Municipalidad Provincial
de Huaylas - Caraz

RESOLUCIÓN DE ALCALDÍA N° 324-2015/MPHy

Caraz, 16 NOV 2015

VISTOS, El Informe Nº 088-2015-MPHy-Cz/06.11 de la Unidad de Tecnologías de la Información; y,

CONSIDERANDO:

Que, de conformidad con lo dispuesto en el Artículo II del Título Preliminar de la Ley Orgánica de Municipalidades Nº 27972, los gobiernos locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia. La autonomía que la Constitución política del Perú, establece para las Municipalidades radica en la facultad de ejercer de gobierno, administrativo y administración, con sujeción al ordenamiento jurídico;

Que, la serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), la serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI); y la ISO/IEC 27001, es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. ¬ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información;

Que, mediante Informe Nº 088-2015-MPHy-Cz/06.11, el Jefe de la Unidad de Tecnologías de la Información, dirigiéndose al Secretario General, pone en conocimiento que, se adjunta las Políticas y Normas de Seguridad de la Información, que tiene como finalidad dar a conocer a los usuarios lo relacionado a los servicios de Tecnologías de la Información, para proteger adecuadamente los activos tecnológicos y la información de la Municipalidad Provincial de Huaylas; para ello, se ha tenido en cuenta la serie de normas internacionales ISO/IEC 27000, que contiene las mejores prácticas recomendadas en Seguridad de la Información, que en nuestro país se dan en la Norma Técnica Peruana NTP – ISO/IEC 17799:2007 y la ISO/IEC 27001:2008;

Que, mediante Decreto de Alcaldía Nº 017-2013/MPHy, se Aprobó la Directiva Nº 003-2013/MPHy-CZ., sobre "POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA" de la Municipalidad Provincial de Huaylas;

SG MPH-Caraz V°B° SECRETARIA GENERAL

GM MPH-Caraz V°B° Ing. Tania C. García Perez GERENTE MUNICIPAL

ALCALDE MPH - Caraz V°B° Renson Martinez Canchumani ALCALDE

Estando a las consideraciones expuestas en el inciso 6) del Artículo 20º de la Ley Orgánica de Municipalidades N° 27972;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR LAS POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE HUAYLAS, la misma que forma parte de la presente resolución.

ARTÍCULO SEGUNDO.- DEJAR SIN EFECTO toda norma que se opongan en la presente resolución.

ARTÍCULO TERCERO.- DISPONER a la Gerencia Municipal, Secretaría General, a través de la Unidad de Tecnologías de la Información, el fiel cumplimiento de la presente resolución.

ARTÍCULO CUARTO.- ENCARGAR a la Secretaría General la notificación de la presente Resolución, conforme a ley.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

SG MPH-Caraz V°B° SECRETARIA GENERAL

GM MPH-Caraz V°B° Tania C. Garcia Perez GERENTE MUNICIPAL

MUNICIPALIDAD PROVINCIAL DE HUAYLAS CARAZ
ALCALDE CARAZ
Renson Martinez Canchumani
ALCALDE PROVINCIAL

MUNICIPALIDAD PROVINCIAL DE HUAYLAS

POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

Contenido

I. Intención

La Unidad de Tecnologías de Información, en adelante Unidad de TI, con el presente documento tiene como finalidad dar a conocer las Políticas y Normas de Seguridad de la Información que deberán observar los usuarios de servicios de Tecnologías de la Información, para proteger adecuadamente los activos tecnológicos y la información de la Municipalidad Provincial de Huaylas, en adelante MPHy.

II. Introducción

La serie de normas ISO/IEC 27000, publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), que contiene las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Una de estas series es la ISO/IEC 27002, que fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.

Se ha tenido en cuenta para su elaboración la Norma Técnica Peruana según Resolución Ministerial Nº 246-2007-PCM, que emitió la "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" y la "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad, sistema de Gestión de Seguridad de la Información. Requisitos".

En este sentido "La Norma Técnica Peruana ISO/IEC 17799:2007", se emite para ser considerada en la implementación de estrategias y planes de seguridad de la información de las Entidades Públicas.

