



**RESOLUCION DE LA SUPERINTENDENTE NACIONAL DE LOS
REGISTROS PUBLICOS N° 111 -2008-SUNARP/SN**

Lima, 15 ABR. 2008

VISTO, el Proyecto de Directiva "Normas para la administración y uso de equipos informáticos y de la información", elaborado por la Gerencia de Informática de la Sede Central de la SUNARP;

CONSIDERANDO:

Que, por Resolución Ministerial N° 246-2007-PCM se aprobó el uso obligatorio en todas las Entidades integrantes del Sistema Nacional de Informática, 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";

Que, de acuerdo la Norma Técnica Peruana mencionada en el considerando, la seguridad de la información debe ser acompañada por procedimientos adecuados de uso, mantenimiento y gestión de equipos e información, por parte de todos los trabajadores de la entidad, a fin que se otorgue seguridad a los equipos informáticos antes, durante y después de su uso, además de normar la responsabilidad sobre dichos activos institucionales;

Que, a través de la Directiva N° 004-2006-SUNARP/GG, aprobada por Resolución N° 064-2006-SUNARP/GG, se aprobó el Reglamento de Políticas de Seguridad de Información, texto que debe ser complementado por disposiciones de uso, mantenimiento y gestión de la información, de acuerdo lo considerado anteriormente;

De conformidad al literal l) del artículo 7° del Estatuto de la SUNARP, aprobado por Resolución Suprema N° 135-2002-JUS;

SE RESUELVE:

Artículo Primero.- Aprobar la Directiva N° 001-2008-SUNARP/SN, "Normas para la administración y uso de equipos informáticos y de la información", con la finalidad de normar el uso adecuado de los equipos informáticos utilizados por el personal de la SUNARP, así como, determinar las políticas de uso de la información.

Artículo Segundo.- Disponer la notificación de la presente a las Jefaturas de las Zonas Registrales, las mismas que se harán responsables de poner en conocimiento del personal que labora en las mismas.

Regístrese y comuníquese,


María D. Cambursano Garagorri
Superintendente Nacional
de los Registros Públicos

DIRECTIVA N° 001-2008- SUNARP/SN

“NORMAS PARA LA ADMINISTRACIÓN Y USO DE EQUIPOS INFORMÁTICOS Y DE LA INFORMACIÓN”

I. OBJETIVO

- Definir normas para el uso adecuado de los equipos informáticos tanto de propiedad de la SUNARP como de otras instituciones (cesión en uso, préstamo, alquiler)
- Determinar las políticas de uso de la información.

II. ALCANCE

A todo el personal de la Superintendencia Nacional de los Registros Públicos, Zonas Registrales y al personal externo que realiza labores en la institución, al cual se le asigne un equipo informático para su uso.

III. BASE LEGAL

1. Directiva N° 004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información.

IV. DEFINICIONES

1. **Equipo Informático:** Todo equipo que permita el procesamiento y transferencia de datos, voz, video, multimedia y cualquier tecnología emergente. Ver Anexo- 1.
2. **Equipo de Procesamiento de Datos :** Equipo informático que permite el procesamiento de información
3. **Equipo de Telecomunicaciones:** Equipo informático que permite la transferencia de datos, voz, video, multimedia entre otros.
4. **Equipo informático crítico :** Son los que se encuentran ubicados en los Centros de Computo, tales como Servidores, Equipos de Telecomunicaciones (firewall, switch, Hub, Modem, router).
5. **Usuario :** todo personal de la Superintendencia Nacional de los Registros Públicos, o personal externo que este 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 de una contraseña.
7. **Información Sensible :** Información importante y necesaria para el desarrollo de las labores del usuario.
8. **Acceso vía Intranet :** Servicio disponible para los trabajadores de la SUNARP para acceso a determinados servicios.
9. **Acceso vía Extranet:** Servicio disponible para los trabajadores de la SUNARP para acceso al Servicio de Publicidad Registral en Línea.



10. **Acceso vía Internet:** Este servicio se encuentra disponible las 24 horas, se otorga a los usuarios que de acuerdo a sus funciones requieran el uso de internet como herramienta informativa para el desarrollo de sus labores. Este servicio puede estar restringidos a determinados sitios Web.
11. **Descargas:** bajar archivos desde internet a una computadora, conocido también con el término "download".
12. **Partición:** Todo disco duro puede tener una o mas particiones. La partición corresponde a una división lógica aplicada al disco a fin de poder separar la parte de sistema operativo, de aplicaciones y datos
13. **USB:** Universal Serial Bus o Bus Universal en Serie, es un subsistema que transfiere datos o electricidad al dispositivo conectado. Puede conectar dispositivos como teclado, mouse, cámaras digitales, impresoras, discos, entre otros.

