GOBIERNO REGIONAL DE LORETO
GERENCIA GENERAL REGIONAL

OFICINA EJECUTIVA DE DESARROLLO INSTITUCIONAL E INFORMATICA

DIRECTIVA GENERAL Nº 004 - 2011-GRL-GGR/OEDII

"NORMAS PARA EL USO DE COMPUTADORAS, INTERNET Y CORREO ELECTRONICO EN EL GOBIERNO REGIONAL DE LORETO"

IQUITOS, MARZO DEL 2011

1. OBJETO

La presente Directiva tiene por objeto, lograr la optimización del Uso de las computadoras, del Ancho de Banda y el Correo Electrónico, estableciendo su uso eficiente y una adecuada distribución de los recursos informáticos en las diversas dependencias de la Sede Institucional.

2. FINALIDAD

La presente Directiva tiene por finalidad, normar el uso adecuado de las computadoras y regular los procedimientos para la determinación de los criterios de asignación de Ancho de Banda y de Uso de Correo Electrónico según las necesidades, relevancia y nivel jerárquico del Usuario de Internet según criterio técnico y racional que adopte la oficina de Informática en el marco de modernización del Estado y la optima disponibilidad de los recursos del Estado.

3. BASE LEGAL

- ✓ Decreto Supremo Nº 066-2003-PCM. Del 27 de junio del 2003. Fusionan la Jefatura de Informática de Instituto Nacional de Estadística e Informática INEI y la Presidencia del Consejo de Ministros, a través de su secretaria de Gestión Publica.
- ✓ Resolución Ministerial N° 206-2004-PCM, constituyen el padrón nacional de unidades informática de la administración pública y autorizan ejecución de registro de unidades informáticas del sistema nacional de informática.
- ✓ Ley Nº 29626, Ley de Presupuesto del sector Público para el año fiscal 2011.
- ✓ Ley Nº 27158 Ley de Modernización de la Gestión del Estado.
- ✓ Resolución de Contraloría General Nº 320-2006-CG. Contralor General (e) aprueba Normas de Control Interno del 3/11/2006.
- ✓ Resolución Jefatural Nº 088-2003-INEI. Del 03 de Abril del 2003, Aprueban Directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública".
- ✓ Ley N° 28493 del 12 de Abril del 2005. Ley que "Regula el uso del Correo Electrónico comercial no solicitado (SPAM)".
- ✓ Directiva General Nº 007-2007-GRL-GGR/OEDII "Normas para la Formulación, Trámite, Aprobación y Actualización de Directivas".

- ✓ Ordenanza Regional Nº 002-2010-GRL-CR; de fecha 08 de enero del 2010, que aprueba el Reglamento de Organización y Funciones del Gobierno Regional de Loreto.

4. **ALCANCE:**

La presente Directiva es de aplicación tanto para la Sede Central, como para los demás órganos dependientes del Gobierno Regional de Loreto.

5. **VIGENCIA:**

Las disposiciones contenidas en la presente Directiva regirán a partir del día de su publicación y permanecerán vigentes hasta la aprobación de normas legales que la modifiquen.

6. **APROBACION:**

La presente Directiva contará con la visación de la Gerencia General Regional, la Oficina Ejecutiva de Asesoría Jurídica, la Oficina Regional de Administración y la Oficina Ejecutiva de Desarrollo Institucional e Informática.

7. **NORMAS GENERALES:**

7.1 El acceso a Internet, es un medio importante de comunicación para el Gobierno Regional de Loreto y provee un medio eficiente para potenciar los trabajos diarios de sus trabajadores, jefes y personal administrativo, como también para muchos de los proyectos y emprendimientos que establezca la Institución. Por esto resulta de fundamental importancia lograr un uso equitativo y eficiente de estos recursos, que permita a todos cumplir con el objetivo antes especificado para lo cual se han elaborado estas normas de uso y seguridad.

7.2 El acceso a Internet se brinda a todo el personal y personas con la autorización expresa y adecuada.

8. **MECANICA OPERATIVA**

8.1. Respecto al uso de las computadoras.

8.1.1. Los usuarios de las computadoras de la contraloría se encuentran prohibidos de:

a. Pegar stickers en las computadoras.
b. Ingerir alimentos sobre las computadoras, así como colocar y/o manipular líquidos en su cercanía.
c. Rociar directamente sobre las computadoras líquidos para ambiente.
d. Fumar cerca de las computadoras.

