"Año de la Inversión para el Desarrollo Rural y la Seguridad Alimentaria"

MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA

RESOLUCION DE ALCALDIA Nº 390 -2013-MDPP

Puente Piedra, 01 de junio del 2013

EL ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA

VISTO: los Informes Nro. 108-2013-MDPP-GIGE de la Gerencia de Informática y Gobierno Electrónico, 130-2013-MDPP-GAJ de la Gerencia de Asesoría Jurídica y el Memorándum N° 499-2013-GM/MDPP de la Gerencia Municipal, y;

CONSIDERANDO:

Que las Municipalidades son órganos de gobierno local que gozan de autonomía política, económica y administrativa en los asuntos de su competencia, y su autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico, de conformidad con lo que establece el artículo 2 del Título Preliminar de la Ley N° 27972 – "Ley Orgánica de Municipalidades";

Que, a mérito de lo dispuesto en los literales f) y j) del artículo 50° del Reglamento de Organización y Funciones de la Municipalidad Distrital de Puente Piedra, aprobado por Ordenanza N° 203-MDPP, de fecha 26 de julio de 2012, entre las funciones de la Gerencia de Informática y Gobierno Electrónico figuran: f) administrar los sistemas, aplicaciones y servicios de seguridad de la información; y j) formular y dirigir el desarrollo y aplicación de lineamientos, políticas, normas, procedimientos y prácticas que aseguren los niveles adecuados de confidencialidad, integridad y disponibilidad de los sistemas de información, de los datos y de las comunicaciones de la Municipalidad;

Que, en ese extremo, la Gerencia de Informática y Gobierno Electrónico mediante informe de vistos, remite el documento POLITICAS DE SEGURIDAD INFORMÁTICA de la Municipalidad Distrital de Puente Piedra, para su revisión y aprobación respectiva;

Que, la Gerencia de Asesoría Jurídica a través del informe de vistos, señala que el proyecto de Políticas de Seguridad Informática, elaborado por la Gerencia de Informática y Gobierno Electrónico, debe ser aprobado, por contener los estándares de las normas técnicas peruanas y constituir una herramienta organizacional;

Que, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la Municipalidad crecer y mantenerse competitiva;

Estando a lo expuesto, y con las facultades conferidas por el numeral 6 del Art. 20° de la Ley 27972 – Ley Orgánica de Municipalidades;

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR el documento **POLÍTICAS DE SEGURIDAD INFORMÁTICA** para la Municipalidad Distrital de Puente Piedra, el mismo que en Anexo forma parte integrante de la presente Resolución.

MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA

ARTICULO SEGUNDO.- ENCARGAR a la Secretaria General remitir a la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI de la Presidencia del Consejo de ministros, el documento aprobado en el párrafo precedente.

ARTICULO TERCERO.- DISPONER que la Gerencia de Informática y Gobierno Electrónico publique la presente Resolución en el Portal de la Municipalidad y difunda a los usuarios internos, a través del correo de dominio institucional.

REGISTRESE, COMUNIQUESE Y CUMPLASE

MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA
ING. ESTEBAN F. MUÑOZON FERNANDEZ
ALCALDE

POLÍTICAS DE SEGURIDAD INFORMÁTICA

MUNICIPALIDAD DE PUENTE PIEDRA

	NOMRBRE	CARGO	FIRMA	FECHA
ELABORADO POR	Nilton Diestro Alvarado	Gerente de Informática y Gobierno Electrónico.		
REVISADO POR		Gerente Municipal		
APROBADO POR		Alcalde		

ÍNDICE

POLÍTICAS DE SEGURIDAD INFORMÁTICA

INTRODUCCION

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes de las empresas para mejorar su productividad y poder explorar mas allá de las fronteras nacionales, cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la Municipalidad.

En este sentido las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la Municipalidad crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas Y debilidades y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

CAPITULO I

POLÍTICAS DE SEGURIDAD INFORMÁTICA: DEFINICIÓN Y ELEMENTOS

1. DEFINICIÓN

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

Las Políticas de Seguridad de la Información, surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Cada empresa definirá sus políticas más convenientes y se asegurará que las mismas cumplan con los requerimientos normativos vigentes. Por tal razón las políticas de seguridad deben concluir en una posición consiente por el uso y limitaciones de los recursos y servicios informáticos.

2. ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD

Como una política debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la Institución para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

3. PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD

Es importante que al momento de establecer las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos.

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con las Gerencias y Subgerencias, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos, bienes y sus elementos de seguridad.
- Identificar quien tiene la autoridad para tomar decisiones en cada Gerencia y Subgerencia, pues son ellos los interesados en salvaguardar los activos críticos de su área.
- Monitorear periódicamente los procedimientos y operaciones de la institución, de tal forma que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explicita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

4. RAZONES QUE IMPIDEN LA APLICACIÓN DE LAS POLITICAS DE SEGURIDAD

A pesar de que un gran numero de organizaciones canalizan sus esfuerzos para definir directrices de seguridad informática y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrentan es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Finalmente es importante señalar que las políticas por si solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores para administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que faciliten la formalización y materialización de los compromisos adquiridos con la organización.

CAPÍTULO II

LINEAMIENTOS QUE DETERMINAN LAS ACTIVIDADES PERMITIDAS AL PERSONAL

1. Política Institucional

Para la Municipalidad Distrital de Puente Piedra los sistemas informáticos y la información relacionados tanto a los contribuyentes como a la Institución, son considerados activos críticos institucionales necesarios para el desarrollo de sus actividades.

Por lo tanto, todos los que laboramos en la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA tenemos como principio y obligación de trabajo, proteger y resguardar los activos críticos, comprometiéndonos a:

a. Mantener y mejorar la disponibilidad, integridad y confidencialidad de los sistemas informáticos y la información, asegurándonos que estos sean reservados y utilizados solo para fines Institucionales.

b. Cumplir con las normas establecidas en Sistema de Seguridad Informática.

2. Políticas Generales

La Alta Dirección de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA, considerando la importancia de los sistemas informáticos y la información, establece que las normas definidas por la Gerencia de Informática y Gobierno Electrónico, son de cumplimiento obligatorio en toda la institución y por ende, por todo su personal.

2.1. Del acceso físico

a. El acceso al DATA CENTER es restringido; únicamente podrá ingresar el personal autorizado por la Gerencia de Informática y Gobierno Electrónico.

b. La Gerencia de Informática y Gobierno Electrónico son los responsables de autorizar el ingreso a este.

2.3 De las cuentas de acceso

a) Las cuentas de acceso serán habilitadas para todo el personal con contrato indefinido o temporal y eventualmente practicante; a excepción de aquellos trabajadores que se encuentren haciendo uso de su periodo vacacional, licencia u otro que contemple la Institución. Las cuentas de acceso deben ser usadas única y exclusivamente para actividades relacionadas con el cumplimiento de funciones asignadas por la Institución y ninguna podrá ser usada para propósitos distintos, ilegales o no éticos.

b) Las cuentas de acceso son estrictamente personales e intransferibles, siendo el usuario responsable por cualquier alteración de información que se produzca con su cuenta.

2.4 De la Fiscalización del uso de los sistemas informáticos

a. A fin de verificar el uso de los sistemas informáticos se realice con estricta sujeción a las reglas que sobre esta materia fija la Entidad, la misma se reserva el derecho a introducir los elementos de registro y control que estime conveniente, así como el derecho de acceder a ellos en su integridad para determinar si su utilización se da en función al desarrollo de las actividades y fines institucionales y/o al cumplimiento de las obligaciones de trabajo.

Lo expuesto en el párrafo precedente no comprende el acceso al servicio de Correo Electrónico del usuario, salvo autorización expresa por parte del mismo.

Para verificar el uso de los sistemas asignados a determinada persona que incluya la revisión integral de estos salvo al servicio de correo electrónico, se requiere contar con la autorización de la Gerencia de Informática y Gobierno Electrónico.

b. La Gerencia de Informática y Gobierno Electrónico podrá deshabilitar las cuentas de usuarios que pongan en peligro el buen funcionamiento de los sistemas informáticos.

2.5 De los sistemas informáticos

a. Las consideraciones de seguridad para los sistemas desarrollados serán contempladas desde la etapa de diseño y serán verificadas en la etapa de homologación.

b. La instalación de dispositivos informáticos y Software; así como el monitoreo de la red deberá ser autorizado y efectuado por la Gerencia de Informática y Gobierno Electrónico.

c. Todo equipo informático de la Institución debe contar con garantía de venta y en ausencia de esta, con servicio de mantenimiento preventivo y correctivo durante su periodo de vida útil.

d. El espacio asignado a los usuarios en los servidores podrá ser modificado atendiendo las necesidades de la Institución.

e. Toda información que se procese en los servidores de la Institución deberá tener un respaldo, así como una copia del mismo.

f. Cualquier incidente que afecte la seguridad informática, debe ser reportado a la Gerencia de Informática y Gobierno Electrónico, para que este tome las acciones correspondientes y prevea futuras ocurrencias.

2.6 Del sistema de servidor de red

a. La configuración de los sistemas operativos seguirá criterios normalizados y será revisada periódicamente.

b. Deberá existir un sistema de control de lógico de acceso, adecuado al carácter de la información que se desee proteger.
c. Para el uso de los recursos y servicios informáticos, los usuarios deberán cumplir las normas que la Gerencia de Informática y Gobierno Electrónico reglamente para tal fin.

d. Todas las computadoras personales deben tener un Software antivirus que proteja la información almacenada en los discos.

e. Únicamente el personal autorizado puede desarrollar aplicativos, los cuales solo serán para fines Institucionales, quedando prohibido el desarrollo o instalación de programas no autorizados que alteren la seguridad, consistencia o que dañen cualquier sistema informático.

f. Los usuarios deberán conectarse únicamente a los recursos de red que se les haya designado explícitamente.

g. Cualquier acceso de usuarios y/o entidades externas a los recursos de red de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA, deberá contar con una autorización expresa de la Gerencia de Informática y Gobierno Electrónico.

