

E) Protección de Servidores

6.15 Las Gerencias de Administración Financiera y Planificación, Presupuesto y Racionalización, deberán viabilizar el presupuesto y la logística necesaria para lo siguiente:

a) Establecer ambientes destinados a los servidores que debe ser exclusivos y estar aislados con temperatura adecuada, acceso restringido al lugar y protegidos contra robos, desastres, incendios. De igual manera dichos ambientes no deben ser accesibles para nadie, excepto para el administrador de la red, administrador de seguridad de la información, administrador de base de datos o quien haga sus veces.

b) Se disponga de UPS's o generadores eléctricos operativos frente a cortes de suministro eléctrico.

6.16 La Sub Gerencia de Informática preverá que los sistemas instalados en los servidores estén configurados para generar archivos de bitácora (logs) y registros de auditoría (audit trails), que graben eventos relevantes sobre la seguridad de la información, debiendo revisarlos periódicamente y guardar como parte de las copias de seguridad. Estos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones y otras actividades de auditoría, por tal razón dichos archivos deben

protegerse para que no sean alterados, y ser leídos sólo por personas autorizadas.

F) Seguridad para Equipos Informáticos

6.17 Todos los usuarios de equipos informáticos deben respetar y no modificar la configuración del hardware y software establecido por la Sub Gerencia de Informática, salvo ésta última lo autorice. Cualquier falla debe informarse inmediatamente a la dependencia antes señalada.

6.18 Está prohibida la instalación de softwares no autorizados por la Sub Gerencia de Informática, toda información externa que se pretenda grabar o usar en el equipo informático, antes debe ser examinada por un programa antivirus previamente instalado por personal de la Sub Gerencia de Informática.

6.19 Los usuarios durante el uso de sus equipos son responsables de:

a) Revisar su buen funcionamiento una vez iniciada su labor;

b) No usarlo con fines recreativos, particulares o de interés personal;

c) Para el retiro temporal de su puesto de trabajo, tomar la precaución de cerrar sesión de los sistemas y aplicativos que utilizan, o activar un salva pantalla (screen saber) con password, clave o contraseña;

d) Cualquier error o alerta de los sistemas aplicativos o del mismo equipo que sea desconocido, se deberá comunicar inmediatamente a la Sub Gerencia de Informática para el soporte necesario;

e) Una vez culminada su labor diaria, deberán de apagar todos los equipos a su cargo (CPU, monitor, impresora y similares).

6.20 Los equipos complementarios como hubs o switches, cualesquiera sean sus características, deben permanecer resguardados en gabinetes especialmente diseñados para contenerlos y deben tener una cerradura que evite manipulación no autorizada y de acceso exclusivo de la Sub Gerencia de Informática.

6.21 La asignación de estaciones de trabajo portátiles (laptops, notebooks, netbooks o similares) será restringida a las personas o dependencias que lo requieran por la naturaleza de sus funciones, es necesario la conformidad del responsable de la dependencia solicitante.

6.22 La Sub Gerencia de Informática de igual forma será responsable del:

a) Mantenimiento preventivo programándose periodos cortos para limpieza de ambientes de servidores y de acuerdo a estadísticas de problemas comunes para limpieza, revisión de piezas, componentes y puesta a un punto de los equipos informáticos. Para ello se elaborará un Plan de Mantenimiento Preventivo Anual de Equipos que incluya unidades de entrada y salida (monitor, teclado, mouse y similares), unidades de almacenamiento (discos duros, disqueteras, lectoras de CD-ROM's y DVD-ROM's, zips y similares), impresoras, hubs, switches, scanners, notebooks, laptops y otros similares que se utilicen en la Municipalidad.

b) Mantenimiento correctivo en el más breve plazo, priorizando la protección de dispositivos de almacenamiento, para ello se debe disponer de una sección destinada a soporte técnico y de proveedores especializados en solucionar las reparaciones que se requieran.