V. RESPONSABILIDADES

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

- El usuario será responsable del equipo de cómputo asignado
- Los componentes del equipo de cómputo está compuesto por CPU, monitor, teclado y mouse. En los casos que el área del usuario solicite equipo adicional, la responsabilidad del equipo le será asignada al usuario solicitante (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo VI Administración de Activos de Información, Artículo 30° - Propietarios y Responsables de los Activos de Información).
- Evitar consumir alimentos sobre los equipos de cómputo, así como beber y fumar.
- En caso de falla en el equipo debe ser reportado inmediatamente (correo electrónico, oficio, memorándum) al área de informática para la revisión respectiva.

VI. INSTRUCCIONES

1 De la seguridad de acceso

- Las computadoras , tanto de escritorio como portátiles, deberán tener instalado un protector de pantalla institucional, con un tiempo de activación, lo cual no impide el desarrollo normal de las funciones, al colocar la contraseña se desbloquea el protector. Para activar el protector presionar la tecla Windows + L a fin de activar la opción de bloqueo por contraseña.
- Las computadoras de escritorio deben estar protegidos por una clave de acceso para recursos compartidos.
- En el caso de los equipos informáticos dispongan de un sello de seguridad provisto por el proveedor, sólo podrá ser removido por el proveedor, dado que si el equipo se encuentra en garantía, puede perderse la misma.

2 De la ubicación de la información

- Las computadoras disponen de 02 particiones (primera partición C:\, segunda partición D:\)
- La primera partición es para los fines de instalación de software estándar y de aplicación.
- La segunda partición es para los fines de almacenar la data del usuario.
- Deberá crearse una carpeta con el nombre de usuario (inicial del nombre seguido del apellido paterno). En esta carpeta se almacenará la información concerniente a datos que provienen de aplicaciones tales como Word, Power Point, Excel, Visio, entre otros. En esta carpeta no deberá contener archivos de sistema o software alguno.

3 De las fallas en los Equipos

- Ante fallas del equipo, el **usuario** reportará el problema (correo electrónico, oficio, memorándum) indicando el tipo de falla a la Gerencia de Informática o Jefatura de Informática; pero **no podrá realizar las coordinaciones directamente con el proveedor de servicios**.
- La Gerencia de Informática o Jefatura de Informática, enviará inmediatamente esté disponible, a su personal (Soporte Técnico) para verificar y dar solución a la falla producida.
- En el caso de que el problema sea de mayor envergadura, se coordinará con el área de Administración para coordinar con el proveedor de servicios para la visita técnica correspondiente.
- La Gerencia de Informática o Jefatura de Informática, emitirá un informe a la Gerencia de Administración y Finanzas indicando el problema presentado en el equipo, a fin de que dicha área se encargue del trámite administrativo correspondiente.
- Si fuera necesario el retiro del equipo, y éste forma parte de un Contrato de Mantenimiento, el equipo se enviará a reparación previa entrega de un equipo de similares características en caso de respaldo, durante el tiempo que dure la reparación. En caso de no existir un contrato de garantía, coordinación con la Gerencia de Administración y Finanzas, se evaluará la posibilidad de proporcionar un equipo mientras dure su reparación.
- Si el equipo requiere de cambio de piezas, se solicitará el informe técnico al proveedor del servicio a fin de informar a la Gerencia de Administración de Finanzas y realicen el trámite administrativo respectivo (solicitar cotizaciones y aceptar el cambio del repuesto defectuoso).
- Al ser devuelto el equipo, éste será probado en las instalaciones del área de informática, en presencia del personal técnico de la Gerencia de Informática o Jefatura de Informática.
- Se solicitará un informe técnico a la empresa de servicios, por el trabajo realizado.
- En caso que el desperfecto fuera ocasionada por manipulación por parte del usuario, la Gerencia de Informática o Jefatura de Informática, emitirá un informe final al Jefe del área al cual pertenezca el equipo revisado, con copia a la Gerencia de Administración y Finanzas, con la descripción de lo sucedido.



4 Del acceso a la Red

- La asignación e instalación de equipos es de responsabilidad de la Gerencia de Informática o Jefatura de Informática.
- Todo equipo que ingrese a la institución, el usuario no podrá conectarlo directamente a la red de datos. Deberá solicitar por escrito a la Gerencia de Informática o Jefatura de Informática, su correspondiente conexión. Para la conexión del equipo a la red de datos se valida lo siguiente:

- Procedencia del equipo
- Verificación de la configuración del equipo. En caso de ser necesario se efectuará una nueva instalación con los estándares de partición de disco, sistema operativo y software base.
- Instalación de antivirus, asignación de dirección IP para acceso a los servicios y recursos (impresoras)

En el supuesto que el usuario no permita efectuar estas instalaciones, no se procederá con la conexión a la red del equipo.