2.7 Del uso de licencias

a. Solo se puede instalar Software que cuente con la respectiva licencia de uso y este autorizado por la Gerencia de Informática y Gobierno Electrónico.

b. La descarga del Software a través del Internet que sirva para fines Institucionales, será efectuada únicamente por la Gerencia de Informática y Gobierno Electrónico.

2.8 Del uso responsable de los recursos informáticos

a. Los usuarios deberán utilizar los recursos informáticos según las normas de conservación y uso que la Gerencia de Informática y Gobierno Electrónico emita.

2.9 Del manejo de la información

a. Cada usuario es responsable de preservar en lugar seguro los documentos y/o medios magnéticos que contengan información confidencial o trascendental evitando dejarlos al alcance de terceros. Si un usuario deja de laborar en la Institución, se deberá generar un respaldo de la información contenida en su equipo asignado.

b. El usuario tiene la obligación de guardar todos los archivos de gestión y documentación generada en cumplimiento de sus obligaciones y funciones designada en las carpetas compartidas asignadas y por ningún motivo será eliminada al término de su vínculo laboral con la Institución.

c. Todo recurso compartido a través de la red se protegerá con medidas de control de acceso coherentes con su importancia.

d. Toda transferencia de información de carácter confidencial o reservado, a través de cualquier medio, será protegida por mecanismos que garanticen su integridad, autenticidad y confidencialidad.

e. Todo equipo que sea entregado a terceros (por motivos de reparación o baja), deberá someterse a un proceso de borrado de archivos digitales el cual se realizara considerando el nivel de confidencialidad más alto de los archivos contenidos en el dispositivo.

f. Todo documento físico con información de carácter confidencial o reservado, proveniente de los sistemas de información y que esté en desuso, deberá ser eliminado utilizando un triturador de papeles para evitar la filtración de información en los canales de eliminación.

g. Todo medio de almacenamiento informático que va a ser eliminado, deberá someterse a un proceso de eliminación física o borrada de archivos digitales, el cual se realizara considerando el nivel de confidencialidad más alto de los archivos contenidos en el dispositivo.

3. De las sanciones

Cualquier acción que vaya en contra de estas políticas será sancionada por la entidad a través de sus procedimientos pertinentes, previo informe de la Sub Gerencia de Personal.

GLOSARIO DE TERMINOS

Activos Críticos.- Recursos físicos o lógicos (Hardware, Software, documentos o personal), importantes para un determinado proceso, sin el cual las operaciones normales inherentes al mismo, no podrían llevarse a cabo exitosamente y cuya recuperación generaría un elevado costo para la Institución.

Antivirus.- Programa que busca y eventualmente eliminar los virus informáticos que puedan haber infectado un disco rígido o disquete.

Confidencialidad.- Condición que asegura que la información no debe estar disponible o ser descubierta por personas, entidades o procesos no autorizados.

Contraseña.- Conjunto de caracteres que permite acceder al uso de equipo o un sistema. (Se le conoce también como palabra clave o password)

Correo Electrónico.- Servicio que permite el intercambio electrónico de mensajes y documentos entre personas conectadas a una red a través de sus correspondientes equipos de procesamiento automático de datos (PAD).

Disponibilidad.- Grado en el que una información está en el lugar, momento y forma en que es requerida por un usuario autorizado.

Integridad.- Condición que garantiza que la información sea modificada, incluyendo su creación y borrado, únicamente por el personal autorizado.

Red.- Agrupación de equipos y programas que comparten recursos entre sí, observando "reglas de comportamiento" a partir del uso de un lenguaje y medios de transmisión comunes, sin importar – en lo esencial - la naturaleza de cada elemento dentro de la red.

Respaldo.- Copia de los datos de un archivo o base de datos de un Soporte que posibilite su recuperación.

Servidor.- Computadora central de un sistema de red que provee servicios y programas a otras computadoras conectadas.

Sistema de seguridad informática.- Conjunto de políticas, procedimientos y herramientas (físicas y lógicas) que permitan asegurar la confidencialidad, disponibilidad e integridad de los sistemas informáticos y la información.

Sistema informático.- Conformado por Hardware, Software (aplicativo y de red) y red de telecomunicaciones.

Sistema operativo.- Programa de control principal que administra la operación de la computadora. Es el Software del sistema primario y actúa como el "despachador principal" y como "controlador de tráfico".

Software.- Conjunto de instrucciones que ordenan al procesador que ejecute acciones y/o operaciones especificas.

CAPITULO III

NORMATIVIDAD PARA EL USO ADECUADO DE EQUIPOS INFORMÁTICOS

I. FINALIDAD :

Definir e implantar las normas para la protección y uso adecuado de los equipos informáticos de propiedad de la Municipalidad Distrital De Puente Piedra, así como la información almacenada en los mismos.

II. ALCANCE :

A todo el personal de la **Municipalidad Distrital de Puente Piedra** o al personal externo que realiza labores en la institución, al cual se le asigne temporal o definitivamente cualquier tipo informático para su uso.

El presente documento aplica a todos los equipos que hayan sido autorizados, evaluados, distribuidos y cuya conformidad técnica haya sido dada por la Gerencia de Informática y Gobierno Electrónico.

III. BASE LEGAL :

1. Reglamento de Organización y Funciones de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA.
2. ISO 9001:2000 y la ISO 14001:2004 esta norma Peruana de Seguridad de la Información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, monitorear, operar, mantener y mejorar un efectivo sistema de gestión de Seguridad de la Información ISMS.
3. Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI"

IV. DEFINICIONES :

1. **Equipo Informático.-** Todo equipo que permite el procesamiento y la transferencia de datos, voz, video, multimedia y cualquier tecnología emergente. (se considera equipos de procesamiento de datos y equipos de telecomunicaciones) ver anexo 1.
2. **Equipo de Procesamiento de Datos.-** Todo equipo informático que permite el procesamiento de información.
3. **Equipo de Telecomunicaciones.-** Todo equipo informático que específicamente permite la transferencia de datos, voz, video, multimedia, etc.
4. **Equipo Informático Crítico.-** Por su naturaleza y la información que alberga, es considerado crítico todo equipo ubicado en las áreas de trabajo, los Equipos de Telecomunicaciones y los servidores con información.

5. **USUARIO.-** Todo personal de la **Municipalidad Distrital de Puente Piedra,** o el personal externo que esté realizando sus funciones dentro de la institución; al cual se le asigne temporal o definitivamente el uso de cualquier equipo informático.

6. **Protector de Pantalla.-** Software que se activa cada cierto tiempo y bloquea el acceso lógico de las computadoras de escritorio y portátiles. Para el desbloqueo requiere una contraseña.

7. **Información Sensible.-** Información muy importante y necesaria para el desarrollo de las labores del usuario.

V. RESPONSABILIDADES:

1. Todo el personal que utiliza equipos informáticos es responsable por el buen uso y cuidado de los mismos.

2. En el caso de las dependencias y Agencias Municipales, la Gerencia de Informática y Gobierno Electrónico, será la responsable de atender los reportes de fallas de los equipos informáticos y coordinar para su atención de ser necesario, con el proveedor.

VI. INSTRUCCIONES:

1. Del uso de las Computadoras Personales (de escritorio y portátiles).

1.1. De la seguridad de acceso

1.1.1. Las computadoras de escritorio y portátiles deberán tener instalado un protector de pantalla institucional, con un tiempo de activación definido (entre 1 y 5 minutos).

1.1.2. La información almacenada en los discos duros de las computadoras de escritorio y portátiles, debe estar protegida por una o más claves de acceso:

a) Clave de acceso (contraseña) de encendido.

b) Clave de acceso o definición de usuarios permitidos en recursos compartidos; según lo permita el Sistema Operativo.

c) Clave de acceso (contraseña a las carpetas con información sensible a fin de evitar que si un usuario se autentica en su PC, pueda tener acceso a todos sus archivos.

1.1.3. En el caso de las computadoras portátiles, el usuario deberá considerar que por la naturaleza del equipo y por el tipo de trabajo, toda la información contenida en el mismo es crítica, por ello, deberá considerar especialmente lo indicado en los puntos 1.1.1. y 1.1.2.

1.1.4. En el caso de los equipos informáticos que tengan sello de garantía colocado por el proveedor, el mismo solo podrá ser removido por este último, de acuerdo a lo especificado en el contrato de adquisición de los equipos o por la Gerencia de Informática y Gobierno Electrónico previa coordinación con el proveedor.

1.2. Del Software instalado

1.2.1. Las computadoras personales adquiridas e instaladas en Municipalidad distrital de Puente Piedra solo pueden contener Software autorizado, a excepción de la Gerencia de Informática y Gobierno Electrónico que por sus funciones pueden realizar pruebas con diferentes tipos de Software.

1.2.2. Todo producto de Software no desarrollado en Municipalidad Distrital de Puente Piedra o todo acceso a Software de terceros deberá contar con la autorización por la Gerencia de Informática y Gobierno Electrónico.

1.2.3. El estándar en la configuración de discos de las computadoras personales deberá considerar dos particiones:

a) En la primera partición (unidad C: \ ) se instalara Software estándar y Software de aplicación.

b) En la segunda participación (unidad D: \ o E:) se creara una carpeta DATA en la que se almacenara la información de los usuarios, tal como: documentos, hojas de cálculo, presentaciones, proyectos, etc. La carpeta mencionada NO deberá contener archivos de sistema o Software alguno.

c) En el caso de los equipos que sean utilizados por más de un usuario, deberá existir una subcarpeta que identifique a cada usuario dentro de la carpeta DATA para efectos de diferenciación.

