R/Alc. # 815 - 2009 - MPCP.
23 - 12 - 2009.

Municipalidad Provincial de Coronel Portillo

GERENCIA DE PLANEAMIENTO PRESUPUESTO Y RACIONALIZACIÓN

SUB GERENCIA DE RACIONALIZACIÓN

DIRECTIVA Nº 011 – 2009 – MPCP – GPPR – SGR

"SISTEMA DE COMUNICACIÓN E INFORMACIÓN EN RED"

Sub Gerencia Racionalización

Pucallpa - Perú
2009

DIRECTIVA Nº 011 – 2009 – MPCP – GPPR – SGR

"SISTEMA DE COMUNICACIÓN E INFORMACIÓN EN RED"

Artículo 1º.- OBJETIVOS

Establecer los mecanismos necesarios para promover y establecer una cultura de dinamismo en el uso y transparencia del acceso a la información que genera y administra los sistemas de comunicación implementados en la Municipalidad Provincial de Coronel Portillo.

Artículo 2º.- FINALIDAD

Asegurar el acceso a toda información relevante para el personal que labora en la Municipalidad Provincial de Coronel Portillo, con el fin de promover la transparencia en la gestión del Estado; fortalecer el proceso de la toma de decisiones y facilitar la participación de los involucrados en la definición de las políticas del Sector Publico.

Artículo 3º.- ALCANCE

El contenido de la norma, es de aplicación para todos los funcionarios, empleados de confianza y servidores de todas las unidades orgánicas de la Municipalidad Provincial de Coronel Portillo.

Artículo 4º.- BASE LEGAL

- Constitución Política del Perú.
- Ley 27444, "Ley de Procedimiento Administrativo General"
- Decreto Ley Nº 26162, Ley del Sistema Nacional de Control.
- Resolución de Contraloría Nº 320-2006-CG, que aprueba las "Normas Técnicas de Control Interno para el Sector Público".
- D.S. Nº 066-2001-PCM, que aprueba los "Lineamientos de Política General para promover la masificación del acceso a internet en el Perú."
- Resolución Jefatural Nº 088-2003-INEI, que aprueba Directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de Administración Pública".
- Ordenanza Municipal Nº 005 – 2009 – MPCP del 20 de marzo del 2009 que aprueba el "Manual de Organizaciones y Funciones de la Municipalidad Provincial de Coronel Portillo"

Artículo 5º.- DISPOSICIONES GENERALES

5.1. Los servicios de red que se proporcionarán a los usuarios podrán ser todos o algunos de los que se detallan a continuación:

- Acceso a los servicios de la Red de Datos y Comunicaciones de la Municipalidad Provincial de Coronel Portillo.
- Acceso a los servicios de correo electrónico.
- Acceso a los servicios de mensajería electrónica.
- Acceso a los servicios de internet.
- Acceso a los servicios de intranet
- Acceso a los servicios FTP (File Transfer Protocol.)
- Acceso a los servicios de acceso remoto RAS (Remote Access Service)
- Acceso a los servicios de compartición de dispositivos periféricos.
- Las funciones propias del usuario determinaran de que servicios y recursos podrá disponer.
- Remota y protocolo de transferencia de archivos-FTP

5.1.1. Cada usuario de red cuenta obligatoriamente con un nombre de usuario (login) y una clave de acceso (password), los cuales posibilitan su acceso. Estos parámetros son personales, confidenciales e intransferibles.

5.1.2. El trabajador que accede a red no podrá, sin previo conocimiento de su Jefe inmediato (con documento), realizar cambios para la optimización del equipo y sin tener en cuenta los estándares de red ya establecidos.

5.1.3. Para tener acceso a internet e intranet de la Institución, se necesita una dirección **TCP/IP** para cada máquina, las que son asignadas manualmente (**TCP/IP estáticos**). Mientras la modalidad de asignación sea a través de **TCP/IP** estáticos queda terminantemente prohibido utilizar direcciones específicas sin la autorización del Jefe inmediato y de la Sub Gerencia de Estadística e Informática.