- Para los casos de demostración de productos o presentaciones, en los cuales se proporcione un equipo por parte de terceros y debe contar con acceso a nuestra red institucional, debe validarse lo expuesto anteriormente, caso contrario no podrá ser conectado a la red de datos, a fin de proteger la información de la institución.

- Todo usuario que requiera tener acceso a aplicaciones instaladas en los servidores y/o bases de datos, debe contar con un usuario y contraseña de acceso (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo II. Control de Accesos a los Sistemas de Información, Artículo 12° Control de Accesos a los Sistemas de Información).

- El Jefe de cada Área, debe solicitar mediante documento a la Gerencia de Informática o Jefatura de Informática acceso a la red para sus usuarios, indicando

- Nombre de usuario
- Tipo de servicio a los cuales tendrá el acceso
- Tipo de acceso (lectura, escritura)

- El personal encargado de la Administración de la Red de la Gerencia de Informática o Jefatura de Informática, procederá a la creación del usuario y la contraseña (clave temporal) para el ingreso a los recursos de red, así como de las aplicaciones. Procederá a asignar los niveles de acceso a la información y aplicaciones (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo II. Control de Accesos a los Sistemas de Información, artículo 11° Gestión de Privilegios de usuario autorizados).

- La nomenclatura de cuentas es la inicial del primer nombre y el apellido del usuario. En caso de existir homonimia, se empleará la inicial del apellido materno.



5 Del uso de Internet

- El uso del servicio de internet es para fines institucionales (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo VII. Seguridad de Las Comunicaciones, Artículo 37° Conexión a Internet).
- El hardware y software que soportan al servicio de internet, son patrimonio institucional, por lo que 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 (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo II Control de Accesos a los Sistemas de Información, artículo 15° Generación y Accesos a Registros, artículo 36° Protección de la Información en la Red, de acuerdo a la normativa vigente y al pronunciamiento emitido por el Tribunal Constitucional en la Res. N° 1058-2004-AA/TC)
- La Gerencia de Informática o la Jefatura de Informática, es el área encargada de asignar los accesos para la salida a internet a fin de poder aprovechar la amplia gama de información para fines de investigación.
- El acceso a Internet debe ser solicitado por escrito (correo, oficio, memorándum) por el Jefe de área a la Gerencia de Informática o Jefatura de Informática, sustentando la necesidad de dicho acceso y los niveles de acceso a los cuales tendrá acceso el usuario.
- Todo acceso, reasignación o revocatoria será solicitado a la Gerencia de Informática o Jefatura de Informática.
- La descarga de archivos mayores a 2 Mb, debe efectuarse fuera del horario de trabajo a fin de no generar tráfico. Las descargas de archivos deben estar relacionados con las funciones del usuario y acordes a los objetivos institucionales o que por motivos laborales así lo requiera.
- No utilizar el servicio de internet para difundir información confidencial de la SUNARP a otros destinos no autorizados.
- No congestionar el servicio de internet producidas por descargas desautorizadas de archivos con capacidades superiores a las establecidas o mediante el envío de mensajes prohibidos, cadenas o spam.



6 Del Correo Electrónico Institucional

El uso del correo electrónico es para fines institucionales (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo VII. Seguridad de las Comunicaciones, Artículo 39° - Correo Electrónico).

Dado que el correo es para fines institucionales, el usuario podrá acceder a otras cuentas de correo privados. En ambos casos se respetará el derecho a la intimidad del trabajador, conforme a la normativa vigente.

Solicitud de Nuevo Correo

- El jefe de área debe solicitar a la Gerencia de Informática o Jefatura de Informática, la creación de una cuenta de correo para el usuario.



- El Jefe de Informática enviará la solicitud a la Gerencia de Informática de la Sede Central.
- En la Sede Central se procederá a verificar la relación de cuentas de correo existentes y cotejarlas siempre con la relación de licencias asignadas de correo electrónico de la oficina.
- Si existe disponibilidad, se procederá con la creación. En caso de no disponer de licencias, se informará al área solicitante indicándose que no es posible atender el pedido, salvo eliminación de alguna cuenta de correo existente que pertenezca al área solicitante y/o adquisición de licencias adicionales.
- Si se procede con la eliminación de cuenta de correo y se da pase con la creación de cuenta, debe indicarse :

Relación de cuenta de correo a eliminar

- Nombre de usuario

Relación de cuenta de correo a crear

- Nombre de usuario, área y cargo



- De acuerdo a la Resolución N° 107-2003-SUNARP/SN que aprueba la Directiva N°004-2003-SUNARP/SN, el uso del correo electrónico es para el personal de la institución. Para el personal contratado se le asignará una cuenta de correo genérica.
- En los casos de renuncia del personal, se procederá con la eliminación automática de la cuenta de correo, dado que una cuenta de correo equivale a una licencia.
- Es necesario que el área de Recursos Humanos mantenga informada a la Gerencia de Informática o Jefatura de Informática, del cese de las labores del personal a efectos de eliminar cuentas de usuario y accesos de red. Asimismo, al área encargada del control del personal contratado y/o las Jefaturas o Gerencias , deberá informar sobre la culminación del contrato para proceder con la eliminación de la cuenta asignada.

