Defensoría del Pueblo

RESOLUCIÓN DE SECRETARÍA GENERAL Nº 009 -2011/DP-SG

Lima, 08 FEB. 2011

VISTO:

El Memorando Nº 0020-2011-DP/SG, que adjunta las Normas de Seguridad de la Información de la Defensoría del Pueblo propuestas por el Comité de Gestión de Seguridad de la Información, mediante el que se solicita la emisión de la resolución que apruebe los proyectos de Normas de Seguridad de la Información de la Defensoría del Pueblo; y,

CONSIDERANDO:

Que, de conformidad con los artículos 161º y 162º de la Constitución Política del Perú se aprobó la Ley Nº 26520, Ley Orgánica de la Defensoría del Pueblo, y mediante Resolución Defensorial Nº 029-2008/DP se aprobó su vigente Reglamento de Organización y Funciones, modificado por la Resolución Defensorial Nº 019-2009/DP;

Que, la información que genera la Defensoría del Pueblo constituye un activo de vital importancia para el adecuado cumplimiento de las funciones que dicha entidad tiene a su cargo, por lo que debe ser protegida de todo tipo de amenazas, sean internas o externas, deliberadas o accidentales, velando por la preservación de la confidencialidad, integridad y disponibilidad de la información en todos sus medios de soporte y tratamiento;

Que, el numeral 5.1.1 de la Norma Técnica Peruana "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", establece que para tener un adecuado control la Alta Dirección debe aprobar, publicar y comunicar a todo el personal de la institución, en forma adecuada, un documento de Política de Seguridad de la Información;

Que, las Normas de Seguridad de la Información propuesto por el Comité de Gestión de Seguridad de la Información de la Defensoría del Pueblo, contribuirán a fortalecer en el personal de la Defensoría del Pueblo una cultura de seguridad de la información, promoviendo a la vez su adecuado tratamiento y protección;

Que, según el documento de visto, se solicita que se apruebe el documento que contiene las Normas de Seguridad de la Información de la Defensoría del Pueblo, siendo conveniente aprobar el documento citado;

Con los visados de las Oficina de Asesoría Jurídica y de los integrantes del Comité de Gestión de Seguridad de la Información;

Defensoría del Pueblo

En uso de las atribuciones conferidas por los literales e), f) y q) del artículo 15° del Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por Resolución Defensorial N° 029-2008/DP, modificado mediante Resolución Defensorial N° 019-2009/DP;

SE RESUELVE:

Artículo Primero.- APROBAR las siguientes Normas que forman parte de la presente Resolución:

- Norma para el uso de Internet en la institución
- Norma para uso de contraseñas
- Norma para el uso de correo electrónico
- Norma de pantalla y escritorio limpio
- Norma de instalación y uso de software
- Norma de instalación y uso de software de protección e inventario de activos de información.

Artículo Segundo.- Las Normas de Seguridad de la Información aprobadas por el artículo precedente entrarán en vigencia en la fecha de emisión de la presente Resolución, siendo de cumplimiento obligatorio para todas las dependencias de la Defensoría del Pueblo.

Artículo Tercero.- ENCARGAR a la Oficina de Tecnología de la Información de la Defensoría del Pueblo, la publicación de la presente Resolución en el Portal Institucional de la entidad.

Regístrese, comuníquese y publíquese.

Alicia Zambrano Cerna
Secretaria General
DEFENSORÍA DEL PUEBLO

	NORMA PARA USO DE INTERNET EN LA INSTITUCIÓN	Código 01.01.01	
		Página 1 de 2	Versión: 1.0

Elaborado por:	Revisado por:	Aprobado por:	Fecha de Elaboración: 12.ene.2011
Francisco Neira B. Encargado Seguridad de la Información	**Comité de Gestión de Seguridad de la Información**	**Comité de Gestión de Seguridad de la Información**	**Fecha de Modificación:**

1 PROPÓSITO

Definir el uso permitido de Internet en la Defensoría del Pueblo

2 ALCANCE

Aplicable para todos los órganos y unidades orgánicas de la Defensoría del Pueblo

3 DEFINICIONES

3.1 Programas P2P: Aplicativos que permiten descargas masivas de información desde Internet. Entre los más conocidos están: Ares, Limewire, Kazaa, Emule, Vuze, etc.