5.1.4. El usuario que utilice un equipo informático conectado a red, deberá tener cuidado de la información que maneja a fin de evitar infectar con virus a la red y causar pérdidas irreparables de información.

5.1.5. Queda prohibido crear carpetas o archivos personales en cualquier unidad pública de la red (la Data).

5.1.6. **\\Respaldo\Compartir**, solo ha sido puesto a disposición de los usuarios para compartir archivos estrictamente necesarios y de manera temporal, significa que la información almacenada no se encuentra segura, salvo que se solicite formalmente su resguardo a la Sub Gerencia de Estadística e Informática.

5.1.7. Para evitar congestión de información en la red (Data) y por la inoperatividad de los siguientes programas y sistemas; Trámite Documentario, Sistema de Caja, Sistema de Rentas (SIAT), Sistema de Planillas, Sistema de Logística Almacén y Patrimonio (Siloalpa), Sistema de Transito (SIIT), Sistema de Control de Asistencia, Sistema de Contratos, etc.; se procederá a eliminar archivos de fechas pasadas, musicales, videos y otros, con la finalidad de proporcionar funcionalidad a los sistemas mencionados y de importancia para la buena gestión de la Municipalidad Provincial de Coronel Portillo.

5.1.8. Cuando se utilice archivos privados, se entenderá que los documentos en estas cuentas serán de carácter oficial, y por motivos justificados; se creará una carpeta con restricciones de uso privado (información confidencial), para lo cual deberá coordinarse con la Sub Gerencia de Estadística e Informática con la finalidad de que la persona que administra la red, otorgue el permiso correspondiente y dicha información se custodie en el Servidor de Archivos.

5.2 Disposiciones para el uso de Correo Electrónico

5.2.1 El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre los trabajadores de la Municipalidad Provincial de Coronel Portillo, no es una herramienta de difusión indiscriminada de información. A través del **e-mail** se podrá remitir información general como, documentos, memorandos, cartas, etc.

5.2.2 Para identificar al remitente, al pie de cada mensaje se deberá enviar una identificación tipo auto firma, que permitirá al receptor identificar formalmente a su autor, de manera que esté vinculada únicamente a él y a los datos para garantizar así la identidad del titular y que éste no pueda desconocer la autoría del documento. No incluir la dirección de correo electrónico en la firma, porque se incluye de manera automática en la cabecera del mensaje.

5.2.3 Para el reenvío de un mensaje, incluir el mensaje original, con la finalidad de que el destinatario conozca el contexto del mensaje que recibe. No incluir archivos adjuntos que se puedan haber recibido originalmente, a no ser que se haya realizado modificaciones al(os) archivos, y deberá citarse siempre la fuente de origen y/o los autores, para respetar los derechos de propiedad intelectual.

5.2.4 Evitar enviar mensajes a personas que no se encuentren registrados en las listas globales, a menos que sea por un asunto oficial que involucre a toda la institución, asimismo revisar que el mensaje sea enviado a los usuarios correctos.

5.2.5 Los usuarios de las cuentas de **correo electrónico** son responsables de las actividades que realizan con las cuentas proporcionadas por la institución. Cuando el usuario deje de usar su estación de trabajo deberá de cerrar el software de correo electrónico, para evitar que otra persona use su cuenta, por lo tanto es responsable de todo aquello que en ella se realice. El tener una cuenta de correo institucional compromete y obliga a cada usuario a aceptar las normas establecidas por la institucion y a someterse a ellas.

5.2.6 Los usuarios que tienen asignada una cuenta de correo electrónico Institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes que desea conservar, agrupándolos por temas en sus carpetas personales.