1.3 Las recomendaciones para el uso adecuado de las Computadoras personales, se especifican en el instructivo: INSTRUCCIONES PARA EL USO ADECUADO DE LOS EQUIPOS INFORMATICOS. Ver Anexo 2.

2. Del uso de los equipos de impresión

2.1. La impresora es un recurso de red para uso compartido y el servicio de impresión se brinda a todo usuario que lo requiera. A excepción de los equipos de la Gerencia de Informática y Gobierno Electrónico que por su naturaleza serán utilizados por el personal autorizado por cada área.

2.2. El usuario deberá tener en cuenta que los equipos de impresión son para trabajos relacionados con el desarrollo de las labores propias de cada área.

2.3. Las recomendaciones para el uso adecuado de los Equipos de Impresión, se especifican en el instructivo: INSTRUCCIONES PARA EL USO ADECUADO DE LOS

EQUIPOS INFORMATICOS. Ver Anexo 2.

3. Del uso de los equipos y accesorios de telecomunicaciones

3.1. Los equipos de Telecomunicaciones son de un recurso de red para uso compartido.

3.2. Los equipos de Telecomunicaciones que por su naturaleza estén ubicados en áreas de trabajos diferentes al DATA CENTER, deberán estar instalados en gabinetes de comunicación, teniendo en cuenta las recomendaciones del fabricante y asegurados de tal modo que no puedan ser accesados por terceros.

3.3. Toda maniobra en los sistemas de cableado estructurado será realizada exclusivamente por personal de la Gerencia de Informática y Gobierno Electrónico y por la personas autorizadas por la Gerencia de Informática y Gobierno Electrónico.

4. Del uso de las Unidades lectoras / grabadoras de Discos compactos, de DVD's, las unidades de discos Zip y cualquier medio removible de almacenamiento de información.

4.1. Las unidades lectoras / grabadoras de discos compactos y de DVD's, también llamadas "quemadores de CD's o DVD's, son de uso restringido el cual deberá ser aprobado por la Gerencia de Informática y Gobierno Electrónico o la Gerencia y Subgerencia Responsable.

4.2. En el caso de las áreas que cuentan con Unidad de discos Zip, estas deberán llevar el control del uso de los mismos, siendo este de uso estrictamente Institucional.

4.3. Los medios removibles de almacenamiento de información, tales como memorias o llaves USB son de uso restringido, el cual deberá ser aprobado por la Gerencia de Informática y Gobierno Electrónico, la Gerencia o Subgerencia Responsable.

4.4. La normatividad para el uso de los accesorios definidos en los puntos 4.1., 4.2. y 4.3. Gerencia de Informática y Gobierno Electrónico.

5. De las Prohibiciones:

Queda prohibido a todo usuario:

a) Ingerir alimentos, bebidas o fumar cerca de los equipos informáticos.

b) Utilizar el equipo para juegos. Si se detectara este mal uso, se procederá a su eliminación del disco y se realizara el informe de la Unidad Organizacional correspondiente.

c) Utilizar el equipo para realizar trabajos ajenos al interés de la Institución.

d) Manipular (abrir, desarmar) los equipos informáticos.

e) Desconectar o conectar los equipos sin la autorización correspondiente, pudiendo generar daño en los mismos.

f) Modificar la configuración estándar (Hardware o Software) del equipo.

g) Instalar Software y/o archivos de trabajo copiados de otras computadoras sin autorización de quien corresponda.

h) Copiar y/o compartir archivos de música o video ajenos al interés de la Institución.

i) Desactivar el servicio antivirus en cualquiera de sus opciones (sistema operativo, correo electrónico, etc). Este servicio está instalado en las computadoras personales.

j) Copiar los programas instaladores disponibles en las computadoras, para el uso personal y ajeno a la Institución.

k) Trasladar el equipo informático a una ubicación diferente de donde fue inicialmente instalado sin la coordinación previa con la Gerencia de Informática y Gobierno Electrónico y la Gerencia de Administración, Finanzas y Planeamiento.

l) Utilizar más de un equipo que realice la misma función (por ejemplo computadora personal portátil y de escritorio).

m) Reasignar el equipo informático sin la autorización correspondiente de la Gerencia de Informática y Gobierno Electrónico.

n) Retirar la etiqueta de código de barras con el código patrimonial del equipo.

6. De las responsabilidades del usuario:

Son responsabilidades de todo usuario:

a) El cuidado de la información almacenada en el Disco Duro de la computadora y en los medios de almacenamiento asignados por la Institución.

b) Las claves de acceso (contraseñas) que haya definido.

c) Almacenar toda su información en una carpeta DATA, en la partición D :\ o E \ : de su Disco Duro, a fin de mantener un orden y facilitar la labor del personal de la Gerencia de Informática y Gobierno Electrónico, en caso que el equipo requiera alguna atención.

d) Ejecutar el antivirus antes de almacenar en el Disco Duro información proveniente de mensajes de Correo Electrónico o copiado de otro equipo a través de un medio de almacenamiento. (Disquetes, CD's, llaves USB).

e) Tener una copia de respaldo (Backup) de los archivos que contienen información sensible, tal como se indica en la normatividad definida al respecto por la Gerencia de Informática y Gobierno Electrónico. Las copias de respaldo deberán mantenerse

dentro del local institucional. Para efectos de la ejecución de Backup, se utilizaran los medios magnéticos u ópticos asignados oficialmente.

f) Si la información almacenada en su computadora personal, se borra total o parcialmente por efecto de algún virus o uso inadecuado de algún Software o falla del equipo.

g) Efectuar periódicamente la depuración (eliminación) de archivos innecesarios de uso personal, del directorio DATA existente en el disco duro de la computadora asignada.

h) Brindar las facilidades necesarias para la realización de los mantenimientos preventivos por parte del proveedor del equipo.

VII. DISPOSICIONES TRANSITORIAS:

1. En tanto se defina el protector de pantalla Institucional, los usuarios deberán utilizar el protector de pantalla del sistema operativo y sus opciones.

2. En tanto no se culmine con los trabajos de Cableado Estructurado en las Sedes que no cuentan con ello, habrán equipos de telecomunicaciones que no se ajustaran a lo indicado en el punto 3.2. de la presente documento.

VIII. ANEXOS:

Anexo 1 Relación de equipos informáticos.
Anexo 2 Instrucciones de uso adecuado de equipos informáticos.

ANEXO 1

RELACION DE EQUIPOS INFORMATICOS Y DE TELECOMUNICACIONES

CAPTURADOR DE IMAGEN (SCANNER)
CARGADOR DE BATERIA EN GENERAL (*ups*)
COMPUTADORA PERSONAL PORTATIL (NOTEBOOK)
CONCENTRADOR DE RED (HUB/SWITCH9
CORTAFUEGOS (FIREWALL)
GATEWAY
DUPLICADOR DE DISQUETES
EQUIPOS MULTIFUNCIONALES
GRABADORA DE DISCO COMPACTO
IMPRESORA DE INYECCION DE TINTA (*)
IMPRESORA LASER (*)
IMPRESORA MATRIZ DE PUNTO (*)
LECTORA DE CINTA MAGNETICA
LECTORA DE DISCO COMPACTO
MONITOR
PROYECTOR MULTIMEDIA (*)
MOUSE
RUTEADOR DE RED (ROUTER)
SERVIDOR
SERVIDOR DE IMPRESIÓN PARA RED (PRINT SERVER)
TECLADO
TELEFONO IP
UNIDAD CENTRAL DE PROCESO (CPU)
UNIDAD DE ARREGLO DE DISCO (DISK ARRAY)
UNIDAD PARA COPIA DE SEGURIDAD (TAPE BACKUP EXTERNO)
UNIDAD PARA GRABACION DE DISCO COMPACTO

ANEXO 2

INSTRUCCIONES PARA EL USO ADECUADO DE LOS EQUIPOS INFORMATICOS

Instrucciones que deberá seguir el usuario para mantener en buen estado de los equipos informáticos asignados a él.

1. Del cuidado de las computadoras personales y portátiles:

1.1. Generales

a) No exponer el equipo a: líquidos, precipitaciones climatológicas, humedad excesiva ni temperaturas extremas.

b) No colocar objetos sobre el equipo o cerca de él, de modo que impidan su ventilación.

c) Al término de sus sesiones de trabajo, el usuario deberá apagar completamente el equipo, incluyendo los monitores de los equipos con autoapagado y las impresoras, así como cubrirlos con su funda protectora.

d) Todo equipo informático crítico, deberá estar conectado al tomacorriente de energía eléctrica estabilizada (red UPS).

e) Los equipos informáticos críticos, no deberán conectarse a las extensiones denominadas supresoras de picos.

f) No deberán conectar a la red de energía eléctrica estabilizada (red UPS) equipos no informáticos como ventilador, radio, cargador de celular, fotocopiadora, microondas, trituradores, etc.

1.2. Especificas para las computadoras portátiles:

a) Trabajar siempre con la batería instalada en la computadora, inclusive cuando utilice alimentación eléctrica externa.

b) Las baterías adicionales deben ser guardadas en un lugar seco y a la temperatura que indique el fabricante mientras no se utilicen. No se debe tratar de abrirlas ni repararlas.

c) La descarga y carga de baterías de las computadoras portátiles se efectuará con la frecuencia y de acuerdo al procedimiento que indique el fabricante en el manual de usuario del equipo.

d) En caso de conectarse a la red con las computadoras portátiles, se debe tener cuidado al conectar o desconectar la tarjeta de adaptador de red.

e) Si se tuviera que viajar con la computadora portátil, nunca se dejara como equipaje de bodega, si no que se deberá llevar como equipaje de mano.