3.2 Programas de mensajería instantánea: Se refiere a aquellos aplicativos que permiten conversaciones en tiempo real. Se pueden mencionar entre los más conocidos: MSN Messenger, Yahoo Messenger, Skype, etc.

3.3 Páginas de radio y TV por Internet: Se refiere a aquellas páginas en Internet que permiten escuchar radio y ver TV en tiempo real.

3.4 Páginas de redes sociales: Se refiere a aquellas páginas Web donde usuarios comparten información personal, videos, fotos, etc. Se pueden mencionar en este tipo las más conocidas: Facebook, Hi5, Youtube, etc.

3.5 Páginas de juegos en línea: Se refiere a páginas en Internet que permiten jugar de manera personal o con otros usuarios en tiempo real

3.6 Páginas de adultos: Se refiere a páginas en Internet con contenido exclusivo para adultos

4 RESPONSABILIDADES

4.1 Jefaturas y Direcciones:

Definir los accesos y permisos en Internet que tendrá el personal de acuerdo a su rol.

4.2 Oficina de Tecnología de la Información (OTI):

Implementar y administrar los accesos a Internet de acuerdo a los roles en la institución.

Monitoreo del desempeño del servicio de Internet.

Emitir reportes de accesos a Internet de acuerdo a requerimientos específicos.

4.3 Oficina de Gestión de Recursos Humanos (OGRH):

Mantener actualizada la información de roles asignados a cada colaborador con el objetivo de asignar adecuadamente los permisos a Internet.

5 LINEAMIENTOS

5.1 No está permitido el acceso a las páginas Web y programas señalados en el punto 3. Tener en cuenta que no está autorizado el uso de dispositivos que permitan capturar señal abierta de TV digital.

5.2 Las jefaturas y direcciones son las únicas autorizadas a solicitar accesos adicionales a cada rol definido, señalando la justificación de labor que lo sustente. Las solicitudes estarán sujetas a la evaluación y aprobación del área de Seguridad la Información.

5.3 OTI podrá suspender el servicio de Internet sin previo aviso cuando existan amenazas contra la seguridad de la red de la institución.

5.4 En caso se suspenda el servicio de internet de forma parcial o total, por razones relacionadas a la presente norma, sólo la Alta Dirección podrá solicitar la reposición del mismo, empleando el formato de autorización establecido.

6 DOCUMENTOS DE REFERENCIA

6.1 Constitución Política del Perú
6.2 Ley Orgánica de la Defensoría del Pueblo, Ley N°26520
6.3 Resolución Ministerial N° 246-2007-PCM – Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI – Tecnología de la Información – Código debuenas prácticas para la gestión de la seguridad de la información. 2A Edición.
6.4 Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por la Resolución Defensorial N° 029-2008/DP, y su modificatoria, aprobado por la Resolución Defensorial N° 019-2009/DP.
6.5 Política Institucional de Seguridad de la Información de la Defensoría del Pueblo, aprobada por la Resolución Administrativa N° 062-2008/DP-PAD
6.6 Estándar ISO/IEC 27002:2005

7 SANCIONES

Se hará el seguimiento respectivo para garantizar el cumplimiento de los lineamientos y responsabilidades de la presente norma en coordinación con la OGRH.