Estas acciones se podrán realizar dentro o fuera de la Municipalidad y por personal de la misma o terceros. Cuando se retiren dichos bienes fuera del local, el Área de Control Patrimonial deberá generar la guía de remisión o documento afín donde se registre lo que se está retirando señalando el motivo de esta acción. Se debe tener especial

cuidado sobre la vigencia de garantías y seguros sobre los equipos, así como un registro de todas las labores de mantenimiento que pesan sobre él.

07. MECANICA OPERATIVA

7.1 La Gerencia Municipal designará mediante resolución a los miembros integrantes del Comité de Seguridad de la Información de los Medios Informáticos (en adelante Comité), el mismo que estará integrado por el Gerente de Administración Financiera, Sub Gerente de Informática y Sub Gerente de Recursos Humanos.

7.2 El Comité, estará presidido por el Gerente de Administración Financiera y será el responsable de coordinar las acciones del Comité; así como de impulsar la implementación y cumplimiento de la presente directiva, dicho Comité deberá sesionar como mínimo cada tres (03) meses y deberá ser convocado por quien la preside.

7.3 La Sub Gerencia de Recursos Humanos, hará de conocimiento a todo el personal nuevo que ingrese a laborar a la Municipalidad, sobre el cumplimiento de la presente Directiva.

7.4 La Sub Gerencia de Informática tendrá a su cargo las siguientes tareas:

7.4.1 Sincronizará la fecha y hora para todos los servidores y por ningún motivo los sistemas tomarán la hora de equipos de trabajo, salvo requerimiento expreso.

7.4.2 Aplicará adecuadamente las actualizaciones (Upgrades y Service Pack) de los Sistemas Operativos, herramientas y lenguajes de programación, asegurando la estabilidad de los diferentes sistemas de información de la Municipalidad, mediante pruebas que estime por conveniente.

7.4.3 En el plazo de 15 días a partir de la vigencia de la presente directiva, deberá elaborar el proyecto de Plan de Seguridad de Información de los Medios Informáticos, considerando obligatoriamente las siguientes acciones:

a) Identificar y evaluar los activos informáticos con que dispone la Municipalidad, como personal, datos, equipamiento, sistemas, servicios, comunicaciones y similares.

b) Identificar amenazas externas como: virus, espionaje, intentos de hacker y similares, así como determinar las amenazas internas, como uso indebido de la información, divulgación a terceros y otros similares.

c) Evaluar riesgos, calculando la probabilidad que se den las amenazas sobre los activos identificados y el costo económico y psicosocial asociado al impacto de la amenaza en caso se diera.

d) Plantear mecanismos de contingencia, frente a amenazas que se pudieran dar para reanudar a la normalidad los medios informáticos en el más breve plazo.

e) Implantará y velará por el cumplimiento de la presente, para ello preverá la adquisición e implementación de productos de seguridad informática.

7.4.4 El Órgano de Control Institucional es responsable de practicar auditorías periódicas sobre los sistemas de información y actividades vinculadas con las tecnologías de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad en la información establecidas en la presente directiva y de las normas vigentes sobre la materia, debiendo recomendar las medidas correctivas pertinentes.

08. DISPOSICIONES COMPLEMENTARIAS

8.1 El Comité anualmente o cuando la situación lo amerite procederá a la revisión

de las normas y procedimientos de los medios de Seguridad Informáticos, a fin de reflejar los cambios producidos durante dicho periodo y se generará en caso sea necesario una nueva versión como parte del proceso de mejora continua.

8.2 La Sub Gerencia de Informática conjuntamente con la Sub Gerencia de Recursos Humanos, ejecutarán programas de formación y sensibilización del personal, contratistas y terceros involucrados, respecto a la seguridad de la información, para garantizar el cumplimiento de la presente Directiva. Para ello deberán evaluar el nivel de conocimientos del personal involucrado, para un buen desenvolvimiento de sus labores y aseguramiento de la protección de la información. Ello implica concientizar al usuario sobre la variedad de formas en que los datos pueden perderse o deteriorarse.