Mantenimiento de casillas de correo



- El software de correo empleado en la institución es Lotus Notes.
- Los usuarios para acceder al correo institucional, lo efectuaran a través de la versión del cliente Lotus notes instalado en el computador o vía web empleando un navegador.
- El usuario deberá efectuar periódicamente la depuración de sus correos electrónicos, en los siguientes casos :
 - ✓ Antes de salir de vacaciones
 - ✓ Antes de salir de licencia
 - ✓ Al mostrarle el mensaje de que la casilla se encuentra llena y debe depurar el mismo
 - ✓ Cuando el usuario lo considere necesario.

- Las casillas de correo, o base de datos de correo de cada usuario, esta conformado por los mensajes entrantes y salientes, así como los archivados en carpetas dentro del mismo software de mensajería.
- El servicio de mensajería, comunicará al usuario, cuando debe efectuar la depuración. El mensaje se activará cuando el usuario llegue al umbral (90% del tamaño de la base de datos asignada)
- En estos casos, el usuario deberá efectuar una depuración o eliminación de sus correos.
- En caso el usuario requiera mantener una copia de respaldo de todos sus mensajes, puede efectuar un Backup del mismo y almacenarlo en el disco duro del computador.

7 Del Software Instalado

- La Gerencia de Informática o Jefatura de Informática, es el área encargada de efectuar las instalaciones de software (licenciado y libre) en los equipos de cómputo de la institución.
- Los usuarios no podrán efectuar instalaciones de productos ya sea libres o personales, debe coordinarse con la Gerencia de Informática o Jefatura de Informática, a fin de resguardar la información de la Red de la SUNARP (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo VII. Seguridad de las Comunicaciones, artículo 36° Protección de la Información en la Red).
- La Gerencia de Informática o Jefatura de Informática, puede efectuar revisiones periódicas de los equipos de cómputo a fin de verificar que se cuenten con los software autorizados. En caso de detectar software no autorizado y no se encuentre en el acta previamente firmada por el usuario, se notificará del mismo al jefe inmediato del usuario.
- Para la instalación de un software, el usuario debe enviar su requerimiento, vía oficio autorizado por su jefe inmediato.
- La Gerencia de Informática o Jefatura de Informática, determinará si se dispone de la licencia de uso respectiva para la instalación. En caso de no contar con la licencia, el usuario deberá solicitar su adquisición mediante oficio dirigido a la Gerencia de Informática o Jefatura de Informática. Si es un software libre, la Gerencia de Informática o Jefatura de Informática, procederá a verificar dicho software, su funcionalidad, y ventajas antes de proceder con la instalación, así como la compatibilidad con el sistema operativo instalado.
- Luego de aprobado e instalado el software en el equipo del usuario, el usuario firmará el acta de conformidad de instalación y actualización del legajo de software instalados en su estación de trabajo.
- La Gerencia de Informática o Jefatura de Informática, procederá a actualizar el Inventario de Software adquiridos y que cuente con la respectiva licencia de uso.

7.1 De la Adquisición de Software

- El usuario debe indicar mediante documento el requerimiento del software para las labores que realiza en su área



Dicho documento debe indicar :

- Finalidad del uso del software,
- Software existentes en el mercado con similares características,
- Sustento del software elegido (si se indica marca y nombre de producto indicar si existe proceso de estandarización)
- Cantidad de instalaciones (para las licencias)
- Autorización del Jefe de Área