	NORMA PARA EL USO DE CONTRASEÑAS	Código 01.01.02	
		Página 1 de 3	Versión: 1.0

Elaborado por:	Revisado por:	Aprobado por:	Fecha de Elaboración: 12.ene.2011
Francisco Neira B. Encargado Seguridad de la Información	**Comité de Gestión de Seguridad de la Información**	**Comité de Gestión de Seguridad de la Información**	**Fecha de Modificación:**

1 PROPÓSITO

1.1 Definir el uso de contraseñas de acceso en la Defensoría del Pueblo

2 ALCANCE

2.1 Aplicable para todos los órganos y unidades orgánicas de la Defensoría del Pueblo

3 DEFINICIONES

3.1 ***Autenticarse o autentificarse:*** Es el procedimiento por el cual el usuario se identifica ante una estación con su nombre y demuestra su identidad al escribir una contraseña que es sólo de su conocimiento. En algunos sistemas este procedimiento se conoce como "login" o "logon".

3.2 ***Órgano:*** Es la unidad de organización que conforma la estructura orgánica de la entidad.

3.3 ***Unidad orgánica:*** Es la unidad de organización que conforma los órganos contenidos en la estructura orgánica de la entidad.

3.4 ***Usuario:*** Persona que, con autorización expresa de un funcionario de la Defensoría, utiliza recursos informáticos o de información de la institución, sin importar si existe o no relación laboral o de dependencia.

3.5 ***Recursos informáticos:*** podrán ser estaciones, servidores, archivos, correo electrónico, acceso a Internet, etc.

3.6 ***Recursos de información***: podrán ser expedientes, cartas, oficios, memorándumes, archivos, grabaciones de audio o video, etc.

4 RESPONSABILIDADES

4.1 Jefes(as) de órganos o unidades orgánicas:

4.1.1 Definir los accesos y permisos a la red institucional, aplicaciones y al correo electrónico que tendrá el personal a su cargo, de acuerdo a su rol.

4.2 Oficina de Tecnología de la Información (OTI):

4.2.1 Implementar y administrar los mecanismos de seguridad de accesos a la red institucional, aplicaciones y al correo electrónico de acuerdo a los roles en la institución.

4.2.2 Monitoreo del desempeño del servicio de correo.

4.2.3 Emitir reportes de accesos a la red y otros servicios de acuerdo a requerimientos específicos.

4.3 Oficina de Gestión de Recursos Humanos (OGRH):

4.3.1 Mantener actualizada la información de roles asignados a cada colaborador con el objetivo de asignar adecuadamente los permisos a Internet.

5 LINEAMIENTOS

5.1 La solicitud para la creación de una nueva cuenta, sea esta de acceso a la red, al sistema de correo electrónico o a cualquier sistema informático, deberá realizarla el jefe del órgano o unidad orgánica, por escrito, tal como se indica en el procedimiento "Solicitud de Contraseñas". El jefe asimismo será el responsable de solicitar las baja (desactivacion) de las respectivas cuentas al terminar la relación laboral o contractual.

5.2 Esta baja será realizada inmediatamente recibida la comunicación por el Área de redes de la OTI, salvo contraorden proveniente de la Alta Dirección y podrá hacerse efectiva para todos los acceso con contraseña o únicamente para el correo electrónico.

5.3 La contraseña asignada tiene carácter de provisional, por lo que es responsabilidad del usuario el cambiarla a la brevedad.

5.4 La contraseña es personal e intransferible.

5.5 Cualquier mal uso o suplantación será atribuíble al usuario por lo que bajo ningún concepto deberá darla a conocer

5.6 Si el usuario sospecha que su contraseña puede haber sido comprometida deberá reemplazarla inmediatamente

5.7 Las contraseñas deberán de ser reemplazadas con la frecuencia indicada en el estandar "Uso y cambio de contraseñas" o más frecuentemente si lo considera el usuario pertinente.