5.2.7 El uso de antivirus, para los servidores y estaciones de trabajo, deben activarse de tal forma que se verifiquen todos los archivos, aun los que se encuentren compactados, y la acción por defecto a seguir revisará que el cliente antivirus se encuentre actualizado

5.2.8 Los servidores de correo deben contar con antivirus. Si el mensaje que detecta contiene un virus o "troyano" que no puede ser removida, debe eliminar el mensaje inmediatamente. Así mismo deberá informar, al destinatario de correo, el nombre del remitente y que su mensaje fue borrado por contener virus. Revisar todos los días que el análisis del antivirus se active automáticamente, en caso contrario comunicarse con la Sub Gerencia de Estadística e Informática y seguir todas las instrucciones impartidas.

5.2.9 La Sub Gerencia de Estadística e Informática asignará las cuentas de correo electrónico institucional a los trabajadores, el Jefe inmediato deberá informar sobre el ingreso de nuevo personal, de la misma forma se debe proceder con la eliminación de los correos en caso de cese del personal. Los usuarios que tienen asignada una cuenta de correo electrónico Institucional, deben establecer una contraseña, en la que no deben usar datos que identifiquen al usuario o frases comunes, debe usar la combinación de mayúsculas, minúscula y números. La contraseña la deben mantener en secreto, la cuenta del correo es personal e intransferible, se recomienda cambiar periódicamente el password (contraseña).

5.2.10 El nombre de la cuenta de correo electrónico institucional debe estar formado por las letras iniciales del **nombre del cargo,** seguido

inmediatamente el **nombre de la oficina al cual corresponde y las iniciales mpcp** (Municipalidad Provincial de Coronel Portillo), ligado con el símbolo **@gmail.com** de acuerdo a lo establecido por la directiva Nº 010-2002-INEI/DTNP "Normas Técnicas para las Asignación de Nombre de Dominio de la Entidades de Administración Pública".

5.2.11 El administrador de la red para asignar las cuentas, distinguirá los tipos de empleados y la duración de las cuentas:

- **Empleados nombrados o permanentes:** la duración de la cuenta será mientras trabajen en la institución.
- **Empleados contratados por funcionamiento:** la duración de la cuenta será de un año fiscal o por la duración del contrato, el más corto de los dos.
- **Empleados por contrato eventual o por proyectos:** la duración de la cuenta será de un semestre o por la duración del contrato, el más corto de los dos, a quienes se les solicitará un cambio de contraseña cada 90 días.
- **Practicantes:** se les asignará una cuenta temporal la cual se mantendrá mientras practique en la institución (3 meses por lo general). Dicha cuenta será renovada, siempre que se informe sobre la vigencia del convenio de prácticas. Se le pedirá que cambie su contraseña por lo menos una vez. El practicante tendrá la responsabilidad de pedir la activación de su cuenta la primera vez con autorización de su jefe.
- **Gerentes, Sub Gerentes o Jefes de Oficina:** a cada uno, se le asignará una cuenta genérica de E-Mail que se usará para recibir correspondencia general interna o externa. La secretaria de la unidad orgánica correspondiente estará a cargo de la cuenta o quien designe el jefe. Se le asignará una contraseña temporal establecida por el administrador, esta contraseña podrá ser cambiada por el usuario en el momento que lo requiera. La contraseña deberá renovarse cada semestre como mínimo.

5.2.12 La Sub Gerencia de Estadística e Informática será responsable de mantener el servicio en línea; de resolver cualquier contingencia en el menor tiempo posible; capacitar al personal en el uso del correo electrónico institucional, asignación de contraseñas a su correo y sobre las diferencias entre el correo electrónico institucional y el correo electrónico privado.

5.2.13 La Sub Gerencia de Estadística e Informática debe garantizar la privacidad de las cuentas del correo electrónico institucional; además establecerá los procedimientos para la detección de faltas graves cometido por los usuarios mediante correo electrónico.

5.2.14 Se considera el mal uso del correo electrónico institucional, a las siguientes actividades:

a) Utilizar el correo electrónico institucional para cualquier propósito comercial o financiero ajeno a la institución.

b) Participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.

c) Distribuir mensajes con contenidos sexuales, terroristas u ofensivos.

d) Falsificar las cuentas de correo electrónico

e) Utilizar el correo electrónico institucional para recoger los mensajes de correos de otro proveedor de internet.