8.3 Las transgresiones que se efectúen a la presente directiva o a cualquier procedimiento que se derive de ésta y que ocasione cualquier riesgo o pérdida para la Municipalidad, ameritará una sanción disciplinaria por parte de la Municipalidad a los servidores que incurran en dicha causal.

8.4 Las transgresiones en que incurran los servidores de la Municipalidad, se clasifican de la siguiente manera:

8.3.1 Transgresiones de seguridad:

a) Ingreso a los ambientes sin autorización;

b) Intentos fallidos para ingresar con un password, clave o contraseña a un equipo informático que le corresponda a otro usuario;

c) Intentos de ingreso a computadoras de trabajo no autorizados;

d) Correos enviados con datos o información no permitida.

e) Ingreso a computadoras de trabajo fuera del horario de trabajo sin contar con autorización de su inmediato superior.

f) Modificación de montos dinerarios de deudas tributarias y no tributarias, sin contar con la autorización oficial.

g) Correos personales enviados a destinos externos a la Municipalidad, sin contar con la autorización correspondiente.

h) Retiro de documentos físicos sin autorización del inmediato superior.

8.3.2 La responsabilidad de la seguridad de la información de los medios informáticos es compartida en el siguiente orden:

a) Gerencias y Sub Gerencias de competencia de la Información, sistemas y equipos;

b) Responsables de la seguridad de la información de los medios informáticos (Comité y Sub Gerencias de competencia de la Información, sistemas y equipos);

c) Responsables de la seguridad de información de los medios informáticos (Sub Gerencia de Informática);

d) Responsables de los Procesos (Usuarios).

09. DISPOSICIONES TRANSITORIAS

9.1 La Sub Gerencia de Informática temporalmente hará las veces del Comité, el mismo que deberá crearse en el plazo de 15 días a partir de la vigencia de la presente Directiva.

9.2 La Secretaría General de la Municipalidad, deberá difundir y comunicar la presente a todo el personal de la Municipalidad siendo su aplicación obligatoria.

9.3 La presente directiva tendrá vigencia a partir del día siguiente de su aprobación mediante resolución de Gerencia Municipal y su cumplimiento será progresivo en base al Plan Integral de Seguridad de la Información de los Medios Informáticos que será propuesto por la Sub Gerencia de Informática y revisado y aprobado por el Comité.

10. DISPOSICIONES FINALES

A) Responsabilidad:

10.1 Todo el personal de la Municipalidad, es responsable de conocer la presente directiva, así como las normas relacionadas con ésta, los procedimientos y los estándares generales y aquellos específicamente relacionados con la dependencia donde labora, teniendo en cuenta el siguiente detalle:

10.1.1 Servidores en General

Deberán garantizar activamente la protección de la información mediante:

a) La utilización de la información y de los sistemas de información solo para fines laborales y no permitir su uso a personas no autorizadas;

b) El cuidadoso manejo de la información y de los sistemas informáticos, diferenciándola entre la pública y la reservada (privada o confidencial) para que su divulgación no atente contra las normas vigentes;

c) La comunicación inmediata al superior jerárquico por las deficiencias encontradas o incidentes ocurridos sobre seguridad de información (virus, intrusos, modificación o pérdida de datos y similares);

d) El fiel cumplimiento de los procedimientos y estándares señalados en la presente directiva.

e) Participar en las pruebas e implementación de contingencias, ante eventuales caídas de los sistemas de información.