6 DOCUMENTOS DE REFERENCIA

6.1 Constitución Política del Perú
6.2 Ley Orgánica de la Defensoría del Pueblo, Ley N°26520
6.3 Resolución Ministerial N° 246-2007-PCM – Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI – Tecnología de la Información – Código debuenas prácticas para la gestión de la seguridad de la información. 2A Edición.
6.4 Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por la Resolución Defensorial N° 029-2008/DP, y su modificatoria, aprobado por la Resolución Defensorial N° 019-2009/DP.
6.5 Política Institucional de Seguridad de la Información de la Defensoría del Pueblo, aprobada por la Resolución Administrativa N° 062-2008/DP-PAD
6.6 Estándar ISO/IEC 27002:2005

7 SANCIONES

7.1 Se hará el seguimiento respectivo para garantizar el cumplimiento de los lineamientos y responsabilidades de la presente norma, en coordinación con la OGRH.

	NORMA PARA EL USO DEL CORREO ELECTRÓNICO	Código 01.01.03	
		Página 1 de 3	Versión: 1.0

Elaborado por:	Revisado por:	Aprobado por:	Fecha de Elaboración: 12.ene.2011
Francisco Neira B. Encargado Seguridad de la Información	**Comité de Gestión de Seguridad de la Información**	**Comité de Gestión de Seguridad de la Información**	**Fecha de Modificación:**

1 PROPÓSITO

1.1 Definir el uso del servicio de correo electrónico en la Defensoría del Pueblo

2 ALCANCE

2.1 Aplicable para todos los órganos y unidades orgánicas de la Defensoría del Pueblo

3 DEFINICIONES

3.1 ***Autenticarse o autentificarse:*** Es el procedimiento por el cual el usuario se identifica ante una estación con su nombre y demuestra su identidad al escribir una contraseña que es sólo de su conocimiento. En algunos sistemas este procedimiento se conoce como "login" o "logon".

3.2 ***Órgano:*** Es la unidad de organización que conforma la estructura orgánica de la entidad.

3.3 ***Unidad orgánica:*** Es la unidad de organización que conforma los órganos contenidos en la estructura orgánica de la entidad.

3.4 ***Usuario:*** Persona que, con autorización expresa de un funcionario de la Defensoría, utiliza recursos informáticos o de información de la institución, sin importar si existe o no relación laboral o de dependencia.

3.5 ***Texto plano:*** Texto sencillo, sin efectos como tablas, subrayados, colores, negrita o itálicas. Es de uso universal y por ello es legible por cualquier programa de correo electrónico.

3.6 ***Archivo ejecutable:*** Es toda porción de código que puede ser interpretado por un computador como una secuencia de instrucciones.

3.7 ***"Over quota":*** Término en inglés que equivale a "cuota excedida" y significa cuando el buzón del usuario ha alcanzado o excedido la capacidad para la cual ha sido programado. Cuando el buzón está en condición *"over quota"*, los mensajes no son recibidos y enviados son rechazados permanentemente.

4 RESPONSABILIDADES

4.1 Jefes(as) de órganos o unidades orgánicas:

4.1.1 Definir qué personal a su cargo deberá tener acceso al correo electrónico de acuerdo a su rol.

4.2 Oficina de Tecnología de la Información (OTI):

4.2.1 Implementar y administrar los mecanismos de seguridad de acceso al correo electrónico de acuerdo a los roles en la institución.

4.2.2 Monitoreo del desempeño del servicio de correo.

4.2.3 Velar por la continuidad del flujo de mensajes y la alta disponibilidad del servicio de correo electrónico.

4.3 Oficina de Gestión de Recursos Humanos (OGRH):

4.3.1 Mantener actualizada la información de roles asignados a cada colaborador con el objetivo de asignar adecuadamente el acceso al correo electrónico.

4.4 Usuarios

4.4.1 Gestionar sus mensajes de correo y el espacio disponible

5 LINEAMIENTOS

5.1 La información contenida y manejada en el sistema de correo electrónico debe ser utilizada con fines institucionales; por ello, deberá de mantenerse a lo mínimo posible el uso de este servicio para temas personales.

5.2 Por tratarse de información institucional, está prohibido utilizarla con el fin de obtener provecho personal.

5.3 Por considerarse inadecuados, están prohibidos también los siguientes:

5.3.1 Difusión de mensajes de contenido inadecuado o ilegal, ejemplo: terrorismo, programas ilegales, pornografía, amenazas, estafas, etc.