5.2.15 Se considera, adicionalmente, malas prácticas en el uso de correo electrónico:

- La difusión de contenidos considerados inadecuados o que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.
- Difusión de publicidad masiva no autorizada a cualquier otro tipo de correo no solicitado, "**spam**".
- Ataques con objeto de imposibilitar o dificultar el servicio, "**mail bombing**".
- Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de las líneas, de la capacidad del servidor de correo, o del espacio del disco del usuario.
- Suscripción indiscriminada a listas de correo. Es una versión de "mail bombing", en que los ataques no vienen de una sola dirección, sino de varias, los cuales son mucho más difíciles de controlar.
- No utilizar los servicios con fines comerciales o publicitarios.
- El usuario no deberá usar los servicios para amenazar, coaccionar, extorsionar, injuriar o calumniar a cualquier persona.
- Está prohibido usar los servicios para realizar conductas discriminatorias, actividades ilícitas o que atenten contra los derechos de las personas y propagar información falsa, engañosa o que pueda causar pánico.

5.2.16 La Sub Gerencia de Estadística e Informática sancionará con la cancelación de la cuenta de correo, el envío de mensajes a foros de discusión (listas de distribución y/o newsgroups) que comprometan la información de la institución o violen las leyes del Estado Peruano, sin perjuicio de poder ser sujetos de otras sanciones y/o penalidades derivadas de tal actividad.

5.2.17 Se considera falta grave que deberá tener en cuenta el Jefe inmediato del usuario que facilita u ofrece la cuenta y/o buzón del correo electrónico institucional a terceras personas.

5.3 Disposiciones para el acceso a la página Institucional

5.3.1 La Sub Gerencia de Estadística e Informática es responsable de la administración de la pagina web, la información que contenga la página debe estar siempre en condiciones operativas para quienes accedan a la misma y puedan recorrerla sin problemas, sin encontrar fallas, faltas o cualquier tipo de anomalía.

5.3.2 El encargado de la página: deberá verificar, añadir o modificar toda la información que se considere necesaria, colocar en los formatos establecidos y verificar el correcto funcionamiento dentro de la estructura de programación, garantizando que la información colocada en la página se efectué según las especificaciones y procedimientos adecuados.

5.3.3 El acceso a la web será restringido, y solo tendrán acceso personas autorizadas, para evitar daños que afecten la operatividad. El administrador del servicio deberá tener un sistema de seguridad, por ejemplo, en barreras de protección como antivirus, firewalls, etc., que impidan los accesos no autorizados.

5.3.4 La información que contenga a página web debe estar en condiciones operativas y completas. Por lo tanto la integridad y veracidad de la información que se muestra en una página web es uno de los factores más importantes de la seguridad, pues de él dependen el interés y la credibilidad de la página. Por lo tanto la información que es agregada o modificada debe estar en condiciones de integridad, y mantenerse hasta que termine el proceso de actualización y modificación.

5.3.5 La institución tiene una página oficial con la siguiente dirección ***www.municportillo.gob.pe;*** se recomienda a la Gerencias, Sub Gerencias y Oficinas tener páginas propias, las mismas que pueden ser alojadas en el servidor de "web" de la institución, donde solo se publicará información para el cumplimiento de los objetivos y no con fines de lucro, dentro del marco de la normatividad vigente.