- La Gerencia de Informática o Jefatura de Informática, encargada de canalizar los requerimientos de los usuarios, llevará el registro del requerimiento, elevando a la Gerencia de Administración y Finanzas el Informe Técnico de Software correspondiente solicitando la adquisición.
- Se procederá a verificar la versión y licencia de software, así como el soporte que se brinde al mismo (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo VIII Desarrollo, Adquisición y Mantenimiento de Sistemas de Información, artículo 44° Adquisición de Sistemas de Información).
- Asimismo, en la Gerencia de Informática o Jefatura de Informática, se solicitará de ser el caso, una versión de demostración del software a efectos de validar su correcto funcionamiento con los distintos sistemas operativos instalados en los equipos. En caso de no ser compatible con la versión de sistema operativo del computador del usuario, deberá emplearse otra aplicación que sea compatible con el sistema operativo.
- Para los casos que el software a adquirirse sea necesario para el cumplimiento de las funciones, deberá validarse si al posible cambio del sistema operativo, las demás aplicaciones instaladas en el equipo funcionarían correctamente, caso contrario deberá evaluarse la posibilidad de elegir otro software.
- Se solicitará la aprobación de la adquisición del producto a la Gerencia General o Jefe de Zona Registral . En caso de aprobarse la adquisición se enviará las especificaciones a la Gerencia de Administración y Finanzas, mediante oficio. En caso de ser denegado su compra, se notificará al área solicitante.
- A la Gerencia de Administración y Finanzas se le enviará un oficio, adjuntando el proveído de aprobación de la Gerencia General, la solicitud de compra del software. En el se indicará las especificaciones técnicas del producto. La Gerencia de Administración y Finanzas se encargará de verificar y/o solicitar cotizaciones a los proveedores y efectuar el proceso de adquisición.
- Efectuado el proceso y habiéndose culminado, la Gerencia de Administración mediante Guía de ingreso, efectuará la recepción del software, el cual debe incluir : media kit original, licencia de uso, manuales. Debe contarse con la presencia de personal de soporte de la Gerencia de Informática o Jefatura de Informática para dejar constancia de lo recibido, en caso de alguna observación será notificado al momento de recibir el software.



- La Gerencia de Administración y Finanzas, mediante comunicación escrita, informará y hará entrega del software y licencia a la Gerencia de Informática o Jefatura de Informática, para su instalación y custodia.
- Se coordinará con el usuario solicitante del software, a efectos de coordinar la fecha de instalación.
- Al concluir con la instalación y puesta en producción del software, el usuario firmará el acta de instalación del software en su equipo, como constancia de instalación por parte de la Gerencia de Informática o Jefatura de Informática.
- La Gerencia de Informática o Jefatura de Informática, procederá a actualizar en el Inventario de Software el producto adquirido y mantendrá en custodia el mismo (media, licencia, manuales).
- El usuario tendrá un plazo de 48 horas, para verificar el correcto funcionamiento del software y posteriormente, emitirá la conformidad del software a la Gerencia de Informática o Jefatura de Informática.
- La Gerencia de informática o Jefatura de Informática, mediante oficio, comunicará a la Gerencia de Administración y Finanzas la conformidad por la instalación y funcionamiento del producto a efectos de culminar con los tramites respectivos (pago).



8 De los puntos de Red

8.1 Solicitud de punto de red

- En caso de ingresar un nuevo usuario y el ambiente donde se ubicará el usuario no dispone de un punto de red, el jefe de área del usuario, deberá solicitar la instalación del punto a la Gerencia de Informática o Jefatura de Informática.
- La Gerencia de Informática o Jefatura de Informática, verificará la existencia de punto de red en la ubicación del usuario. En caso de no existir, se solicitará a la Gerencia de Administración la instalación del punto de red.
- El proveedor coordinará con la Gerencia de Informática o Jefatura de Informática, a fin de verificar la ubicación del punto, su numeración y la conexión hacia los equipos de comunicación.
- Cuando se efectúe la instalación del punto de red por parte del proveedor contactado por la Gerencia de Administración y Finanzas, se verificará la conectividad de la estación a la red, tiempo de respuestas a fin de brindar la conformidad respectiva.



8.2 Solicitud de verificación de punto de red

- Cuando el usuario reporte problemas de conexión a los servidores e inclusive a internet, verificar el cable de datos que va de la estación al punto de red, posiblemente durante la limpieza del ambiente puede haber ocurrido una desconexión del punto.
- Proceder a desconectar el cable de red y volver a conectarlo.
- En caso no lograr comunicación, informar al área de Soporte Técnico de la Gerencia de Informática o Jefatura de Informática de la Sede Central y/o Zona Registral.