5.3.2 Distribución masiva de mensajes o publicidad no solicitada, conocida como "spam".

5.3.3 Suscripcion indiscriminada a listas de correo,

5.3.4 Correos electrónicos anónimos difamatorios.

5.4 Los correos electrónicos que se reciban por error y correspondan a terceros deben ser tratados con el mismo cuidado con el que se trata cualquier información de la institución y debera ser devuelto en el menor tiempo posible al remitente original, informándole de su error.

5.5 Todos los usuarios deberán leer sus correos permanentemente

5.6 Es obligación del usuario eliminar los mensajes que considere innecesarios. Los mensajes de importancia deberán ser respaldados fuera del servidor para evitar pérdidas ante un posible fallo del servicio dado que en caso de contingencias, la OTI no garantiza el contenido de los buzones.

5.7 Por lo expuesto en el punto anterior, el no recibir mensajes de correo por "over quota" o "buzón lleno" es atribuíble solamente al usuario. La capacidad de los buzones está especificado en el estándar "Correo electrónico".

5.8 No está permitido el envío de archivos ejecutables, imágenes en formato bitmap o scripts ni adjuntos que excedan lo especificado en el estándar "Correo electrónico".

5.9 Cuando el usuario se ausente por un período extenso de tiempo como vacaciones o licencias, deberá de habilitar la opción de mensaje de respuesta por vacaciones y de ser posible, dejar derivados sus mensajes al reemplazante.

5.10 A pesar de que el sistema de correo tiene un detector de virus y spam, el usuario deberá ser cauto y no abrir adjuntos de remitentes que desconoce o seguir enlaces a páginas web sin haberlos solicitado.

6 DOCUMENTOS DE REFERENCIA

6.1 Constitución Política del Perú
6.2 Ley Orgánica de la Defensoría del Pueblo, Ley N°26520
6.3 Resolución Ministerial N° 246-2007-PCM – Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI – Tecnología de la Información – Código debuenas prácticas para la gestión de la seguridad de la información. 2A Edición.
6.4 Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por la Resolución Defensorial N° 029-2008/DP, y su modificatoria, aprobado por la *Resolución Defensorial N° 019-2009/DP.*
6.5 Política Institucional de Seguridad de la Información de la Defensoría del Pueblo, aprobada por la Resolución Administrativa N° 062-2008/DP-PAD
6.6 Estándar ISO/IEC 27002:2005

7 SANCIONES

7.1 Se hará el seguimiento respectivo para garantizar el cumplimiento de los lineamientos y responsabilidades de la presente norma, en coordinación con la OGRH.

	NORMA DE PANTALLA Y ESCRITORIO LIMPIO	Código 01.01.04	
		Página 1 de 2	Versión: 1.0

Elaborado por:	Revisado por:	Aprobado por:	Fecha de Elaboración: 12.ene.2011
Francisco Neira B. *Encargado Seguridad de la Información*	**Comité de Gestión de Seguridad de la Información**	**Comité de Gestión de Seguridad de la Información**	**Fecha de Modificación:**

1 PROPÓSITO

1.1 Definir la politica de "pantallas limpias" y "escritorios limpios" en la Defensoría del Pueblo.

2 ALCANCE

2.1 Aplicable para todos los órganos y unidades orgánicas de la Defensoría del Pueblo

3 DEFINICIONES

3.1 ***Órgano:*** Es la unidad de organización que conforma la estructura orgánica de la entidad.
3.2 ***Unidad orgánica:*** Es la unidad de organización que conforma los órganos contenidos en la estructura orgánica de la entidad.
3.3 ***Usuario:*** Persona que, con autorización expresa de un funcionario de la Defensoría, utiliza recursos informáticos o de información de la institución, sin importar si existe o no relación laboral o de dependencia.
3.4 ***Escritorio limpio:*** Es aquel cuya superficie queda libre de documentos cuando el usuario no está presente.
3.5 ***Pantalla limpia:*** Es aquella que queda protegida por un salvapantallas con contraseña y cuya información no es visible sin la intervención del usuario que inició la sesión para desbloquearla.
3.6 ***Salvapantallas:*** Denominado también *protector de pantalla*. Es un programa informático que forma parte del sistema operativo y que permite ocultar temporalmente la información desplegada en la pantalla de la computadora. Para que sea realmente eficaz, este programa deberá estar configurado con contraseña, que es la misma de la red o de la computadora.