CAPÍTULO IV

POLÍTICAS Y NORMAS LA CREACIÓN, ENTREGA Y UTILIZACIÓN DE LAS CUENTAS Y CLAVES DE ACCESO A LOS SISTEMAS.

I. FINALIDAD:

Implantar el procedimiento para la solicitud, creación y uso adecuado de las cuentas y claves de acceso a los sistemas en producción.

II. ALCANCE:

A todo el personal de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA.

III. BASE LEGAL:

- Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI"

  Esta Norma Peruana de Seguridad de la Información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, monitorear, operar, mantener y mejorar un efectivo sistema de gestión de seguridad de la información ISMS.

IV. DEFINICIONES:

1. **Cuenta:** Código alfanumérico que sirve para identificar a un usuario y registrar las operaciones y transacciones que realiza interactuando con los sistemas operativos.
2. **Cuentas de accesos básicos:** Cuenta a la cual se otorgaran los accesos que por defecto corresponden a todo el personal nuevo que se incorpora a la Institución, los cuales son: acceso a la red, correo electrónico, intranet en línea,
3. **Clave de acceso:** Conjunto de caracteres que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.
4. **Sistema en producción:** Conjunto de programas puestos a disposición del usuario para que a través de su uso se automatice uno o más procesos.
5. **Titular de cuenta:** Persona a quien se le asigna una cuenta y su clave respectiva a un sistema en producción.
6. **Perfil de usuario:** Nivel de permisos a los que un grupo de usuarios tiene y a los diferentes opciones para interactuar con los sistemas en producción.
7. **Nivel de permisos:** Autorización para procesar información en el siguiente orden: leer (consultar), insertar, modificar y borrar una información.

V. RESPONSABILIDADES:

1. La Gerencia Municipal a través de la Gerencia de Informática y Gobierno Electrónico, será la encargada de normar el esquema de generación de cuentas, así como los lineamientos de los procedimientos que se requieran.

2. La Gerencia de Informática y Gobierno Electrónico, será la encargada de investigar y proponer soluciones de control de accesos, así como otras medidas de seguridad que se requieran.

3. La Gerencia de Informática y Gobierno Electrónico, será la encargada de efectuar revisiones periódicas de los accesos con la finalidad de detectar el mal uso de las cuentas y comunicarlo al jefe inmediato del usuario involucrado y de ser el caso, comunicar a la Sub Gerencia de Recursos Humanos para que tome las medidas pertinentes.

4. La Gerencia de Informática y Gobierno Electrónico, será la responsable de centralizar el proceso de adquisición de las soluciones propuestas por las Gerencias y Sub Gerencias.

5. La Sub Gerencia de Recursos Humanos de la Municipalidad de Puente Piedra será la responsable de informar de las acciones de alta o baja de personal, según lo considerado en el numeral 8.2 b) del presente.

6. La Gerencia de Informática y Gobierno Electrónico, será la encargada de la recepción de las Solicitudes de Acceso al Sistema (SAS) y de la entrega de cuentas a los usuarios de La Municipalidad de Puente Piedra.

7. Los jefes inmediatos, serán los responsables de solicitar el alta, baja y/o modificación de opciones de las cuentas del personal a su cargo.

8. Los usuarios deberán dar conformidad de la recepción de la cuenta y clave de acceso solicitadas.

VI. INSTRUCCIONES:

1. Marco general de las cuentas de acceso

1.1 Todas las cuentas de acceso deberán ser creadas tomando en consideración los perfiles que se definan para cada aplicación.

1.2 La generación de claves deberá ser en forma automática.

1.3 La entrega de cuentas será utilizando medios electrónicos.

2. De la solicitud de cuentas de acceso

2.1 Toda cuenta de acceso debe ser solicitada mediante la presentación de la SAS a través de la Gerencia de Informática y Gobierno Electrónico, de acuerdo al procedimiento vigente, debiendo adjuntarse anexos que detallen el acceso solicitado y el sustento del mismo.

2.2 Las SAS deberán ser remitidas a las siguientes áreas:

Usuarios	**Área a remitir**
Personal de la Municipalidad de Puente Piedra	Helpdesk del área que les corresponde

2.3 La información reportada por la Oficina de los jefes responsables de cada área, según lo indicado en el numeral 5 del rubro VI, será atendida por la Gerencia de Informática y Gobierno Electrónico y corresponderá generarle o dar de baja a las cuentas de acceso básico. En cuanto a las bajas de cuentas de otros aplicativos, estas serán atendidas por cada área encargada, de acuerdo a lo indicado en el numeral 3.1. según corresponda.

2.4 Las cuentas de acceso del correo externo, servicio Internet, entidades externas, accesos remotos así como otros accesos especiales, se otorgaran de acuerdo a la respectiva normatividad vigente.

2.5 Podrán solicitar cuentas de acceso a los sistemas en producción:

a) Todo personal de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA con la autorización respectiva y según la normatividad vigente que corresponda.

b) Excepcionalmente, el personal que se encuentre realizando prácticas pre-profesionales y profesionales, con el sustento del caso y autorización respectiva. En el caso de acceso al correo electrónico, únicamente se otorgara acceso al correo interno.

3. De la creación de cuentas y asignación de claves de acceso

3.1 De acuerdo a lo indicado en la SAS y el perfil correspondiente, el área encargado, según el siguiente detalle, generará la cuenta de acceso.

Usuarios	**Área encargada**
Personal de la Municipalidad de Puente Piedra.	La Gerencia de Informática y Gobierno Electrónico

Para tal fin, la Gerencia de Informática y Gobierno Electrónico, coordinara con dichas áreas, la elaboración y estandarización del Instructivo de Creación de Cuentas.

3.2 En caso de olvido de la clave de acceso, el usuario debe solicitarla mediante una Solicitud de HelpDesk.

4. De la entrega de cuentas y asignación de claves de acceso

4.1 Al momento de recibir sus cuentas, los usuarios deberán cambiar la clave de acceso inicial por una personalizada tomando en consideración las recomendaciones del numeral 5 del presente rubro.

4.2 El usuario debe dar la conformidad de la recepción de su cuenta de acceso. Cada área encargada de esta entrega, solicitara esta conformidad.

4.3 Excepcionalmente en caso de solicitudes masivas, la conformidad de recepción de cuentas, deberá ser otorgada por la persona designada para el envío de la solicitud, quien mantendrá el control respecto a la asignación individual de las cuentas generadas.

5. De la construcción de claves de accesos seguras

La clave de acceso:

a. Debe ser privada y conocida solo por el titular de la cuenta.

b. Debe ser secreta y no aparecer escrita en ningún papel o archivo.

c. Debe tener por lo menos seis caracteres, mientras más breve sea es más fácil descifrarla.

d. Debe estar compuesta de caracteres, números y símbolos.

e. Debe ser diferente para cada sistema.

f. No debe estar relacionada con sus datos personales, como la fecha de su cumpleaños, nombre de su esposo(a), hijos, marca de su automóvil o documento de identidad.

g. Debe ser cambiada inmediatamente por el usuario al recibirla por primera vez.

6. Del correcto uso de las cuentas

6.1 las cuentas que se asignan son únicas, confidenciales y personales, por lo tanto no deben ser compartidas y toda acción que se realice con ellas, es responsabilidad del usuario titular.

6.2 Las claves de acceso deben ser cambiadas cada 6 meses, tomando en consideración las recomendaciones del numeral 5 del presente rubro. En el caso de cuentas

genéricas, la Gerencia de Informática y Gobierno Electrónico será el responsable de realizar dicha acción.

6.3 Las cuentas de acceso deben ser usadas única y exclusivamente para actividades relacionadas con el cumplimiento de las funciones asignadas por la institución, tal y como se detalle en el SAS. Ninguna podrá ser usada para propósitos distintos, ilegales o no éticos.

6.4 De existir sospecha de mal uso de la cuenta de acceso, el usuario debe cambiar la clave de acceso y notificar a la Gerencia de Informática y Gobierno Electrónico como un incidente de Seguridad Informática.

7. De la administración de las cuentas de acceso a los sistemas de producción.

7.1 El encargado de la administración de cuentas que se generen en sus respectivas áreas, es la Gerencia de Informática y Gobierno Electrónico.

7.2 Las cuentas entregadas que no se utilicen por más de 30 días deben ser desactivadas por las áreas señaladas en el numeral 3.1 del presente rubro. Se emitirá un reporte de las cuentas que fueron desactivadas por este motivo, para ser entregado a los jefes de los usuarios dueños de dichas cuentas.

7.3 Los accesos a bases de datos son de uso restringido y serán otorgados únicamente con permiso de consulta. El personal de la Municipalidad de Puente Piedra podrá solicitar dicho acceso solo a las bases de datos de su área y a tablas específicas que permitan verificar la operatividad de las aplicaciones, las cuales deberán ser detalladas en el SAS.

7.4 El personal con el acceso señalado en el numeral 7.3, será responsable por todo proceso que se ejecute, verificando su correcta aplicación y cumplimiento con los lineamientos establecidos por las Gerencias y Sub Gerencias respectivas que aseguren la continuidad y disponibilidad de los servicios informáticos.

7.5 Las nuevas aplicaciones deben contar con mecanismos de control de acceso, los cuales permitan cerrar las sesiones de aquellos usuarios internos que habiendo accesado a determinado sistema no realicen o generen movimiento con su cuenta en un tiempo que debe determinarse para cada aplicación.