10.1.2 Funcionarios

Deberán garantizar e implementar la seguridad de la información y de los sistemas de información dentro de su dependencia a su cargo, mediante:

a) La supervisión periódica del personal a su cargo a fin de detectar posibles deficiencias en materia de seguridad de la información;

b) El inicio rápido de medidas correctivas e informar al Comité o a quien haga sus veces, de las deficiencias encontradas o incidentes ocurridos en materia de seguridad de información de los medios informáticos;

c) La difusión a sus subordinados en forma regular sobre los alcances de la presente directiva, así como sus actualizaciones sobre todo en aquellos servidores nuevos en su dependencia;

d) La definición de roles y niveles de acceso a la información y los sistemas de información de acuerdo a los cargos que desempeñe el personal;

e) La designación de usuarios administradores que participen activamente en la definición, creación, pruebas, implementación y mantenimiento de los sistemas de información;

f) La coordinación de acciones para la activación de las contingencias ante eventuales caídas de los sistemas de información, asegurando la continuidad

de los servicios y actividades de la dependencia a su cargo y por ende de la Municipalidad.

10.1.3 Comité de Seguridad de la Información de los Medios Informáticos

Deberá establecer mecanismos de monitoreo, evaluación y actualización de las políticas de seguridad de la información, mediante:

a) La evaluación y coordinación en la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;

b) La coordinación del análisis de riesgos, contingencias y prevención de desastres;

c) La evaluación y revisión de la situación luego de incidentes ocurridos y que ponga en peligro la seguridad de la información;

d) La revisión y aprobación de proyectos de seguridad de información y programas de formación y sensibilización del personal, contratistas y terceros involucrados respecto a la seguridad de información;

e) La garantía de hacer y cumplir las normas vigentes en cuanto a materia de seguridad de información dentro o fuera de la Municipalidad.

11. ANEXOS:

11.1 Anexo 01: Definiciones

Anexo Nº 01

- **Acceso:** Es el resultado positivo de una autenticación.
- **Administrador de Red:** Encargado de asegurar la correcta operación de la red.
- **Administrador de Seguridad de la Información:** Encargado de implementar medidas de protección adecuada, supervisar los registros de actividades y controlar las alertas de seguridad.
- **Administrador de sistemas:** Encargado de mantener y esperar un sistema.
- **Aplicativo:** Software o programa de computador elaborado con el fin de sistematizar la información que se trabaja durante la realización de un proceso.
- **Archivo bitácora:** Archivo que registra errores y mal funcionamiento de los servidores (sistemas operativos y sistemas de información).
- **Base de Datos:** Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
- **CD-ROM:** Disco compacto utilizado de sólo lectura.
- **Computadora:** Máquina electrónica que recibe y procesa datos para convertirlos en información útil.
- **Contingencia:** Acontecimiento que se presenta de modo sorpresivo y que puede poner4 en peligro la seguridad de la información.

  Correo electrónico: Servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente.
- **C. P. U.:** Unidad Central de Proceso, caja que contiene la placa madre, el microprocesador, discos duros y las tarjetas de expansión.
- **Dirección IP:** (IP: Protocolo de Internet), es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora).
- **Dirección MAC:** (MAC: Control de acceso al medio) Identificador asignado de fábrica para los dispositivos de red contenidos en una computadora.
- **Disco duro:** Dispositivo de gran capacidad que se utiliza para almacenar datos y programas.
- **Disquetera:** Dispositivo de una computadora donde se introduce el disquete para leer, grabar o modificar los datos que éste contiene.
- **DVD-ROM:** Dispositivo de almacenamiento similar al CD-ROM, pero de mayor capacidad.
- **Estación de Trabajo:** Computadora conectada a la red.
- **Generador eléctrico:** Máquinas destinadas a transformar la energía mecánica en eléctrica.
- **Hub:** Dispositivo capaz de enlazar físicamente varias computadoras.
- **Información:** Conjunto organizado de datos que puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes o expuesta en una conversación.
- **Internet:** Gran red descentralizada de computadoras, de ámbito global y públicamente accesible, que proporciona una ingente cantidad de servicios de comunicación de varios

tipos, incluyendo la World Wide Web, el correo electrónico y muchos otros.