4 RESPONSABILIDADES

4.1 Jefes(as) de órganos o unidades orgánicas:

4.1.1 Velar por que sus subordinados cumplan con la presente norma.

4.2 Oficina de Tecnología de la Información (OTI):

4.2.1 Implementar y administrar los mecanismos de seguridad que permitan el ocultamiento de información desplegada en la pantalla luego de un período de inactividad o a pedido del usuario, y el pedido de contraseña al reestablecerse la actividad.

4.3 Usuarios

4.3.1 Guardar todos los documentos bajo llave al abandonar su lugar de trabajo.

4.3.2 Asegurar con el salvapantalla con contraseña al alejarse de su estación (PC).

5 LINEAMIENTOS

5.1 Al dejar su puesto de trabajo, todos los usuarios deberán de guardar bajo llave todos los documentos con los cuales estuvieron trabajando, teniendo particular atención en aquellos que contengan información que de ser divulgada pueda perjudicar la reputación o la integridad física y/o moral de los ciudadanos.

5.2 Al alejarse de la computadora, el usuario deberá de dejarla con el protector de pantalla activo y con contraseña. Adicionalmente, podrá apagar el monitor pero sin omitir el aseguramiento del acceso por contraseña.

5.3 Lo indicado en el punto anterior incluye ausencias breves como asistir a reuniones, ir al servicio higiénico, atender llamadas en teléfonos alejados del escritorio, pasar faxes, sacar copias, etc.

6 DOCUMENTOS DE REFERENCIA

6.1 Constitución Política del Perú
6.2 Ley Orgánica de la Defensoría del Pueblo, Ley N°26520
6.3 Resolución Ministerial N° 246-2007-PCM – Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI – Tecnología de la Información – Código debuenas prácticas para la gestión de la seguridad de la información. 2A Edición.
6.4 Decreto Supremo N° 009-2009-MINAM – Medidas de Ecoeficiencia para el Sector Público.
6.5 Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por la Resolución Defensorial N° 029-2008/DP, y su modificatoria, aprobado por la Resolución Defensorial N° 019-2009/DP.
6.6 Política Institucional de Seguridad de la Información de la Defensoría del Pueblo, aprobada por la Resolución Administrativa N° 062-2008/DP-PAD
6.7 Estándar ISO/IEC 27002:2005

7 SANCIONES

7.1 Se hará el seguimiento respectivo para garantizar el cumplimiento de los lineamientos y responsabilidades de la presente norma, en coordinación con la OGRH.

	NORMA DE INSTALACION Y USO DE SOFTWARE	Código 01.01.05	
		Página 1 de 2	Versión: 1.0

Elaborado por:	Revisado por:	Aprobado por:	Fecha de Elaboración: 12.ene.2011
Francisco Neira B. Encargado Seguridad de la Información	**Comité de Gestión de Seguridad de la Información**	**Comité de Gestión de Seguridad de la Información**	**Fecha de Modificación:**

1 PROPÓSITO

1.1 Definir el uso y la instalación del software en los equipos de cómputo en la Defensoría del Pueblo.

2 ALCANCE

2.1 Aplicable para todos los órganos y unidades orgánicas de la Defensoría del Pueblo

3 DEFINICIONES

3.1 ***Órgano:*** Es la unidad de organización que conforma la estructura orgánica de la entidad.
3.2 ***Unidad orgánica:*** Es la unidad de organización que conforma los órganos contenidos en la estructura orgánica de la entidad.
3.3 ***Usuario:*** Persona que, con autorización expresa de un funcionario de la Defensoría, utiliza recursos informáticos o de información de la institución, sin importar si existe o no relación laboral o de dependencia.