7.6 Con la finalidad de mantener actualizada la base de datos de cuentas, cada área encargada, señalada en el numeral 3.1 del presente rubro, emitirá reportes que serán enviados a todas áreas con la finalidad que los jefes respectivos, den conformidad a las cuentas que están asignadas a su personal o de lo contrario indiquen la baja correspondiente. Estos reportes serán generados cada 6 meses.

7.7 Las cuentas root, o administrador son de uso restringido y en caso se requiera, únicamente serán utilizadas por el personal de Gerencia de Informática y Gobierno Electrónico. Para tal fin la clave de acceso de dichas cuentas será asignada por

la Gerencia de Informática y Gobierno Electrónico. La clave de acceso será cambiada cada vez que las cuentas sean utilizadas.

8. De la modificación y baja de cuentas

8.1 Se podrá solicitar la modificación de una cuenta, respecto a al adición de opciones de acceso o Cambio de perfil. Esta modificación quedara sujeta a la solicitud del usuario según lo indicado en el numeral 2.1 del presente rubro.

8.2 La baja de una cuenta de acceso, la realizara el área encargada según numeral 3.1 del presente rubro y debe efectuarse de acuerdo a las siguientes condiciones:

a) A solicitud del usuario, siguiendo el procedimiento descrito en el numeral 2.1 del presente rubro.

b) Por licencia mayor a 30 días, renuncia o cese del trabajador.

c) Por traslado del trabajador a otra unidad organizacional, la que debe ser efectuada a solicitud del jefe del área de origen.

d) Si se llegara a constatar que alguna cuenta de usuario estuviera poniendo en peligro el buen funcionamiento de los sistemas informáticos o se sospeche sea algún intruso utilizando una cuenta ajena, la Gerencia de Informática y Gobierno Electrónico ejecuta dicha acción.

VII. NORMAS COMPLEMENTARIAS

1. Las nuevas aplicaciones a implementarse deberán contar con perfiles de acceso, los cuales serán coordinados con la Gerencia de Informática y Gobierno Electrónico considerando lo siguiente:

1.1 Todo sistema que pasa a producción debe tener definidos los grupos de perfiles por cada opción del Menú de Opciones por aplicativo. Por cada opción del aplicativo que acceda a una tabla debe registrarse en el perfil de tipo de acceso a dicha tabla: select, insert, update, o deleite. Debe acompañar a esta definición de perfiles un instructivo de Creación de cuentas en coordinación previa con la Gerencia de Informática y Gobierno Electrónico.

1.2 Los perfiles deben ser definidos bajo el esquema de grupos funcionales y detallando los permisos que tendrán sobre la diferentes tablas y por módulos.

1.3 En el caso de los sistemas en producción ya existentes y que no cuenten con perfiles definidos, estos deben ser implementados gradualmente, considerando las recomendaciones descritas en los numerales 1.1 y 1.2 de la presente Norma complementaria.

1.4 La asignación de perfiles de usuario a las cuentas de acceso es responsabilidad

de quien autoriza y solicita su creación.

2. En cuanto a las bajas de otros aplicativos mencionadas en el numeral 2.3 del rubro VII, serán derivadas por la Gerencia de Informática y Gobierno Electrónico al área encargada que corresponda según numeral 3.1 del mismo rubro, hasta que se implemente el mecanismo que permita que cada una de ellas pueda disponer de la información de su dependencia.

3. Lo mencionado en el numeral 3.1 del rubro VII, respecto al Instructivo de Creación de Cuentas, será ejecutado una vez que la Gerencia de Informática y Gobierno Electrónico releve información de las áreas encargadas de la Municipalidad de Puente Piedra.

4. En tanto se implemente el sistema automático de generación de claves de acceso señalado en el numeral 1.2 del rubro VII, continuaran vigentes los procedimientos de cada área encargada indicadas en el numeral 3.1 del mismo rubro.

5. En tanto se implemente la entrega de cuentas vía medios electrónicos, establecida en el numeral 3.1 del rubro VII, esta se realizara de acuerdo a los procedimientos establecidos por las áreas encargadas.

Usuarios	**Área encargada de la entrega**
Personal de la Municipalidad de Puente Piedra	Helpdesk del área al que corresponda

6. Los usuarios deben cambiar las claves iniciales tal como se indica en el numeral 4.1 del rubro VII, hasta que se implementen mecanismos en los sistemas que permitan que soliciten automáticamente el cambio cuando se ingresa por primera vez.

7. El mecanismo del control que se menciona en el numeral 7.2 del rubro VII, será implementado gradualmente, conforme sea desarrollado por parte de la Gerencia de Informática y Gobierno Electrónico.

8. La Gerencia de Informática y Gobierno Electrónico deben buscar soluciones que permitan adecuar a las aplicaciones existentes, los mecanismos de control que mencionan en el numeral 7.5 del rubro VII.

CAPITULO V

POLÍTICAS Y NORMAS PARA EL SERVICIO INTERNET.

1. FINALIDAD:

Establecer las políticas y normas que se regirán para el acceso al servicio Internet y del uso adecuado por parte de los usuarios.

2. ALCANCE:

A todo el personal de la MUNICIPALIDAD DE PUENTE PIEDRA.

3. BASE LEGAL:

- Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI"

  esta norma peruana de seguridad de la información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, monitorear, operar, mantener y mejorar un efectivo sistema de gestión de seguridad de la información ISMS.

4. POLITICAS PARA EL USO DEL SERVICIO DE INTERNET

4.1 El uso del servicio Internet será únicamente para fines Institucionales.

4.2 El acceso al servicio Internet para el personal que labora dentro de la Municipalidad de Puente Piedra será otorgado automáticamente.

4.3 El personal no comprendido en el numeral 6.2 y los practicantes podrán tener acceso al servicio con la autorización del Jefe responsable o Gerente según sea el caso.

4.4 El Hardware, Software y redes de comunicación que soportan al servicio Internet, son patrimonio Institucional, por lo que la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA, en concordancia con su política informática institucional se reserva el derecho de introducir los elementos de registro y control que estime conveniente para garantizar la seguridad del sistema informático.

4.5 Todo acceso o revocatoria será solicitado con una Solicitud de Acceso al Sistema (SAS).

4.6 Cualquier acción que vaya en contra de lo estipulado en la presente política de seguridad informática será sancionada por la Sub Gerencia de Recursos Humanos de la Municipalidad de Puente Piedra en concordancia con las disposiciones legales y reglamentarias vigentes.

5. RESPONSABILIDADES:

5.1 La Gerencia de Informática y Gobierno Electrónico es la responsable de:

a. Implementar y administrar la infraestructura y funcionamiento del servicio Internet.

b. Velar por el óptimo rendimiento y funcionamiento de los equipos que brindan el servicio Internet, así como el tráfico del enlace.

c. Implementar en coordinación con la Gerencia de Informática y Gobierno Electrónico las recomendaciones de seguridad Informática establecidas.

d. Desarrollar y mantener actualizados los instructivos técnicos que correspondan a la Plataforma Internet.

e. Recibir las Solicitudes de Acceso al Sistema (SAS) que los usuarios presenten, así como de efectuar las coordinaciones necesarias con las áreas involucradas para la atención de dichas solicitudes.

5.2 La Gerencia de Informática y Gobierno Electrónico es responsable de recomendar a las áreas competentes el uso de las herramientas y acciones para optimizar el uso del servicio Internet y obtener mayor seguridad en el servicio. Asimismo, de efectuar revisiones periódicas de los accesos y generar reportes con la finalidad de verificar el uso del servicio, en caso de detectar un mal uso, comunicar a las jefaturas inmediatas de los usuarios infractores de ser necesario se revocará o suspenderá el servicio.

5.3 La Gerencia de Informática y Gobierno Electrónico a través de sus revisiones periódicas del uso de servicio de internet. Podrá proponer el filtrado de determinadas direcciones que atenten contra la seguridad y/o disponibilidad del servicio.

5.4 La Sub Gerencia de Recursos Humanos de la MUNICIPALIDAD DE PUENTE PIEDRA es responsable de comunicar a la Gerencia de Informática y Gobierno Electrónico, dentro de los plazos señalados en la presente política, todos los movimientos de personal respecto a ceses y cambio del personal considerando en el numeral 6.2.

5.5 La Gerencia de Informática y Gobierno Electrónico, es responsable de coordinar y evaluar los sitios web a incorporar en Enlaces de Interés para el acceso libre a través de la Intranet.

5.6 Los Jefes inmediatos de los usuarios con cuenta de acceso al servicio Internet son los responsables de comunicar y solicitar, en el transcurso de las primeras 24 horas, la revocatoria del servicio en los siguientes casos: traslados (cambio de unidad organizacional), retiros de la Institución y licencias mayores a 30 días.

5.7 Todos los usuarios son responsables del cumplimiento de las políticas, normas y procedimientos establecidos en la presente circular, así como de todo acceso que se efectué en su cuenta.

6. INSTRUCCIONES

6.1 De la autorización de accesos

Todo acceso al servicio Internet, excepto del personal considerado en el numeral 6.2, se solicitara a través del SAS mediante la solicitud de Acceso al Sistema debidamente llenada, con el sustento del caso y con la autorización del Jefe área o gerente según sea el caso.

6.2 De las revocatorias de los accesos

6.2.1 Cuando ocurra el cese en el cargo del personal considerando en el numeral 6.2, Sub Gerencia de Recursos Humanos remitirá a la Gerencia de Informática y Gobierno Electrónico, el movimiento del personal en esa situación, dentro de las 24 horas de ocurrido el hecho, a fin se proceda desactivar los accesos al servicio Internet dentro de las 24 horas de recibida la Información.