5.6.3 Responsabilidades de los usuarios

- Mantener confidencialidad de la información contenida en los sistemas, especialmente aquella concerniente a la gestión administrativa, del personal y otros, protegidos por Ley.
- Imprimir la información necesaria para efectuar la tarea a realizar y destruir informes con datos confidenciales una vez terminado su revisión.
- La información ingresada o suministrada para la entrada a los sistemas administrativos será la más correcta. No se entrará o se suministrará datos que sean incorrectos, parcialmente incorrectos, o falsos, ni se retendrá información.
- **Las contraseñas, códigos de acceso y números personales de identificación suministrados al usuario serán personales y por ende, cada uno será responsable de su uso.** El usuario deberá mantener la confidencialidad de su(s) contraseña(s), código(s) de acceso y números(s) personal(es) de identificación y no permitirá su uso por otra persona.
- Toda actividad generada con los recursos de información de la institución deberá ser para uso legítimo y de carácter oficial. Se prohíbe todo uso personal de los recursos de información. Cualquier uso indebido, actividad sospechosa o ilegal, concerniente a la seguridad de las cuentas o de los recursos de la información se informará inmediatamente a la Sub Gerencia de Estadística e Informática.
- El usuario que es custodio del equipo informático es también responsable de su contenido. Deberá tomar medidas para evitar el acceso no autorizado al equipo, a su contenido, instalación ilegal de programas, almacenamiento de información y de trabajo no relacionado a las actividades que realiza su unidad orgánica o la institución.

Artículo 6º.- DE LAS PROHIBICIONES ESTABLECIDAS

6.1. Las prohibiciones que a continuación se detallan, describen las conductas indebidas:

a) Alterar los sistemas y configuración del equipo de computación y de comunicación sin autorización de la Sub Gerencia de Estadística e Informática.

b) Interrumpir o interferir en los recursos de comunicación y de computación.

5.4.4 Se espera que el usuario realice sus propias búsquedas en el internet, pero en caso de requerir apoyo al respecto, el personal de la Sub Gerencia de Estadística e Informática proporcionará las orientaciones necesarias.

5.4.5 Se restringirá automáticamente el acceso a internet a usuarios que naveguen en páginas no productivas como: páginas de adultos, chat, descargas de Mp3 y/o videos. La Sub Gerencia de Estadística e Informática emitirá un informe de amonestación dirigido a su Jefe inmediato superior en caso de hacer uso de las páginas restringidas o prohibidas.

5.4.6 Es restringido el uso de los programas de mensajería online: Yahoo, Messenger. Esta medida obedece principalmente a pérdida de tiempo y recursos de la institución, consumo excesivo del ancho de banda de nuestro acceso a internet por dichos programas así como también la propagación de virus y correos spam por estos medios.

5.5 Procedimientos de Digitalización, Impresión y FTP

5.5.1 El uso del equipo de digitalización de documentos (scanner) e impresión son exclusivamente para actividades institucionales y de actividades relacionadas con el trabajo del usuario, quedando estrictamente prohibido la digitalización e impresión de:

- ✓ Todo tipo de billetes emitidos por el Banco Central de Reservas del Perú.
- ✓ Todo tipo de moneda circulante de países extranjeros.
- ✓ Todo tipo de títulos de créditos emitidos por el gobierno, los estados o instituciones bancarias.

5.5.2 El personal deberá imprimir en las impresoras de sus respectivas oficinas. El papel destinado a las impresiones será proporcionado por el Jefe inmediato del área que requiere dicha impresión.

5.5.3 El **FTP (protocolo de transferencias de archivos)** es la transferencia de archivos entre sistemas conectados a una red TCP/IP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar al servidor para descargar archivos desde el, o para enviar nuestros propios archivos independientemente del sistema operativo utilizado en los equipos.

5.6. Obligaciones y Responsabilidades del personal de la Sub Gerencia de Estadística e Informática (Unidad de Informática y Usuario)

5.6.1 Obligaciones del administrador de los servicio s de red.

El administrador de la red deberá ser personal de planta de la institución, de preferencia nombrado y de reconocida integridad moral, ética y profesional,

púes tendrá bajo su responsabilidad la administración de la información procesada en red. Será designado mediante memorando del Gerente, y realizará las siguientes funciones:

a) Administrará la información de acuerdo a las Políticas de Seguridad de Información.

b) Mantendrá funcionando los servicios que le corresponde administrar.

c) Velará por la privacidad de los servicios de red; y solo pueden suministrar información de quienes los utilizan a las autoridades competentes.

d) Impedirá que circule información que afecte los intereses y fines de la institución.

e) Implementará los medios tecnológicos de seguridad adecuados para cada tipo de servicio.

f) Reconocerá y acatará las disposiciones en materia y de seguridad informática.

g) Informará oportunamente a quienes corresponda, según el usuario, sobre el incumplimiento de las reglas sobre el uso de los servicios de tecnología informática y de telecomunicaciones de la institución.