La NTP-ISO/IEC 17799, que es el descenso de la norma ISO 27002:2005 en el escenario peruano, es ideal para tomarse como base para el desarrollo de los procedimientos que se proponen.

La NTP fue redactada para que fuera flexible y no induce a las organizaciones que la cumplan al pie de la letra en su elaboración, se deja a estas dar una solución de seguridad de acuerdo a sus necesidades.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos Normas que consideran los siguientes puntos:

- Seguridad de Recursos Humanos.
- Seguridad Física y del Entorno.
- Gestión de Comunicaciones y Operaciones.
- Control de Accesos.
- Cumplimiento.

III. Disposiciones Generales

Ámbito de aplicación y Fines:

Las Políticas y Normas de Seguridad de la Información tienen por objeto establecer medidas técnicas y de organización de las Tecnologías de la Información y de las personas que interactúan haciendo uso de los servicios informáticos que proporciona la MPHy y contribuyendo con la función informática a la mejora y cumplimiento de metas institucionales.

Es aplicable a los usuarios de servicios de las Tecnologías de la Información, adscritos a la MPHy.

De igual forma es una herramienta que:

- Difunde las Políticas y Normas de Seguridad Informática a todo el personal de la MPHy.
- Asegurará mayor integridad, confidencialidad y confiabilidad de la información generada por la MPHy, al personal, los datos, el hardware y software disponibles.
- Minimiza los riesgos en el uso de las Tecnologías de Información.

Frecuencia de Evaluación de las Políticas:

Las políticas tendrán una revisión semestral, o según sea el caso, para efectuar, actualizaciones, adecuaciones y/o modificaciones basadas en la experiencia y lecciones aprendidas.

Beneficios:

Las Políticas y Normas de Seguridad de la Información establecidas dentro de este documento son la base para la protección de los activos tecnológicos y la información de la MPHy.

1. Seguridad de Recursos Humanos

Política:

Todo usuario de bienes y servicios informáticos al ingresar como trabajador a la MPHy acepta las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información, así como el estricto cumplimiento a las Políticas y Normas de Seguridad de la Información.

1.1. Usuarios:

1.1.1. El jefe inmediato o que haga sus veces, debe informar a la Unidad de TI los datos del nuevo personal, para que sean ingresados en el sistema y se les de los permisos correspondientes. Así mismo para quien deja de laborar o que le cambien de área, para realizar las configuraciones respectivas en su equipo de cómputo, en el sistema, etc.

1.2. Obligaciones de los usuarios:

1.2.1. Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Normas de Seguridad de la Información.

1.3 Entrenamiento en seguridad informática:

1.3.1 Todo trabajador nuevo deberá contar con la inducción sobre el documento "Políticas y Normas de Seguridad de la Información", donde se le da a conocer las obligaciones a los usuarios y las sanciones que pueden existir en caso de incumplimiento.

1.4 Medidas disciplinarias:

1.4.1 Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la MPHy, o de que se le declare culpable de un delito informático.

2. Seguridad Física y del Entorno

Política:

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la MPHy sólo a personas autorizadas para la salvaguarda de los equipos de cómputo, de comunicaciones y la información.

2.1. Resguardo y protección de la información:

2.1.1. El usuario deberá reportar de forma inmediata a la Unidad de TI cuando detecte que existan riesgos reales o potenciales en equipos de cómputo o comunicaciones, como pueden ser fugas de agua, posible incendio, descargas eléctricas u otros.

2.1.2. El usuario tiene la obligación de proteger la información reservada o confidencial que están en las unidades de almacenamiento de la computadora que se encuentren bajo su administración, aun cuando no se utilicen.

2.1.3. Es responsabilidad del usuario evitar en todo momento la fuga de la información de la MPHy que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

2.2. Controles de acceso físico:

2.2.1. Cualquier persona que tenga acceso a las instalaciones de la MPHy, deberá registrar al momento de su entrada en el área de recepción, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento o cualquier otro objeto electrónico que no sea propiedad de la MPHy, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

2.2.2. Las computadoras personales, las computadoras portátiles, y cualquier activo de TI, que se destinadas a reparación, podrá salir de las instalaciones de la MPHy únicamente con la autorización de salida de la Unidad de Patrimonio anexando la papeleta de salida del equipo debidamente firmado por la Gerencia Municipal.