6.2.2 Al inicio y termino de una licencia mayor de 30 días, Sub Gerencia de Recursos Humanos de la Municipalidad de Puente Piedra remitirá a la Gerencia de Informática y Gobierno Electrónico el movimiento del personal en esa situación dentro de las 24 horas de ocurrido el hecho, a fin de que proceda a revocar o activar los accesos según corresponda.

6.2.3 Para los casos señalados en el numeral 7.6, los jefes inmediatos presentaran la SAS correspondiente.

6.3 De la Administración del Servicio de Internet

6.3.1 La Gerencia de Informática y Gobierno Electrónico podrá deshabilitar temporalmente los accesos a recursos de Internet que resten la performance de la plataforma Internet o por mal uso.

6.3.2 La función de administración de la plataforma Internet está a cargo de la Gerencia de Informática y Gobierno Electrónico.

6.3.3 La función de administración de los servidores de la plataforma Internet está a cargo de la Gerencia de Informática y Gobierno Electrónico.

6.3.4 Gerencia de Informática y Gobierno Electrónico llevara un registro de las descargas de Software que efectué de acuerdo a los requerimientos autorizados.

6.3.5 Para la administración y control de los accesos a Internet se considerara los lineamientos técnicos que la Gerencia de Informática y Gobierno Electrónico recomienda, así como lo precisado, en la presente circular.

6.4 Del uso del Internet

6.4.1 El servicio de Internet será revocado o suspendido por mal uso del servicio, en función a la gravedad y/o reincidencia de la falta.

6.4.2 El acceso a los servicios de correo no Institucional que se brindan a través de Internet que queda autorizado para Gerentes y Sub Gerentes así como para el resto de usuarios será permitido excepcionalmente por necesidad de contingencia y operatividad del negocio, así como a otra categoría considerada como no institucional por necesidad estrictamente de investigación. Esta solicitud de excepción autorizada será por el jefe de area que corresponda.

6.4.3 Para el uso de software denominado "freeware" o "shareware" a través de Internet, las cuales son accesibles vía "download".

6.4.4 La descarga deberá efectuarse considerando los lineamientos técnicos que indique la Gerencia de Informática y Gobierno Electrónico, los mismos serán difundidos a través de la Intranet.

La solicitud de descarga se presentara en el formato de Comunicación de Utilización de Descarga de Software.

6.4.5 La cuenta de acceso con autorización de servicio de Internet es de uso único del usuario a quien se le otorga dicho acceso, siendo responsable por toda acción que se realice con ella.

6.4.6 La necesidad de acceso a Internet para servidores en producción, tales como Windows Server, Unix, etc., será autorizado por la Gerencia de Informática y Gobierno Electrónico, debiendo estar fundamentado y delimitado a la funcionalidad que posean dichos equipos.

6.5 Prohibiciones en el uso de Internet

Está prohibido:

6.5.1 Instalar software del tipo proxies u otros similares que permitan que usuarios no autorizados tengan salida a Internet.

6.5.2 Facilitar u ofrecer a otras personas su cuenta de acceso al servicio Internet.

6.5.3 Utilizar la cuenta Internet de otro usuario.

6.5.4 Acceder a sitios Web considerados por la Alta Dirección como categorías no Institucionales, las mismas que serán difundidas por la Gerencia de Informática y

Gobierno Electrónico para conocimiento de todos los usuarios.

6.5.5 Utilizar el servicio Internet para difundir información confidencial a receptores no autorizados.

6.5.6 Congestionar el servicio Internet mediante la descarga desautorizada de archivos con capacidades superiores a las establecidas o mediante el envío de mensajes prohibidos.

6.5.7 Utilizar el servicio para efectuar carga ("upload") de información en servidores que se encuentren en Internet.

7. ANEXOS:

01 Glosario de términos

ANEXO 01

GLOSARIO DE TERMINOS

DOWNLOAD.- Descargar, bajar, Transferencia de información desde Internet a una computadora.

FREEWARE.- Software de dominio público, es decir, el que no es comercial y puede distribuirse gratuitamente, aunque no se pueda modificar, pues el autor mantiene los derechos de copyright.

INTERNET.- Red de redes, Sistema mundial de redes de computadoras interconectadas. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

PÁGINA WEB.- Documento electrónico que contiene información específica de un tema en particular y que es almacenado en algún sistema de cómputo que se encuentre conectado a la red mundial de información denominada Internet. Este documento puede ser consultado por cualquier persona que se conecte a esta red mundial de comunicaciones siempre y cuando cuente con los permisos apropiados para hacerlo.

PLATAFORMA INTERNET.- Conjunto equipos informáticos y de telecomunicaciones que permiten el acceso a los usuarios a la red internet.

PROXIES.- Son ciertos software o programas que permiten otorgar accesos a Internet a maquinas de la red interna que no disponen de este servicio.

SERVIDOR.- Computadora central de un sistema de red que provee servicios y programas a otras computadoras.

SERVIDOR WEB.- Servidor que aloja las paginas estáticas o aplicaciones.

SHAREWARE.- Software protegido por las leyes de copyright, que se encuentra disponible gratuitamente durante cierto tiempo para su evaluación por el usuario. Al pasar dicho tiempo, el programa expira y no podrá volver a ser utilizado.

SITIO WEB.- Es un conjunto de archivos electrónicos y páginas web referentes a un tema en particular, que incluye una página inicial de bienvenida, generalmente denominada "home page", con un nombre de dominio y dirección en Internet específicos.

CAPÍTULO VI

POLÍTICAS Y NORMAS PARA EL SERVICIO DEL CORREO ELECTRÓNICO INSTITUCIONAL.

I. FINALIDAD:

Implantar las políticas y normas que regirán la gestión y uso del correo electrónico institucional de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA.

II. ALCANCE:

A todo el personal de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA.

III. BASE LEGAL:

- Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI"

  esta norma peruana de seguridad de la información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, monitorear, operar, mantener y mejorar un efectivo sistema de gestión de seguridad de la información ISMS.

  Ley Nª 27269, "Ley de firmas y certificadas digitales" y de su reglamento aprobado mediante Decreto Supremo 019-2002-JUS.

IV. RESPONSABILIDADES:

1. De la Gerencia de Informática y Gobierno Electrónico

1.1 La Gerencia de Informática y Gobierno Electrónico es responsable de implementar la infraestructura y administrar el funcionamiento del servicio de Correo Electrónico Institucional en concordancia con las normas de seguridad informática vigentes.

1.2 La Gerencia de Informática y Gobierno Electrónico es responsable de atender los requerimientos de usuario por problemas con el correo electrónico, solicitudes de envío de mensajes a través del Administrador del WebServer, así como impartir instrucciones y recomendaciones a los usuarios sobre el uso del Correo Electrónico Institucional.

1.3 La Gerencia de Informática y Gobierno Electrónico es responsable de establecer las políticas y gestionar las herramientas necesarias para la seguridad en el uso del correo electrónico. Asimismo de efectuar revisiones periódicas, preservando la confidencialidad con la finalidad de detectar el mal uso del servicio y comunicarlo al jefe inmediato del usuario involucrado y de ser el Caso, a Sub Gerencia de Recursos Humanos según corresponda par las acciones disciplinarias o la suspensión del servicio, debiendo llevar un registro de los mismos.

2. De la Sub Gerencia de Recursos Humanos de la Municipalidad Distrital de Puente Piedra

Es responsable de comunicar a la Gerencia de Informática y Gobierno Electrónico dentro de los plazos establecidos, la información actualizada a la que se refiere los numerales 1.6, 1.7 y 1.8 del rubro VII y autorizar las comunicaciones señaladas en el numeral 1.2 del rubro VII de la presente circular.

3. De los jefes inmediatos

Son responsables de comunicar y solicitar mediante la Solicitud de Accesos al Sistema la cual deberá ser tramitada durante las 24 horas, la baja de cuenta de un usuario por renuncia o cese, o restricciones del servicio tanto par correo externo, acceso desde el exterior y/ o filtros de correo. Asimismo comunicar a la dirección de Recursos Humanos el mal uso del servicio del personal a su cargo.

4. De los Usuarios

Son responsables de toda actividad que se realice con la cuenta de correo electrónico que le ha sido asignada por la Institución; así como, del cumplimiento de las políticas, normas y procedimientos establecidos en la presente circular.

V. POLITICAS PARA EL SERVICIO DE CORREO ELECTRONICO INSTITUCIONAL

1. El correo electrónico Institucional es el medio oficial de comunicación e intercambio de información que brinda la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA a sus trabajadores con el fin de facilitar sus labores en beneficio de la Institución, excepcionalmente lo otorga en forma restringida y temporal a los practicantes y personas externas a la Institución, con el fin de facilitar el cumplimiento de lo establecido en su plan de prácticas o plan de trabajo según corresponda.

2. Para el intercambio de información entre instituciones y notificaciones oficiales a los contribuyentes, se deberá propender a la utilización del correo electrónico seguro para lo cual la Gerencia de Informática y Gobierno Electrónico podrá recomendar el uso de firma y certificados digitales y/o otros mecanismos y procedimientos de seguridad informática y verificación de adecuados.

3. Los trabajadores de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA deben utilizar el servicio exclusivamente para el desempeño de sus labores. Los practicantes y personas externas a la institución que excepcionalmente dispongan del servicio lo utilizaran exclusivamente para los fines indicados en el numeral 1 del presente rubro.

4. El nombre de la cuenta de correo que identifique a cada trabajador de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA está formado por la letra inicial de su primer nombre seguido inmediatamente por su apellido paterno y ligado

por el símbolo @ al nombre de dominio **Municipalidad Distrital de Puente Piedra.gob.pe**. Dicha cuenta estará asociada al nombre del buzón de correo que llevara el nombre completo del trabajador de acuerdo al padrón que nos brinda la Sub Gerencia de Recursos Humanos.