5.6.2 Obligaciones del personal de soporte informático

- El personal de soporte técnico no podrá adoptar medidas para la configuración de los equipos informáticos, que no sean de conocimiento del administrador de la red, y que vayan en contra de los estándares establecidos para su administración.
- El personal de soporte técnico, bajo ninguna circunstancia, configurará claves sin previa información a su Jefe inmediato. Asimismo no podrá ingresar a un equipo para configurar o realizar cambios sin tener en cuenta estándares y políticas establecidas para su administración.
- Informar a los usuarios sobre variaciones en la prestación de los servicios, funcionamiento y la forma como debe ser utilizado asi como brindar el soporte técnico oportuno para ello.
- El personal de soporte informático, que incurra en incumplimiento a lo establecido en la presente directiva, será sancionado de acuerdo a la falta cometida, sin perjuicio de los responsables civiles y penales correspondientes.

5.6.3 Responsabilidades de los usuarios

- Mantener confidencialidad de la información contenida en los sistemas, especialmente aquella concerniente a la gestión administrativa, del personal y otros, protegidos por Ley.
- Imprimir la información necesaria para efectuar la tarea a realizar y destruir informes con datos confidenciales una vez terminado su revisión.
- La información ingresada o suministrada para la entrada a los sistemas administrativos será la más correcta. No se entrará o se suministrará datos que sean incorrectos, parcialmente incorrectos, o falsos, ni se retendrá información.
- **Las contraseñas, códigos de acceso y números personales de identificación suministrados al usuario serán personales y por ende, cada uno será responsable de su uso.** El usuario deberá mantener la confidencialidad de su(s) contraseña(s), código(s) de acceso y números(s) personal(es) de identificación y no permitirá su uso por otra persona.
- Toda actividad generada con los recursos de información de la institución deberá ser para uso legítimo y de carácter oficial. Se prohíbe todo uso personal de los recursos de información. Cualquier uso indebido, actividad sospechosa o ilegal, concerniente a la seguridad de las cuentas o de los recursos de la información se informará inmediatamente a la Sub Gerencia de Estadística e Informática.
- El usuario que es custodio del equipo informático es también responsable de su contenido. Deberá tomar medidas para evitar el acceso no autorizado al equipo, a su contenido, instalación ilegal de programas, almacenamiento de información y de trabajo no relacionado a las actividades que realiza su unidad orgánica o la institución.

Artículo 6º.- DE LAS PROHIBICIONES ESTABLECIDAS

6.1. Las prohibiciones que a continuación se detallan, describen las conductas indebidas:

a) Alterar los sistemas y configuración del equipo de computación y de comunicación sin autorización de la Sub Gerencia de Estadística e Informática.

b) Interrumpir o interferir en los recursos de comunicación y de computación.

c) Acceder a información, cuentas, archivos o correo electrónico de otros usuarios sin su autorización.

d) Falsa representación o usurpación de la identidad de otro usuario en los medios de comunicación.

e) Instalar, copiar, distribuir o usar programas en violación a las leyes estatales y/o directivas o reglamentos internos de la institución.

f) Uso de cuentas por otro usuario para el cual no fue registrado, salvo que cuente con su autorización y se demuestre que fue totalmente necesario.

g) Permitir o facilitar el acceso a los recursos de información a usuarios no autorizados.

h) Usar los recursos de información para interferir con el uso de los recursos compartidos y actividades legítimas de otros usuarios, incluyendo actividades para estudios, investigaciones, gestiones y operaciones administrativas.

i) Usar los recursos de información para actividades ilegales o no aceptadas, según las leyes, reglamentos o políticas aplicables. Estas actividades, incluyen pero no necesariamente se limitan a accesos no autorizados, material pornográfico, amenazas, hostigamiento, difamación, robo y copiar o distribuir ilegalmente programas pertenecientes a la institución.