- **Intruso:** Persona que intenta accesar a un sistema informático sin autorización.
- **Laptop o Notebook:** Computadora portátil que funciona con baterías recargables.
- **Log:** Archivo que registra movimientos y actividades de un sistema determinado
- **Manejo de riesgo:** Método utilizado para afrontar riesgos y proteger la información
- **Microprocesador:**
- **Monitor:** También conocido como "pantalla", dispositivo de salida que muestra los resultados del procesamiento de una computadora.
- **Mantenimiento correctivo:** Es el mantenimiento destinado a prevenir la aparición de fallos.
- **Módulo:** Es una parte de un programa de computadora. Es una parte de las opciones del menú de un sistema.
- **Netbook:** Computadora portátil de bajo costo y reducidas dimensiones lo cual aporta una mayor movilidad y autonomía. Son utilizadas principalmente para navegar por Internet y realizar funciones básicas como procesador de texto y de hojas de cálculo.
- **Nivel de acceso:** Listado de derechos que pueden ser por escritura, lectura, consulta o ninguno de los antes mencionados.
- **Password, clave o contraseña:** Conjunto de caracteres que una persona debe dar para ser reconocida como un usuario autorizado.
- **Pérdida de datos:** Cuando los usuarios de equipos informáticos consideran que los datos perdidos se han destruido de forma permanente y no hay ninguna esperanza de recuperarlos.
- **Placa madre: (placa base, tarjeta madre, motherboard o mainboard):** Es una tarjeta de circuito impreso donde se conectan las demás partes de la computadora.
- **Programa:** Conjunto de instrucciones que una vez ejecutadas realizarán una o varias tareas en una computadora.
- **Recurso:** Elemento informático como base de datos, sistemas operacionales, redes, sistemas de información o comunicaciones.
- **Red:** Es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten la información.
- **Registro de auditoría (Audit trail):** Conjunto de datos relacionados con las actividades de los usuarios, excepciones y eventos de la seguridad de la información.
- **Rol de usuario:** Conjunto de permisos y privilegios.
- **Salva pantalla:** (protector de pantalla) programa de computadora diseñado para conservar la calidad de imagen del monitor, dejando imágenes en movimiento cuando la computadora no esté siendo usada.
- **Scanner:** Dispositivo que utiliza una haz de luz para convertir una foto o texto impreso en información digital para ser manipulado por una computadora.
- **Servidor:** Computadora que forma parte de una red, provee servicios a otras computadoras denominadas clientes.
- **Sistema:** Un sistema es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos,

energía o materia del ambiente y proveen (salida) información, energía o materia. Un sistema puede ser físico o lógico (una computadora, un televisor, un humano) o puede ser abstracto o conceptual (un software).

- **Sistema de información:** Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad.
- **Sistema operativo:** Conjunto de programas que guían en una computadora la realización de tareas básicas. Responsable de gestionar los recursos de la computadora, discos duros, memorias, control de periféricos como monitores, teclados etc.
- **Software:** Procedimientos y reglas lógicas escritas en la forma de programas y aplicaciones que definen el modo de operación de las computadoras.
- **Switch:** Dispositivo capaz de enlazar físicamente varias computadoras de forma activa, enviando los datos exclusivamente a la computadora que va destinada.
- **Tarjetas de expansión:** Dispositivos con diversos circuitos integrados y controladores que insertadas en las ranuras de la placa madre amplia la capacidad de la computadora.
- **UPS: (Uninterrumpible Power Suplly – Sistema de Alimentación ininterrumpida**): Fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de un apagón.
- **Usuario:** Identificación personal para acceder a un aplicativo, sistema o equipo.
- **Usuario anónimo:** Usuario que no se ha autenticado.
- **Usuario genérico:** Usuario que define a un conjunto de usuarios y que no tiene identificación personal definida como familia, practicante, abogado, tributaria, alcalde.
- **Usuario invitado:** Usuario que tiene acceso a la información de consulta.
- **Utilitario:** Programa diseñado para realizar una función particular, enfocados o relacionados con el manejo de sistema operativo de la computadora.
- **Virus:** Programa que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.
- **Zip:** Unidad portátil de almacenamiento (parecidos a los disquetes, pero de mayor capacidad).