4 RESPONSABILIDADES

4.1 Jefes(as) de órganos o unidades orgánicas:

4.1.1 Velar por que sus subordinados cumplan con la presente norma.

4.2 Oficina de Tecnología de la Información (OTI):

4.2.1 Implementar y administrar los mecanismos de control de inventario de software y sus licencias.

4.2.2 Preparar y actualizar la lista de software autorizado.

4.2.3 Revisar periódicamente el inventario de software instalado en los equipos de cómputo de la institución y compararlo contra la lista de licencias de software, informando a la Secretaría General y a Seguridad de la Información todas las discrepancias que pudieran aparecer.

4.3 Oficina de Gestión de Recursos Humanos (OGRH):

4.3.1 Mantener actualizada la información de roles asignados a cada colaborador con el objetivo de definir adecuadamente el software que deberá de ser instalado en cada computadora, según el uso que se le vaya a dar.

4.4 Usuarios

4.4.1 Observar y cumplir la siguiente norma, sus procedimientos y estándares.

5 LINEAMIENTOS

5.1 Todo el software que se use o instale en los equipos de cómputo de la institución deberá de contar con su respectiva licencia, ya sea del tipo propietario o del tipo libre.

5.2 De ninguna manera se permitirá la instalación de software ilegal, pirata o de procedencia dudosa.

5.3 Solamente el personal de la OTI está autorizado a instalar software en los equipos de cómputo de la institución. En algunos casos, por razones específicas y previa autorización escrita de la OTI, será personal externo quien realice estas instalaciones.

5.4 La OTI mantendrá actualizados tanto el inventario de software como la lista de software autorizado y estandarizado para la institución. Esta lista está detallada en el estándar correspondiente.

5.5 En un procedimiento adjunto a esta norma se detalla cómo se deberá de solicitar la instalación o actualización del software en casos específicos.

6 DOCUMENTOS DE REFERENCIA

6.1 Constitución Política del Perú
6.2 Ley Orgánica de la Defensoría del Pueblo, Ley N°26520
6.3 Resolución Ministerial N° 246-2007-PCM – Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI – Tecnología de la Información – Código debuenas prácticas para la gestión de la seguridad de la información. 2A Edición.
6.4 Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por la Resolución Defensorial N° 029-2008/DP, y su modificatoria, aprobado por la Resolución Defensorial N° 019-2009/DP.
6.5 Política Institucional de Seguridad de la Información de la Defensoría del Pueblo, aprobada por la Resolución Administrativa N° 062-2008/DP-PAD
6.6 Estándar ISO/IEC 27002:2005

7 SANCIONES

7.1 La persona que desatienda la presente norma será sancionada por la institución con la multa que le corresponda pagar a la Defensoría por la infracción.

	NORMA DE INSTALACION Y USO DE SOFTWARE DE PROTECCIÓN E INVENTARIO DE ACTIVOS DE INFORMACIÓN	Código 01.01.06	
		Página 1 de 2	Versión: 1.0

Elaborado por:	Revisado por:	Aprobado por:	Fecha de Elaboración: 12.ene.2011
Francisco Neira B. Encargado Seguridad de la Información	**Comité de Gestión de Seguridad de la Información**	**Comité de Gestión de Seguridad de la Información**	**Fecha de Modificación:**

1 PROPÓSITO

1.1 Definir el uso y la instalación del software de protección y de inventario de activos de información en los equipos de cómputo en la Defensoría del Pueblo.