En caso de surgir dos o más construcciones similares, se agregara los caracteres del apellido materno hasta que sean diferentes.

Para los practicantes se seguirá el mismo criterio de construcción antecedido del término "prac y para el personal de entidades externas por Convenio o Contrato de Servicios se crearan las cuentas tal y como se describe en el primer párrafo y la estructura de su dirección de correo será cuenta rol entidad @ dominio y se visualizara el nombre del usuario precedido por el rol y la entidad a la que representa.

5. Las cuentas de correo también pueden otorgarse a nombre de una unidad organizacional o de una función específica designándose un responsable de la cuenta quien será autorizado por el jefe inmediato de la unidad organizacional solicitante. La construcción del nombre de la cuenta para estos casos así como su asociación con el buzón de correo (comunitario o institucional) seguirá un criterio estandarizado, el cual será determinado por la Gerencia de Informática y Gobierno Electrónico.

6. El servicio de **correo electrónico interno** para el personal de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA con contrato indeterminado, contrato especifico o practicantes no requiere de la presentación de una solicitud de acceso al sistema se otorga en forma inmediata previa comunicación de la Sub Gerencia de Recursos Humanos a la Gerencia de Informática y Gobierno Electrónico. A personas externas por Convenio o Contrato de Servicios se le otorgara previa solicitud de acceso al sistema y con autorización del Jefe de la Unidad Organizacional donde se encuentra adscrito.

7. El Hardware, Software y redes de comunicación que soportan el servicio de correo electrónico son patrimonio Institucional, por lo que la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA, en concordancia con su Política de Seguridad Informática Institucional, se reserva el derecho de implementar los elementos de registro y control que estime conveniente para garantizar la seguridad de su sistema informático

8. La cuenta "Administrador del WebServer" es la única autorizada a remitir mensajes para conocimiento de todo el personal de la Institución. Los lineamientos para la solicitud de envío de dichos mensajes serán definidos por la Gerencia de Informática y Gobierno Electrónico y publicada en la Intranet institucional para conocimiento de todos los usuarios.

9. El correo Electrónico Institucional permitirá listas de Distribución con el fin de remitir comunicaciones a una unidad organizacional o a un grupo de funcionarios.

   Las listas se crearan según la Estructura Orgánica de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA y podrán ser utilizadas por el funcionario principal de cada unidad organizacional y adicionalmente con máximo dos responsables que el autorice:

ÓRGANO DE GOBIERNO

- Consejo Municipal

ÓRGANO DE ALTA DIRECCIÓN

- Alcaldía
- Gerencia Municipal

ÓRGANOS CONSULTIVOS DE COORDINACIÓN

- Consejo de Coordinación Local Distrital
- Junta de Delegados Vecinales Comunales
- Comité Distrital de Seguridad Ciudadana
- Comité Distrital de Defensa Civil

ÓRGANO DE CONTROL

- Órgano de Control Institucional

ÓRGANO DE ASESORAMIENTO

- Gerencia de Asesoría Jurídica

ÓRGANOS DE APOYO

- Procuraduría Pública Municipal
- Secretaria General
- Gerencia de Participación Vecinal
- Gerencia de Administración, Finanzas y Planeamiento
  - Subgerencia de Planeamiento y Presupuesto
  - Subgerencia de Logística
  - Subgerencia de Contabilidad

- Subgerencia de Tesorería
- Subgerencia de Recursos Humanos

❖ Gerencia de Administración Tributaria

- Subgerencia de Registro y Fiscalización Tributaria
- Subgerencia de Recaudación y Ejecutoria Coactiva

❖ Gerencia de Informática y Gobierno Electrónico

ÓRGANOS DE LÍNEA

❖ Gerencia de Desarrollo Urbano y Económico

- Subgerencia de Catastro y Planeamiento Urbano
- Subgerencia de Obras y Habilitaciones Urbanas
- Subgerencia de Desarrollo Económico
- Subgerencia de Defensa Civil

❖ Gerencia de Seguridad Ciudadana y Fiscalización

- Subgerencia de Serenazgo
- Subgerencia de Fiscalización

❖ Gerencia de Desarrollo Humano

- Subgerencia de Desarrollo Educativo y Social
- Subgerencia de Juventudes
- Subgerencia de Programas Alimentarios

❖ Gerencia de Gestión Ambiental

- Subgerencia de Limpieza Pública
- Subgerencia de Parques y Jardines

❖ Subgerencia de Atención al Ciudadano

❖ Gerencia de Inversiones Públicas

- Subgerencia de Estudios y Proyectos

ÓRGANOS DESCONCENTRADOS

- ❖ Agencia Municipales

10. El uso del servicio de correo podrá ser suspendido en forma inmediata al usuario, ante la detección de acciones que evidencien su mal uso y/o representen riesgo para la seguridad de la información.

11. El acceso desde el exterior al servicio del correo electrónico Institucional, se rige bajo los mismos lineamientos y normatividad definidos para Accesos remotos.

12. De acuerdo a lo establecido en el inciso (g) del artículo 39, del reglamento Interno de Trabajo, el trabajador tiene la obligación de cumplir con las normas referidas al uso adecuado del correo electrónico. El incumplimiento de lo estipulado en la presente circular constituye falta disciplinaria sujeta a sanción.

VI. INSTRUCCIONES:

1. De las solicitudes de accesos y solicitudes para levantar restricciones

1.1 las solicitudes para el otorgamiento y/o revocación del servicio de correo electrónico externo acceso desde el exterior, así como la creación desactivación o el cambio de administrador de las casillas comunitarias, casillas institucional y carpetas públicas, se efectúa mediante la Solicitud de Acceso al Sistema **(SAS)** debidamente llenada, con el sustento del caso y con el V°B° de los funcionarios responsables.

1.2 Las solicitudes de envío de mensajes para todo el personal de la institución a través del Administrador del WebServer, se efectúa mediante la Solicitud de Atención al Usuario (SAU), la cual deberá contar con la autorización del Gerente o Sub Gerente que elaboro dicha comunicación, siendo responsables del contenido y forma de los mensajes a difundirse.

1.3 La atención de requerimientos por problemas de acceso con el correo electrónico se efectúa mediante la Solicitud de Atención Helpdesk **(SHD).**

1.4 Excepcionalmente cuando exista la necesidad por interés institucional de recibir y/o enviar mensajes con información que exceda los tamaños de envío establecidos por la Gerencia de Informática y Gobierno Electrónico se podrá solicitar el levantamiento de la restricción con el sustento del caso a través de una SAS autorizada por el Gerente o Sub Gerente, según corresponda.

1.5 Para levantar la restricción mencionada en el numeral 4.1 del rubro VII de la presente política, se solicitara mediante una SAS, con el sustento del caso y Autorizado por el Gerente o Sub Gerente, según corresponda.

1.6 Cuando ocurran cambios en el Personal, Asesores de Alta Dirección y secretarias a las que se refiere el numeral 7 del rubro VI de la presente política, la Sub Gerencia de Recursos Humanos comunicara a través de una SAS a la Gerencia de Informática y Gobierno Electrónico el movimiento de personal en tal situación, dentro de las 48 horas de ocurrido el hecho a fin que esta proceda otorgar o desactivar el acceso al servicio del correo electrónico extremo dentro de las 24 horas de recibida la información. De igual modo con dicha información se actualizaran las listas de distribución correspondientes mencionadas en el numeral 11 del rubro VI.

1.7 Al inicio de una licencia mayor de 30 días, la Sub Gerencia de Recursos Humanos de la Municipalidad de Puente Piedra comunicara semanalmente a la Gerencia de Informática y Gobierno Electrónico el movimiento del personal en esa situación para que esta proceda generar la copia de seguridad del buzón y luego darle de baja. No están considerados los casos de comisiones de servicio.

1.8 Cuando ocurran incorporaciones bajas de personal o al término de una licencia mayor de 30 días la Sub Gerencia de Recursos Humanos comunicara a la Gerencia de Informática y Gobierno Electrónico el movimiento de personal en esa situación en forma semanal a fin de que proceda a otorgar habilitar o dar de baja según corresponda, el acceso al servicio de correo electrónico interno y asignar el buzón de correo electrónico.

1.9 El trabajador podrá solicitar a través de una SAS la corrección del nombre consignado en la libreta de direcciones del servicio del correo electrónico, en caso se haya generado con errores. Los datos a modificar deberán estar en concordancia con el registro del padrón de personal.

2. Del uso del servicio de correo

Los usuarios del servicio de correo electrónico institucional, deben:

2.1 crear un repositorio (carpeta personal) de mensajes en su estación de trabajo para transferir y almacenar los mensajes que residan en su casilla, los cuales requieran ser conservados a efectos de tener una eficiente administración.

2.2 Considerar que el envió de mensajes y archivos a través del servicio de correo electrónico debe ajustarse al Código de Ética, las políticas y reglamentos de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA.

2.3 Considerar de que cada carpeta publica tendrá un administrador de carpeta, cuya función es darle mantenimiento en cuanto a su contenido y accesos.

2.4 Acceder a su casilla de correo por lo menos dos (2) veces en el día para tomar

conocimiento de los mensajes recibidos, uno al inicio de la jornada laboral y el otro al final de la misma.

2.5 Dar buen uso y mantener la confidencialidad del contenido de las carpetas públicas.

2.6 Verificar cuidadosamente que los nombres del destinatario del mensaje que va enviar sean los correctos a fin de que estos no lleguen por error a destinos que no corresponden.