6.2. El usuario, que sea sorprendido incurriendo en los compartimientos antes señalados, el superior inmediato comunicará por escrito a la Sub Gerencia de Estadística e Informática con copia a las demás unidades orgánicas para establecer las sanciones correspondientes.

Artículo 7º.- SANCIONES POR EL USO INDEBIDO DE LOS EQUIPOS INFORMÁTICOS

7.1. Las violaciones a las políticas y directivas establecido por la MPCP para el uso y administración de los equipos informáticos constituyen un uso indebido de los recursos. Las personas que violen la presente directiva serán sancionadas por las autoridades competentes de nuestra institución y pueden ser objeto de acciones disciplinarias y legales incluyendo las cancelaciones de privilegios de uso de equipos de computación. El usuario que sea encontrado responsable del mal uso de los recursos informáticos recibirá sanción administrativa-pecuniaria de acuerdo a lo siguiente:

a) Equipo mal operado (funcionamiento).

b) Equipo parcialmente sucio.

c) Equipo con software innecesario
d) Mala conexión por reubicación de quipos.
e) Equipo totalmente sucio.
f) Equipo con virus informáticos.
g) Equipo usado con fines particulares.
h) Equipo abierto son autorización.
i) Equipo con cambio de piezas sin informe técnico.
j) Equipos con juegos o pornografías.

7.2. Inicialmente el usuario será amonestado por su Jefe inmediato de manera escrita con copia a su File Personal. Si el usuario es reincidente habrá cometido falta grave y pasible de imposición de sanción por parte de la comisión de Procesos Administrativos y Disciplinarios, quienes tendrán que evaluar la naturaleza y gravedad de la infracción, el daño causado y la reincidencia en la comisión, y se aplicará la sanción prevista para la infracción de mayor gravedad.

7.3. Si el usuario hubiere retirado o cambiado piezas del equipo informático sin conocimiento o autorización de la Sub Gerencia de Estadística e Informática, se le aperturará un proceso administrativo (reposición de la pieza dañada o reposición de la PC en un plazo que no excederá los 20 días hábiles) sin perjuicio de las responsabilidades civiles y penales que le correspondan; el monto será establecido por la Sub Gerencia de Logística.

7.4. Constituyen infracciones muy graves, además de las tipificadas, el incumplimiento de las obligaciones referidas a salvaguardar la inviolabilidad y el secreto de las comunicaciones y la violación de las normas sustanciales del **Código de Ética y conducta de Servicio Público.**

Artículo 8º.- DISPOSICIONES COMPLEMENTARIAS

8.1 Todos los funcionarios directivos y servidores que requieran del uso de las computadoras, periféricos y servicios informáticos en red, están obligados a conocer y respetar cada uno de los puntos contemplados en la presente directiva, con el objeto de no incurrir en faltas sujetas a sanción.

8.2 Es responsabilidad del funcionario o directivo hacer de conocimiento del personal a su cargo, sobre lo estipulado en la misma y exigir su fiel cumplimiento.

8.3 El Órgano de Control Institucional, cautelará según su competencia, el cumplimiento de lo dispuesto en la presente directiva.

Artículo 9º.- DISPOSICIONES FINALES

9.1 La Institución no se hace responsable de la información emitida a través de la red, por el uso mal intencionado o ilegal de la misma por parte de sus usuarios, o el daño causado a terceros.

9.2 La Sub Gerencia de Estadística e Informática a través de la Gerencia de Planeamiento, Presupuesto y Racionalización se encargará de la actualización y/o cumplimiento de lo dispuesto en la presente Directiva.

9.3 Déjese sin efecto las disposiciones internas, en tanto se opongan a la presente Directiva.

GERENCIA DE PLANEAMIENTO, PRESUPUESTO Y RACIONALIZACIÓN
Sub Gerencia de Racionalización