2.3. Seguridad en áreas de trabajo:

2.3.1. El Centro Datos, ubicado en la Unidad de TI es considerado área restringida, por lo que sólo el personal autorizado por la Unidad de TI, puede acceder a él.

2.4. Protección y ubicación de los equipos:

2.4.1. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Unidad de TI. En caso de requerir este servicio deberán solicitarlo.

2.4.2. El usuario es responsable del resguardo de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada. Esto es en coordinación entre la oficina de la Unidad de TI y la Unidad de Patrimonio

2.4.3 El equipo de cómputo asignado, deberá ser de uso exclusivo para las funciones asignadas. Así como la impresora, solo para archivos según el trabajo que desempeña.

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

2.4.5. Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro asignado a Datos (D:) o en la carpeta "Mis Documentos" ya que las otras están destinadas para archivos de programa y sistema operativo.

2.4.6. Mientras están haciendo uso del el equipo de cómputo, no deberán consumir alimentos o ingerir líquidos.

2.4.7. Se debe evitar colocar objetos encima del equipo de cómputo o cubrir los orificios de ventilación del CPU.

2.4.8. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

2.4.9. El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos, en caso de que no se cumpla solicitar un reacomodo de cables con el personal de soporte de la oficina de la Unidad de TI.

2.4.10. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al personal de soporte de la Unidad de TI a través de un plan detallado.

2.4.11. Está prohibido que el usuario abra o desarme los equipos de cómputo.

2.4.12. Los equipos informáticos (inclusive estabilizadores, ups, etc.) deberán ser apagados totalmente a la hora del descanso (13:00 hrs – 14:30hrs), salvo casos justificados y al final de la jornada laboral. El ahorro de energía es considerable y se prolonga el tiempo de vida útil de los equipos.

2.5. Mantenimiento de equipo:

2.5.1. Únicamente el personal autorizado por la Unidad de TI, podrá llevar a cabo los servicios y reparaciones al equipo informático.

2.5.2. Los usuarios deberán asegurarse de respaldar en las carpetas que le fueron asignadas en el servidor la información que consideren relevante cuando el equipo sea enviado a reparación o mantenimiento y borrar aquella información sensible que se encuentre en el equipo, previniendo así la pérdida involuntaria de información, derivada del proceso de reparación.

2.5.3. La Unidad de TI realizará 3 tipos de mantenimiento:

2.5.3.1. PREVENTIVO: La Unidad de TI elaborará un cronograma de mantenimiento preventivo para anticiparse a problemas o situaciones riesgosas que perjudiquen el buen funcionamiento de los servicios existentes.

2.5.3.2. PROACTIVO: En caso de fallas permanentes de un equipo o sistema computacional, la Unidad de TI buscará la causa de dicha falla y procederá a su eliminación mediante la implementación, cambio o incorporación de nuevas tecnologías.

2.5.3.3. CORRECTIVO: La Unidad de TI, dispondrá de personal calificado para solucionar y corregir problemas computacionales que presente el usuario, no obstante de no poder dar solución, se podrá contratar un servicio técnico especializado.

2.6. Pérdida de Equipo:

2.6.1. El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.6.2. El préstamo de algún equipo tendrá que solicitarse a la Gerencia Municipal y el área que tenga el equipo. El préstamo se hará con un acta en donde indique que recae toda la responsabilidad por daño o pérdida a la persona y/o institución que ha solicitado dicho préstamo.

2.6.3. El usuario deberá dar aviso inmediato a la Unidad de TI y a la Unidad de Patrimonio de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7. Uso de dispositivos especiales:

2.7.1. El uso de los grabadores externos de discos, discos duros portátiles es exclusivo para copias de seguridad y para respaldos de información que por su volumen así lo justifiquen.