2.7 Cerrar o bloquear sus sesiones de Windows cuando se retire o ausente temporalmente de la PC de donde se accede al servicio.

2.8 Verificar y clasificar la información que transferirá de su casilla a su carpeta personal, quedando bajo su responsabilidad efectuar oportunamente la trasferencia de dicha información teniendo en consideración con determinada frecuencia se eliminaran los mensajes del servidor.

2.9 Facilitar las investigaciones relacionadas al mal uso del servicio del correo electrónico que tengan que ver con la seguridad informática.

2.10 Citar la fuente de origen y/o los autores de los documentos que se adjunten en el correo y que no son los propios, a fin de respetar los derechos de propiedad intelectual.

3. De las prohibiciones en el uso del servicio de correo

El usuario está prohibido de:

3.1 utilizar el servicio de correo electrónico institucional para fines distintos al desempeño de sus labores.

3.2 Facilitar u ofrecer a otras personas el uso de su cuenta y/o buzón del correo electrónico institucional.

3.3 Utilizar la cuenta de correo institucional de otro usuario.

3.4 Utilizar para el desempeño de sus funciones otros servicios de correos electrónicos que no sea el Oficial.

3.5 Difundir información confidencial o reservada dentro y/o fuera de la Municipalidad Distrital de Puente Piedra a receptores no autorizados.

3.6 Imposibilitar o dificultar el servicio del Correo Electrónico Institucional mediante mensajes que provoquen la congestión del mismo.

3.7 Suscribirse por internet, para fines no institucionales a listas de interés o grupos temáticos, tomando la dirección electrónica del correo asignada por la institución.

3.8 Enviar mensajes a foros de discusión listas de distribución y newgroups de internet que comprometan la información de la institución o violen las leyes del Estado Peruano.

3.9 Enviar mensajes de amenaza apología del terrorismo, esquemas de enriquecimiento piramidal o similar, racismo, propagación de virus, contenido pornográfico y cualquier otro de contenido impropio o lesivo a la moral.

3.10 Enviar mensajes para realizar negocios personales, apuestas o estafas.

3.11 Usar seudónimos u otros sistemas de ocultación de identidad. El destinatario debe conocer la identidad de la persona que envía el mensaje.

3.12 Enviar mensaje con publicidad y/o críticas personales que afecten la imagen institucional.

3.13 Enviar mensajes tomando el nombre de la institución o de alguna Unidad organizacional sin su autorización.

3.14 Transmitir rumores, cadenas de buenos deseos, mensajes de solidaridad no autorizados y alarmas de falsos virus informáticos

3.15 Enviar y/o intercambiar archivos ejecutables con extensión exe. Com. sys y otros similares, archivos con contenido de sonido y/o imágenes que no sean para fines institucionales.

3.16 Intercambiar software sin la respectiva licencia de uso, así como fomentar la piratería.

3.17 Utilizar el servicio del correo para cualquier actividad ilícita o maliciosa.

3.18 Deshabilitar las configuraciones de antivirus de la estación de trabajo (PC), relacionados al correo electrónico.

3.19 Retirar de la institución copia de los mensajes de correo electrónico enviados y/o recepcionados, para ser entregados a personas ajenas a la misma institución y/o hacer mal uso de ellos.

4. De las restricciones y excepciones de los mensajes

4.1. El envió y/o recepción de mensajes determinados dominios o direcciones podrán ser restringidos por:

a. La Sub Gerencia de Recursos Humanos al considerar que el contenido remitido no sea relevante y/o apropiado para la institución.

b. La Gerencia de Informática y Gobierno Electrónico ante situaciones que evidencien riesgo para la disponibilidad de servicio.

4.2 excepcionalmente por necesidad de contingencia y operatividad de negocio se podrá

hacer uso de forma eventual de otros servicios de correo electrónico los cuales se solicitaran de acuerdo a lo establecido en la normatividad vigente de uso de internet.

5. Responsabilidades específicas de la Gerencia.

5.1 De la Gerencia de Informática y Gobierno Electrónico:

a. Administrar la plataforma del servicio de correo electrónico institucional velando por su óptimo funcionamiento.

b. Velar que el software antivirus para servidores de correo y estaciones de trabajo estén actualizados y se activen de tal forma que se verifiquen todos los archivos aun los que se encuentren compactados siendo su acción por defecto eliminar el virus automáticamente

c. Verificar la presencia de virus en los servidores de correo proceder a eliminarlos inmediatamente.

d. Determinar en función la infraestructura y capacidad técnica instalada, el tamaño del buzón de correo electrónico por usuario, tamaño de cada personal, tamaño de los mensajes enviados y/o recibidos tanto a nivel interno como externo, así como, el tiempo de vigencia para los mensajes en el servidor, los mismos que serán difundidos a través de la Intranet Institucional.

e. Configurar el bloqueo de mensajes que exceden los límites de capacidad de envío/recepción normados, mediante el uso de mecanismo de verificación del tráfico de red en los servicios de correo.

f. Efectuar la generación baja y desactivación de cuentas de usuario y movimiento de los buzones de correo.

g. Efectuar los respaldos de seguridad de todos los mensajes recibidos y/o enviados del servidor de correo electrónico institucional considerando para ello lo establecido sobre la generación y custodia de los respaldos informáticos institucionales, así como, lo establecido en el numeral 1.8 del rubro VII del presente capitulo.

h. Ejecutar el proceso de eliminación de los mensajes del servidor de correo según la frecuencia que la Gerencia Informática y Gobierno Electrónica defina.

i. Velar por el óptimo funcionamiento de la plataforma telecomunicaciones la cual garantice la disponibilidad del servicio de correo.

j. Administrar y configurar el software de bloqueos destinados a la restricción de mansajes mencionados en el numeral 4.1 del rubro VII del presente capitulo.

k. Atender las solicitudes para levantar las restricciones señaladas en el numeral 1.5 del rubro VII del presente capitulo.

VII. NORMAS TRANSITORIAS Y COMPLEMENTARIAS

1. En tanto la Gerencia Informática y Gobierno Electrónica automatice la entrega de cuentas mencionada en el numeral 1.1 del rubro V, la entrega de cuentas y claves de los usuarios.

2. En tanto culmine el proceso de migración, se actualizaran gradualmente las cuentas ya existentes para dar cumplimiento a los numerales 4 y 5 del rubro VI.

3. En relación con lo normado en el literal b) del numeral 5.1 del rubro VII de la presente circular la Gerencia de Informática y Gobierno Electrónico implementara en forma gradual la ejecución de los respaldos mencionados.

4. Se efectuara gradualmente la actualización de los registros de los buzones de correo que se estipula en el literal a. del numeral 5.1 del rubro VII de la presente circular.

VIII. ANEXOS:

01 Glosario de Términos

GLOSARIO DE TERMINOS

Buzón de correo: Espacio en el disco del servidor de correo asignado a una cuenta del sistema operativo de red, donde residen los mensajes recibidos y enviados por el titular de la misma.

Buzón de correo comunitario: Casilla que se asigna para el uso de un grupo funcional, temático, organizacional, etc.

Buzón de correo institucional: Casilla de carácter institucional que se asigna a los trabajadores para la comunicación con entidades o personas externas.

Carpeta pública: Repositorio donde se puede de una manera sencilla y efectiva recopilar, organizar y compartir información con otras personas de un equipo de acuerdo al permiso otorgado por el administrador. Las carpetas públicas también pueden utilizarse para almacenar elementos como calendarios y contactos compartidos por dos o más personas.

Carpeta Personal: Espacio en el disco del computador de un usuario para conservar los mensajes y archivos transferidos desde su casilla postal.

Correo electrónico (e-mail): Todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión de computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico (ley 28493).

Correo externo: Es el correo electrónico que permite al personal de MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA, realizar el intercambio electrónico de mensajes y documentos con instituciones o personas externas.

Correo interno: Es el correo electrónico que permite al personal de la MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA realizar el intercambio electrónico de mensajes y documentos dentro de la red MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA.

Dominio: Conjunto de caracteres que identifica un sitio de la red accesible por un usuario.

Hardware: Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman un ordenador incluidos sus periféricos.

Lista de distribución: Lista que contiene una relación de buzones de correo cuya finalidad es agrupar usuarios para realizar envíos múltiples con una sola dirección.

Lista de interés. Grupo de discusión electrónica que permite mediante la distribución automática de correos electrónicos (e-mail) comentar, intercambiar y discutir puntos de vista sobre algún tema en particular.

Personas externas. Personas sin vínculo laboral con MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA que realizan labores dentro de las instalaciones de MUNICIPALIDAD DISTRITAL DE PUENTE PIEDRA como consultores, comisiones especiales de otras entidades, convenios y otros.

Respaldo: Copia de los datos de un archivo o base de datos en un soporte que posibilite su recuperación.

Servidor de correo: Es el computador que administra el servicio de correo electrónico y el envío de mensajes entre las casillas postales.

Software: Conjunto de instrucciones que ordenan al procesador que ejecute acciones y/o operaciones especificas.

SAS: Solicitud de acceso al sistema. Formato electrónico establecido por la Gerencia de Informática y Gobierno Electrónico que permite debidamente llenado y autorizado (visado) por los niveles jerárquicos correspondientes, solicitar entre otros el acceso o la revocación de acceso determinado sistema informático.

SHD: Solicitud de atención Helpdesk.- Formato electrónico establecido por la Gerencia de Informática y Gobierno Electrónico, que permite solicitar entre otros la atención por problemas de acceso con el correo electrónico.

SAU: Solicitud de atención a usuarios.- Formato electrónico establecido por la Gerencia de Informática y Gobierno Electrónico que permite solicitar entre otros, el envío de comunicados o mensajes al personal a través del Administrador del WebServer.