2 ALCANCE

2.1 Aplicable para todos los órganos y unidades orgánicas de la Defensoría del Pueblo

3 DEFINICIONES

3.1 ***Órgano:*** Es la unidad de organización que conforma la estructura orgánica de la entidad.
3.2 ***Unidad orgánica:*** Es la unidad de organización que conforma los órganos contenidos en la estructura orgánica de la entidad.
3.3 ***Usuario:*** Persona que, con autorización expresa de un funcionario de la Defensoría, utiliza recursos informáticos o de información de la institución, sin importar si existe o no relación laboral o de dependencia.
3.4 ***Malware:*** Software utilizado para obtener o eliminar ilegalmente la información almacenada en un recurso informático.
3.5 ***Software de protección:*** Software dedicado a proteger la disponibilidad, integridad y confidencialidad de la información contenida en los equipos informáticos. Entiéndase por ellos el software antivirus, antispyware y de detección de malware en general.
3.6 ***Software de inventario de activos de información:*** Software destinado a tomar inventario del hardware y software instalado en los diversos equipos y reportarlo a un servidor principal.

4 RESPONSABILIDADES

4.1 Jefes(as) de órganos o unidades orgánicas:

4.1.1 Velar por que sus subordinados cumplan con la presente norma.

4.1.2 Informar a la OTI sobre los equipos que no estén cumpliendo con esta norma.

4.2 Oficina de Tecnología de la Información (OTI):

4.2.1 Implementar y administrar los mecanismos de control de inventario de software y sus licencias.

4.2.2 Preparar y actualizar la lista de software autorizado.

4.2.3 Instalar, configurar y actualizar el softwarde protección y de inventario, objeto de esta norma.

4.3 Usuarios

4.3.1 Observar y cumplir la siguiente norma, sus procedimientos y estándares.

4.3.2 Observar que cada equipo informático en su poder cuente con el software indicado debidamente instalado y operativo y reportar cualquier novedad a su jefe.

4.3.3 Si el equipo informático es entregado para ser reparado por terceros, se le deberá de volver a instalar el software objeto de esta norma.

5 LINEAMIENTOS

5.1 Toda computadora personal, servidor y computadora portátil deberá tener instalado, actualizado y activo el software de detección de virus de uso en la institución.

5.2 Las computadoras portátiles de visitantes, consultores o trabajadores itinerantes deberán también contar con un antivirus actualizado y activo.

5.3 Todos los equipos arriba indicados deberán también tener instalado, actualizado y activo el agente del software para toma de inventario de hardware y software.

5.4 Si por alguna razón el equipo informático fuese reinstalado o formateado por técnicos externos, éstos deberán de volver a instalar, actualizar y reactivar el software indicado en esta norma. Para ello podrán contactar con el área de Soporte de la OTI para ser provistos de los instaladores actualizados y los detalles de configuración.

5.5 Todo equipo que salga de Almacén o del depósito de Control Patrimonial para ser puesto en servicio en la institución deberá de contar el software debidamente configurado, actualizado y operativo.

5.6 La OTI mantendrá actualizados tanto el inventario de software como la lista de software autorizado y estandarizado para la institución. Esta lista está detallada en el estándar correspondiente.

6 DOCUMENTOS DE REFERENCIA

6.1 Constitución Política del Perú
6.2 Ley Orgánica de la Defensoría del Pueblo, Ley N°26520
6.3 Resolución Ministerial N° 246-2007-PCM – Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI – Tecnología de la Información – Código debuenas prácticas para la gestión de la seguridad de la información. 2A Edición.
6.4 Reglamento de Organización y Funciones de la Defensoría del Pueblo, aprobado por la Resolución Defensorial N° 029-2008/DP, y su modificatoria, aprobado por la Resolución Defensorial N° 019-2009/DP.
6.5 Política Institucional de Seguridad de la Información de la Defensoría del Pueblo, aprobada por la Resolución Administrativa N° 062-2008/DP-PAD
6.6 Estándar ISO/IEC 27002:2005

7 SANCIONES

7.1 Se hará el seguimiento respectivo para garantizar el cumplimiento de los lineamientos y responsabilidades de la presente norma, en coordinación con la OGRH.