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

2.7.3. Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por la Unidad de TI.

2.8. Daño del equipo:

2.8.1. El equipo de cómputo o cualquier recurso de TI que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de las Políticas y Normas de Seguridad de la Información.

2.9. Solicitudes de adquisición y administración de hardware:

2.9.1. Las solicitudes para la adquisición de cualquier equipo computacional (impresora, scanner, monitor y demás recursos informáticos) deben ser enviadas por cada Jefe o Gerente a la Gerencia Municipal que en coordinación con la Unidad de TI determinarán y evaluarán la justificación presentada, los planes y prioridad para la dotación, dependiendo de las necesidades y requerimientos del usuario.

2.9.2. Corresponde a la Unidad de TI, proveer las especificaciones técnicas de cualquier equipo computacional, como también la realización de las pruebas técnicas respectivas.

3. Gestión de Comunicaciones y Operaciones

Política:

Los usuarios deberán proteger la información que reside y utiliza la infraestructura tecnológica de la MPHy. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la MPHy o hacia redes externas como Internet.

Los usuarios de la MPHy que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

3.1. Administración de la Información:

3.1.1. La Unidad de TI de la MPHy debe conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial. Por lo que está prohibido la extracción por cualquier medio.

3.1.2. Las actividades que realicen los usuarios en la infraestructura de Tecnología de la Información de la MPHy son registradas y susceptibles de auditoría en cualquier momento.

3.2. Instalación de software:

3.2.1. Los usuarios que requieran la instalación de software que no sea propiedad de la MPHy, deberán justificar su uso indicando el equipo de cómputo, donde se instalará el software y el período de tiempo que permanecerá dicha instalación y solicitar su autorización a la Unidad de TI, quienes evaluaran si se procede o no.

3.2.2. No está permitido que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la MPHy, que no esté autorizado por la Unidad de TI.

3.2.3. Los usuarios de los equipos no tendrán ningún privilegio administrativo sobre el equipo que se le ha entregado. El personal de la Unidad de TI, tendrá privilegios especiales en las estaciones por las funciones que desempeñan de soporte, auditoría, configuración e instalación de software y hardware así como administración de red y seguridad de información.

3.3. Identificación del incidente:

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

3.3.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario deberá notificar a la Unidad de TI.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de cómputo de la MPHy debe ser reportado a la Unidad de TI.

3.4. Administración de la configuración:

3.4.1. Los usuarios de las áreas de la MPHy no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP, SSH), u otro tipo de protocolo para la transferencia de información sin la autorización de la Unidad de TI.

3.5. Seguridad para la red:

3.5.1. Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Unidad de TI, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la MPHy, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

3.6. Uso del correo electrónico corporativo:

3.6.1. Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo corporativo, quedando prohibido hacerlo a una dirección de correo electrónico externa a la MPHy, a menos que cuente con la autorización de la Unidad de TI.

3.6.2. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la MPHy. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3. Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vaya encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

3.6.4. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.6.5. Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

3.7. Seguridad para las comunicaciones:

3.7.1. Con el fin de mejorar la productividad de los usuarios, la Unidad de TI promueve el uso responsable de las comunicaciones en forma electrónica, en particular los teléfonos IP, el mensaje de voz, el correo electrónico, Internet y la mensajería instantánea. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben

considerar como propiedad de la MPHy y no propiedad de los usuarios de tales servicios.

3.7.2. La asignación de números de anexos de telefonía IP y la instalación de nuevos teléfonos IP, son aprobados por la Gerencia Municipal.

3.7.3. Se establece el aplicativo de Mensajería Instantánea provisto por la Unidad de TI, como el único medio oficial para las comunicaciones internas. Todos los usuarios que inicien sus labores en la computadora deberán obligatoriamente iniciar sesión en el aplicativo de Mensajería Instantánea.

3.7.4. El uso de Mensajería Instantánea es exclusivamente para temas relacionados al trabajo.

3.8. Controles contra código malicioso:

3.8.1. Para prevenir infecciones por virus informático, los usuarios de la MPHy no deben hacer uso de software que no haya sido proporcionado y validado por la Unidad de TI.