9 Del uso de los suministros

- Para sujetar un Diskette o Cd debe hacerse por los bordes y nunca por la parte interna, ya que es grabado magnéticamente y al contacto con alguna parte del cuerpo se desmagnetiza rápidamente (diskettes) o quedar huellas que impida su lectura.
- En el caso de los diskettes, no deben acercarse a ningún otro medio magnético (parlantes, pilas, imanes, etc.), ni de generación de calor (fuente de poder o a cualquier otro tipo de equipos como el CPU de la computadora), ya que esto podría causar la pérdida total o parcial de la información.
- Cuando se esté grabando, leyendo o borrando información (mientras se encuentre el indicador del drive encendido) no se debe levantar la tapa de protección, ni presionar el botón de expulsión del mismo; ya que esto ocasionará la aparición de sectores dañados en el Disco.
- Durante el uso de los suministros se debe tener en cuenta lo siguiente :

Diskettes

- No doblar los Diskettes, ni quitar la protección metálica del disco.
- No colocar peso sobre ellos, debiendo mantenerse en lugares apropiados (cajones especiales o porta diskettes).
- Evitar guardarlos en bolsillos, carteras o junto con cualquier otro artículo.
- No debe usarse clips, grapas o ligas para agruparlos.
- Revisar el buen estado de las etiquetas (que se encuentren bien adheridas al diskette), ya que ésta puede ocasionar que se atasque el disco a la hora de ser retirado de la disquetera.
- Se recomienda formatear el diskette antes de ser usado por primera vez, aunque indique que ya ha sido formateado en fábrica.
- No escribir o pintar en el diskette con ningún tipo de objeto puntiagudo de preferencia escribir la etiqueta antes de ser colocada.
- Evitar regrabar o modificar un archivo excesivamente; ya que esto ocasiona que se desgaste y debilite el medio magnético, por lo que se recomienda cambiar de diskette periódicamente, y usar los antiguos como copia de seguridad.

Cd's

- Mantenerlos dentro del estuche
- No apilar los Cd's unos sobre otros sin sus estuches respectivos
- Al limpiar el Cd, emplear un paño suave y no limpiar de manera circular, sino de adentro hacia fuera.

Memorias - USB

- Conectar preferiblemente a los puertos USB de la parte posterior del CPU.
- Nunca fuerce la conexión de la memoria al puerto USB, debe entrar completamente hasta el límite.
- Las memorias son para transportar información, no para trabajar sobre ellas. Lo preferible es grabar o copiar los datos en el disco duro y una vez culminado copiarlo a la memoria USB.



- Después de su uso expulse la memoria correctamente:

Windows XP

Click derecho sobre la letra de la unidad de la memoria > Expulsar, luego click derecho en el icono de la bandeja del sistema de la barra de tareas y click en "Quitar Hardware con seguridad", elige la unidad de la memoria y la expulsamos definitivamente.

Windows 98

Sólo con click derecho sobre la unidad > Expulsar
Una vez expulsada por software, verifique que el el indicador (luz o led) de la memoria que indica actividad esté apagado antes de retirarla.

- Una memoria puede dañarse si sufre algún golpe, caída o calentamiento

10 De las responsabilidades del usuario

Los usuarios tienen las siguientes responsabilidades :

De la Información

- Es responsable de efectuar el respaldo periódico de la información de su disco duro, dicha información debe permanecer en el local institucional.
- De utilizar los sistemas de la institución únicamente para fines aprobados por esta (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo IV Seguridad de Personal, artículo 22° Responsabilidades del Personal).
- De no utilizar la información para fines contrarios a los intereses de la institución.
- De no divulgar la información obtenida de los sistemas de la institución (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo I. Propiedades de la Información, artículo 7° Confidencialidad).
- De aceptar que toda la información conservada en los equipos informáticos (archivos y correos electrónicos residentes en servidores de datos centralizados y/o estaciones de trabajo) es de propiedad de la institución.
- De no realizar instalación de ningún tipo de software no homologado por la institución. La Gerencia de Informática o Jefatura de Informática, es el único autorizado a instalar aplicaciones y llevar el control de los mismos por cada equipo de la institución.
- De no detener o cancelar el proceso de actualización automática del software antivirus o cualquier otro que le sea instalado en su computador, así como desactivar la vacuna residente en memoria.
- El antivirus se encuentra programado para efectuar descargas automáticas desde internet, así como para ejecutar la búsqueda de virus en el disco duro, la cual esta programada a las 13:00 todos los días (hora de refrigerio). La búsqueda de virus es importante a fin de eliminar posibles virus en el sistema y prevenir daños posteriores.

De los accesos y contraseñas



- Al usuario se le otorgará cuentas de usuario y contraseña para las aplicaciones asignadas, aceptando las responsabilidades sobre el uso de dichas cuentas de usuario (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo II, Artículo 13° Gestión de Claves de Acceso de Usuarios).
- No debe revelar el usuario y contraseña otorgados.
- El uso de las claves es de plena responsabilidad del titular, así como el extravío, pérdida y uso indebido que terceras personas pudieran hacer del mismo, quedando la SUNARP liberada de toda responsabilidad
- No permitir la utilización de la cuenta de usuario por terceros.
- Desconectarse de la estación de trabajo correspondiente, cada vez que finalice con las tareas que en ella desarrolla, a fin de evitar el uso de la clave por otra persona o en su defecto haciendo uso del protector de pantalla con clave a fin de proteger la información.
- El intento de ganar acceso a recursos no asignados, tales como obtener ilegalmente la cuenta de usuario y/o contraseña de otro trabajador, modificar la configuración del equipo, será considerado intento de violación a la seguridad del sistema en el cual la institución se reserva el derecho de tomar las acciones pertinentes del caso.



De los emails

- El uso del correo es para fines institucionales (Directiva N°004-2006-SUNARP/GG, Reglamento de Políticas de Seguridad de Información, Capítulo VII, Seguridad de las Comunicaciones, Artículo 39° Correo Electrónico).
- No deberá enviarse correos con contenido de bromas, cadenas a fin de no saturar los enlaces y casillas de correo de otros usuarios.
- Efectuar la destrucción de todo mensaje cuyo origen es desconocido. En estos casos, no se deben contestar dichos mensajes y debe ser enviado una copia al administrador para que efectúe las tareas de seguimiento e investigación necesarias.

11 De las prohibiciones

El usuario queda prohibido a :



- Manipular los equipos informáticos
- Desconectar o conectar los equipos sin la autorización correspondiente, dado que pueden ocasionar daño en los mismos.
- Trasladar el equipo a una ubicación diferente de donde fue inicialmente instalado sin la coordinación previa con el personal de soporte de la Gerencia de Informática o Jefatura de Informática.
- Reasignar el equipo informático sin la autorización correspondiente de la Gerencia de Informática o Jefe de Informática.
- Retirar la etiqueta de inventario físico o el sello de seguridad del equipo.
- Modificar la configuración estándar del equipo.
- Instalar software sin la autorización correspondiente.
- Utilizar el equipo para juegos.

- Copiar y/o compartir archivos de música o video ajenos al interés de la institución.
- Desactivar el servicio antivirus de las estaciones de trabajo.
- Descargar programas en la computadora para uso personal y ajeno a la institución.

VII. ANEXOS

Anexo 1 Relación de equipos informáticos

Anexo 2 Uso adecuado de los equipos informáticos

VIII. VIGENCIA

- A partir del día siguiente de su publicación en la página Web.



[Handwritten signature]

Maria D. Cambursano Geronzi
Superintendente Nacional
de los Registros Públicos



ANEXO 1

RELACION DE EQUIPOS INFORMATICOS

Cámara digital
Capturador de imágenes o Escáner
Computador de escritorio (PC, estación de trabajo)
Computadora personal, portátil (Notebook)
Concentrador (Switch, Hub)
Estabilizador
Impresora (matricial, inyección, láser)
Lector Código de Barras
Lector de disco compacto
Lector de cinta magnética
Monitor
Mouse
Multifuncionales
Palm
Proyector
Refrendadora
Ruteador de red (Router)
Servidor
Unidad Central de Proceso (CPU)
Unidad de Arreglo de disco(Disk Array)
Unidad de disco ZIP
Unidad para copia de seguridad (Tape Backup Externo)
Unidad para grabación de disco compacto
Teclado
UPS



ANEXO 2

USO ADECUADO DE LOS EQUIPOS INFORMATICOS

1. Del cuidado de las computadoras:

GENERALES

- No exponer el equipo a : líquidos, humedad excesiva, altas temperaturas
- No colocar objetos cerca y/o sobre el equipo a fin de impedir su ventilación
- Al termino de las labores, el usuario deberá apagar el equipo (CPU, monitor, impresora) .
- Los equipos informáticos deben estar conectados al tomacorriente de cómputo (dispone de una conexión para el pozo a tierra) el cual se encuentra estabilizada.
- Los equipos pueden estar conectados a un supresor de picos, estabilizador o al tomacorriente para cómputo
- No se debe conectar a la red de energía eléctrica estabilizada o tomacorrientes para cómputo los siguientes : ventilador, calculadora, cargadores, fotocopidora, microondas, trituradora de papel, ventiladores, radio, TV, entre otros.

ENCENDIDO Y APAGADO

Para mantener el buen estado de los equipos se recomienda el siguiente orden para el encendido :

- a- Estabilizador y/o Supresor de Picos.
- b- UPS (si se tuviera).
- c- CPU.
- d- Monitor.
- e- Impresora.

El apagado de los mismos se realizará en orden inverso.