3.8.2. Los usuarios de la MPHy deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Unidad de TI.

3.8.3. Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

3.8.4. Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Unidad de TI.

3.8.5. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y comunicar a la Unidad de TI para la detección y erradicación del virus.

3.8.6. Los usuarios no deberán alterar o eliminar, las configuraciones implantadas por la Unidad de TI de seguridad para detectar y/o prevenir la propagación de virus.

3.8.7. Debido a que algunos virus son extremadamente complejos, ningún usuario debe intentar erradicarlos de las computadoras.

3.9. Uso del servicio de Internet:

3.9.1. El acceso a Internet provisto a los usuarios de la MPHy es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

3.9.2. La Unidad de TI contará con una herramienta de control de páginas Web, que controle el contenido de las páginas durante el proceso de navegación.

3.9.3. Los niveles de los usuarios para la navegación por Internet serán coordinados previamente con el área respectiva, definiéndose el criterio por las necesidades de trabajo de cada uno.

3.9.4. El acceso a páginas de Chat, mensajería instantánea externa o páginas de envió de información queda prohibido, y su utilización genera responsabilidad en el Jefe de área por cualquier infección de virus o problema de espionaje de información ya que la Unidad de TI no puede controlar el envío de información por estos medios, solo por necesidad justificada y autorizada por el área respectiva y la Unidad de TI se podrá utilizar estos servicios.

3.9.5. Se establecen las siguientes prohibiciones en cuanto al uso del servicio de internet:

- Ingresar a páginas ajenas a la labor diaria (pornografía, juegos, mp3, religión, hackers, violencia, etc.).
- La instalación de cualquier tipo de software o plug-in que no haya sido proporcionado por la Unidad de TI.
- Cualquier forma de envío/recepción de información hacia/desde destinatarios que no pertenecen a la Municipalidad, por medios que no sean los autorizados.
- La descarga de Archivos no relacionados a las labores propias de la Municipalidad.

- La descarga de archivos de audio y video desde internet.
- Escuchar música por internet
- Escuchar radio por internet
- Ingresar a páginas de redes sociales, páginas de videos u otros de gran consumo de ancho de banda.

3.9.6. Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la MPHy, en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por la Unidad de TI.

3.9.7. Los usuarios de Internet de la MPHy tienen que reportar todos los incidentes de seguridad informática a la Unidad de TI inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.9.8. Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización de la Unidad de TI.
- La utilización de Internet es para el desempeño de su función y puesto en la MPHy y no para propósitos personales.

4. Control de Accesos

Política:

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es su usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de la MPHy, por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la MPHy, debe ser proporcionado por el dueño de la información, con base en el principio de la "necesidad de saber" el cual establece que únicamente se

deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

4.1. Controles de acceso lógico:

4.1.1. Cada usuario es responsable por el usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.2. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Unidad de TI antes de poder usar la infraestructura tecnológica de la MPHy.

4.1.3. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la MPHy.

4.1.4. Cada usuario que acceda a la infraestructura tecnológica de la MPHy debe contar con un nombre de usuario único y personalizado. Por lo cual no está permitido el uso de un mismo nombre de usuario por varios usuarios.

4.1.5. Los usuarios son responsables de todas las actividades realizadas con su nombre de usuario. Los usuarios no deben divulgar ni permitir que otros utilicen sus nombres de usuario, al igual que tiene prohibido utilizar el nombre de usuario de otros usuarios.

4.2. Administración de privilegios:

4.2.1. Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a la Unidad de TI, para el cambio de privilegios.

4.3. Equipo desatendido:

4.3.1. Para prevenir el acceso no autorizado, los equipos están configurados de manera tal que al cabo de quince (15) minutos de inactividad, se active el protector de pantalla y se bloquee el acceso a la computadora, por lo que se requiere ingresar nuevamente la contraseña para reanudar la actividad. El usuario debe bloquear su computador presionando las teclas Windows + L, cada vez que se ausente de su oficina.