- **C.P.U.** Mantener la parte posterior del CPU libre en por lo menos 10 cm., para así asegurar una ventilación mínima adecuada y evitar el resquebrajamiento de los cables y conectores.
- **Monitor.** No cubrir ni colocar en la rejilla superior ningún objeto, mientras éste permanezca encendido, a fin de garantizar su debida ventilación. Se recomienda ubicarse a una distancia mínima de 60 cm. de la pantalla. Con esto no sólo reducirá su exposición a las radiaciones, sino que puede ayudar a reducir el esfuerzo visual.
- **Teclado.** Mantener fuera del teclado grapas, clips, uñas, cabellos, entre otros, ya que éstos podrían causar la perforación de la membrana interna; así como tampoco ingerir ningún tipo de alimentos sobre el mismo, con el fin de evitar se introduzcan en el interior y ocasionen un cruce de función, como también el mal funcionamiento de alguna tecla.



- **Mouse.** Desplazar el Mouse sobre una superficie plana y limpia, de tal manera que no se ensucien los rodillos, además verificar el libre desplazamiento de éste y de su cable, sin que nada lo obstruya.
- **Impresora.** El manejo de las impresoras es por lo general a través de los botones del panel. Dependiendo del tipo de impresora:
 - Matricial no mover el rodillo en caso de estar encendido el equipo,
 - Inyección, en caso de atasco de papel, retirar con cuidado dado que puede dañarse el sensor de arrastre de papel y quedar inutilizable el equipo.
 - Láser, no manipular el equipo mientras este encendido en especial el fusor (pieza que se mantiene a alta temperatura y permite la adhesión del tóner al papel).

La limpieza interna de los equipos estará a cargo del personal de informática y/o proveedor.

DEL CUIDADO DE LOS EQUIPOS DE IMPRESIÓN

- El papel a emplearse en las impresoras debe ser de las características que figuran en los manuales de usuario (calidad, tipo y peso) y recomendados por el fabricante.
- Considerando que existe amplia variedad en marca y modelo de las impresoras deberá tenerse presente lo siguiente:

Papel Bond (todas las impresoras Laser e Inyección)

- Gramaje : 80 gramos
- Alisado : ambos lados
- Tamaños : A4, A3, Oficio, Carta

Papel continuo (impresoras matriciales)

- Gramaje : mínimo de 60 grs
- Tamaños : 9 7/8" X 11", 14 7/8" X 11" y demás tamaños personalizados

- No debe emplearse papel reciclado, así como tampoco que contengan clips o grapas, pues puede ocasionar daño en los mecanismos de la impresora (rotura de sensores, rodillo, fusores).
- No debe imprimirse transparencias en las impresoras láser salvo que el modelo de la impresora tenga el soporte que lo permita. En todo caso antes de emplear transparencias, consultar con el área de Soporte Técnico de Informática.
- Las impresoras matriciales deben mantenerse con sus cubiertas para evitar el ingreso de polvo a los mecanismos de impresión.
- Para el caso de las impresoras láser debe colocarse papel suficiente en la bandeja automática, a fin de evitar el abrir y cerrar de la bandeja lo cual puede originar la rotura de los mecanismos. Dado que algunas áreas tienen restricciones en cuanto a la cantidad de papel empleado por el personal, puede hacerse uso de la bandeja manual a fin de colocar el papel necesario por cada persona del área y evitar el deterioro de la bandeja automática.



DE LA LIMPIEZA DE LOS EQUIPOS

- La limpieza externa de los equipos puede ser realizada por personal de limpieza, por lo tanto la responsabilidad es sobre la empresa encargada de la del Servicio de Limpieza.
- Los artículos de limpieza debe ser superficial en CPU, Teclados y Mouse
- Deberá tenerse especial cuidado al limpiar el teclado a fin de no despintar el valor impreso en cada tecla. Asimismo sobre las etiquetas relacionadas a inventario de equipos, series de sistema operativo y del equipo.
- En el caso de los equipos con pantalla plana, portátiles o Notebook, **NO EMPLEAR KITS DE LIMPIEZA** solo con una paño o franela seca (sin restos o residuos de algún liquido) pues puede restar brillo.
- Los materiales a emplearse pueden ser :
 - Alcohol isopropílico (especial para equipos electrónicos)
 - Glasex
 - Cera o pasta para limpieza de equipos de computo.
 - Franela

Los líquidos o cera, deberán aplicarse sobre la franela y no directamente sobre el equipo.

DE LOS EQUIPOS PORTÁTILES

- Al emplear un equipo portátil o Notebook, deberá coordinarse con Soporte Técnico de la Gerencia de Informática o Jefatura de Informática, antes de ser conectados a la red o suministro eléctrico para cómputo.
- El equipo debe contar con batería a fin de que esta se cargue y disponga de autonomía cuando no se encuentre con el suministro eléctrico.
- Las baterías deben guardarse en un lugar seco y a la temperatura que recomienda el fabricante (dependiendo del modelo), se sugiere coordinar con personal de informática.
- Al viajar con un equipo portátil, este no debe ir en la bodega sino como equipaje de mano.