4.3.2. El protector de pantalla y fondo de escritorio deben ser los institucionales. No se permite el uso de estos de manera personalizada tanto en los computadores de escritorio como en las portátiles que son propiedad del MPHy.

4.4. Administración y uso de contraseña:

4.4.1. La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

4.4.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá solicitarlo a la Unidad de TI para que se le proporcione una nueva contraseña.

4.4.3. Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

4.4.4. Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.

4.4.5. Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente.

4.4.6. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

4.5. Control de accesos remotos

4.5.1. La administración remota de equipos conectados a Internet desde fuera de la MPHy no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y de la Unidad de TI.

4.5.2. La Unidad de TI podrá realizar la asistencia remota que le permitirá conectarse con el equipo de cómputo, previo aviso al usuario del mismo, con la finalidad prestarle ayuda.

5. Cumplimiento

Política:

La Unidad de TI tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

5.1. Derechos de propiedad intelectual:

5.1.1 Los sistemas desarrollados por personal interno o externo que controle la Unidad de TI son propiedad intelectual de la MPHy.

5.2. Revisiones del cumplimiento:

5.2.1. La Unidad de TI realizará acciones de verificación del cumplimiento del documento Políticas y Normas de Seguridad Informática.

- Proporcionar soporte computacional a las distintas dependencias de la Institución.
- Realizar mantenimientos: preventivo, proactivo y correctivo a los equipos, programas, Sistemas y Software pertenecientes al MPHy y que sean de su responsabilidad.
- Prestar ayuda y asesoría solo cuando se trate de asuntos relacionada con su área de conocimiento.
- Eliminar todo software (juegos, reproductores de audio y video, etc.) que haya sido instalado sin previa autorización de la Unidad de TI
- Verificar la integridad, configuración y estado de los equipos.

5.2.2. La Unidad de TI podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado.

5.2.3. Los jefes y responsables de los procesos establecidos en la MPHy deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y Normas de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

5.3. Tipos de Faltas:

5.3.1. Las faltas cometidas por los usuarios serán sancionadas de acuerdo a la gravedad de las mismas y se clasifican en leves, menos graves y graves; según se señalan a continuación, las cuales se incorporarán al régimen de los Empleados y Funcionarios de la MPHy.

Leves:

- Usar los equipos de la Institución, para actividades no laborales como juegos y pasatiempos.
- Manipular alimentos sobre los equipos computacionales
- Utilizar fondos y/o protectores de pantalla que no son los institucionales (personalizados), sean computadores personales y/o portátiles, propiedad de la MPHy.
- Exponer los equipos a riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- No reportar inmediatamente fallas en los computadores o en la red que consecuentemente cause problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Mover (cambiar de lugar, desplazar) los equipos o reubicarlos sin autorización previa.
- No reportar a la Unidad de TI la detección de virus u otro agente potencialmente peligroso.
- La no utilización de un programa antivirus para examinar todo archivo que venga de afuera o inclusive de otras dependencias de la Institución.
- Utilizar medios de almacenamiento en cualquier computadora portadores de virus u otros agentes dañinos.
- Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.
- La falta de cuidado, pulcritud y limpieza del equipo de informática asignado.
- La navegación en Internet para fines personales por períodos prolongados de tiempo.
- Bajar archivos de música o vídeo desde Internet.

Menos Graves:

- La reincidencia en la comisión de una falta leve.

- Modificar la configuración de hardware y/o software establecida por la Unidad de TI.
- Llevar al sitio de trabajo computadores portátiles (laptop) que sean propiedad particular del empleado sin la autorización previa.
- La instalación de programas y la modificación de los programas, paquetes y configuraciones ya instalados en los computadores.
- Visitar o acceder a sitios web obscenos, que distribuyan material pornográfico, o materiales ofensivos en perjuicio de terceros.

Graves:

- La reincidencia en la comisión de una falta menos grave.
- La pérdida o robo de cualquier componente de hardware o programa de software por negligencia debidamente comprobada.
- Realizar impresiones, copias y escaneos para fines personales, ajenos a la MPHy.
- Llevar un equipo fuera de la Institución sin autorización previa.
- Revelar datos confidenciales.
- Conectar a la red de la MPHy computadores portátiles (laptop) que sean propiedad particular del empleado sin la autorización previa.
- Hacer copias o usar software tanto adquirido como desarrollado, para fines personales y en violación a derechos de autor.
- Hacer uso de software bajado de Internet (software libre, gratis, demos, etc.) y en general software que provenga de una fuente no confiable.
- El uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado.
- Copiar a un medio removible (DVD, USB, CD), el software o los datos residentes en las computadoras del MPHy, sin la aprobación previa.
- Utilizar/usurpar el acceso a las claves utilizadas para el cifrado y descifrado.
- Abrir los equipos computacionales.
- Prestar, compartir, usurpar, contraseña.
- Burlar los sistemas de seguridad informática.
- Sacar (extraer) o cambiar componentes de los equipos.
- Prestar e intercambiar los equipos computacionales sin la correspondiente autorización.
- Instalar equipos sin la supervisión y autorización expresa de la Unidad de TI

- Leer, copiar, o cambiar los archivos de cualquier otro usuario.
- Inspeccionar, copiar y almacenar programas computacionales, software y demás materiales electrónicos que violen la ley de derechos de autor.
- Enviar a través de Internet mensajes con información confidencial a menos que tal información esté cifrada y autorizada.
- Divulgar, duplicar, modificar, destruir, extraviar, robar y acceder a información confidencial.
- Ingresar al Centro de Datos de la Unidad de TI, intentar abrir y/o revisar los gabinetes de red, que es uso exclusivo para personal autorizado.

Glosario de Términos

- **Acceso Físico:** Es la actividad de ingresar a un área.
- **Acceso Lógico:** Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.
- **Centro Datos:** Es donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
- **Equipo de cómputo:** Conjunto compuesto por una pantalla, CPU, teclado, mouse, UPS o estabilizador, cables de red.
- **Hardware:** Se refiere a las características técnicas y físicas de las computadoras.
- **Norma:** Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.
- **Respaldo:** Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
- **Servidor:** Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas.
- **Software:** Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
- **Usuario:** Persona que presta servicios en la institución, bajo cualquier régimen laboral y que interactúa con la computadora.

Municipalidad Provincial de Huaylas
Secretaría General
Unidad de Tecnologías de la Información

"Año de la Diversificación Productiva y del Fortalecimiento de la Educación"

INFORME Nº 088-2015-MPHy-Cz-A/06.11

A : **PROF. EBER TITO GUTIEREZ VAZQUES**
Secretario General

DE : **ING. AMÓS PAULINO MEJÍA LEÓN**
Jefe de la Unidad de Tecnologías de la Información

ASUNTO : Políticas y Normas de Seguridad de la Información

FECHA : **18 de Mayo de 2015**

Mediante el presente me dirijo a usted para hacerle llegar mi saludo y a la vez informar que adjunto las "Políticas y Normas de Seguridad de la Información", que tiene como finalidad dar a conocer a los usuarios lo relacionado a los servicios de Tecnologías de la Información, para proteger adecuadamente los activos tecnológicos y la información de la Municipalidad Provincial de Huaylas.

S G MPH-Caraz V°B° SECRETARIA GENERAL

Para ello se ha tenido en cuenta se ha tenido en cuenta la serie de normas internacionales ISO/IEC 27000 que contiene las mejores prácticas recomendadas en Seguridad de la Información, que en nuestro país se dan en la Norma Técnica Peruana NTP -ISO/IEC 17799:2007 y la ISO/IEC 27001:2008.

El presente debe ser emito bajo Decreto de Alcaldía. Sustituye al Decreto de Alcaldía N°017-2013/MPHy con título "Políticas y Estándares de Seguridad Informática".

Es todo cuanto informo a usted.

Atte,

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN MUNICIPALIDAD PROVINCIAL DE HUAYLAS
Ing. Amós P. Mejía León
JEFE

18 MAY 2015

S G MPH - CARAZ RECIBIDO SECRETARIA GENERAL

03:00 p