e. Colocar y/o apilar documentos u otros objetos sobre las computadoras, y en ubicaciones que obstruyan o impidan su adecuada ventilación.
f. Ubicar el CPU en una posición distinta a su diseño original (horizontal o vertical).
g. Dejar los equipos portátiles (laptop) y sus accesorios, en lugares inseguros.
h. Conectar artefactos eléctricos sobre la línea eléctrica estabilizada de uso exclusivo para las computadoras, o sobre los estabilizadores de corriente.
i. Trasladar las computadoras a otra área, sin autorización escrita emitida por el jefe de la unidad orgánica del usuario y de la Oficina de Patrimonio.
j. Utilizar protectores de pantalla para los monitores de las computadoras con fotos de artistas, modelos, deportistas, dibujos animados, u otra imagen que pueda resultar poco seria u ofensiva.
k. Utilizar un fondo de escritorio distinto al fondo configurado por el personal de informática.
l. Instalar programas informáticos en las computadoras.
m. Modificar los parámetros o configuración de las computadoras de la institución así como el software y/o sistema informático.
n. Abrir las computadoras, así como, extraer o cambiar componentes.

8.1.2. Solo el personal autorizado de la oficina de desarrollo institucional e informática, y los operadores de las oficinas descentralizadas, direcciones regionales y subregionales, están facultados de realizar las acciones señaladas de los incisos i, m y n del numeral 8.1.1.

8.1.3. Disposiciones de seguridad:

a. Las contraseñas o claves de acceso asignadas a cada usuario son de carácter personal y confidencial, siendo responsable de su adecuado uso.
b. No usar contraseñas que sean fácilmente deducibles, las cuales deberán ser formadas con una combinación de números, letras y símbolos, y tener una longitud mínima de 8 caracteres.
c. Cuando los usuarios se retiren o suspendan sus labores, deberán dejar los equipos bloqueados o cerrar su sesión de trabajo, así mismo, después de concluidas sus labores diarias deberán apagar la computadora asignada.
d. Los usuarios deberán utilizar únicamente los servicios para los cuales están autorizados. No podrán utilizar la cuenta de otra persona, ni intentar apoderarse de claves de acceso de otros usuarios, como tampoco deberán intentar burlar los sistemas de seguridad bajo ningún motivo; el usuario afectado, o aquel que advierta una incorrecta utilización de las contraseñas o claves deberá informar a la Oficina de Desarrollo Institucional e Informática.
e. Los usuarios no deberán entrar a cuentas que no sean las propias haciendo uso de conexiones remotas, tampoco están autorizados a establecer comunicaciones entre una computadora de la institución y cualquier otro equipo informático ajeno a la institución sin la autorización de la Oficina de Desarrollo Institucional e Informática.

f. Queda prohibido encriptar carpetas y/o archivos, sin autorización de la unidad orgánica del usuario y apoyo técnico de la OEDII, a efectos de evitar la pérdida de información ante una falla en el sistema operativo. Dichos mecanismos de seguridad solo podrán ser utilizados por el usuario autorizado, y será responsabilidad exclusiva de éste la custodia diligente y confidencial de dichos mecanismos, así como cualquier daño y perjuicio que eventualmente pudiera derivarse de su falta de diligencia.

8.2. Respecto al uso de Internet

a. Utilizar software de navegación web designado por el Gobierno Regional de Loreto, el que deberá estar configurado con las directivas establecidas por los procedimientos de instalación de software de navegación web.
b. Acceder a Internet mediante los protocolos HTTP a través del servidor proxy designado para tal fin.
c. Los usuarios que requieran acceso a través de protocolo FTP deberán ser explícitamente autorizados a este tipo de acceso.
d. Cada usuario es responsable de las acciones efectuadas mediante el uso de internet, así como de las páginas que accede desde su computadora y/o cuenta de usuario asignada. Los usuarios no pueden usar el acceso a Internet para los siguientes propósitos salvo expresa autorización:

   - ✓ Acceso a sitios que puedan considerarse por su contenido sexista, racista, homofóbico, xenofóbico, pornográfico, pedófilo o similarmente discriminatorio y/u ofensivo.
   - ✓ Acceso para audio, video en línea (TV, Radio, música, etc.).
   - ✓ Acceso a sitios de juegos en red.
   - ✓ Bajada de software sin autorización.
   - ✓ Bajada de archivos de audio o video sin autorización.
   - ✓ Utilización para realizar ataques sobre otros sitios, usuario o servidores.
   - ✓ Brindar servicios externos desde el puesto de trabajo.
   - ✓ Acceso a sitios que reproduzcan en forma no autorizada material protegido.
   - ✓ Acceso a sitios que provean instrucciones o claves para utilizar o acceder a software, servicios o sitios en forma ilegal (piratería).
   - ✓ Efectuar llamadas telefónicas usando algún software para este propósito.
   - ✓ Utilizar programas de mensajería instantánea (bajo cualquier modalidad, esto es CHAT, Messenger, entre otros). Previa autorización de la Oficina de Desarrollo Institucional e Informática y de la Unidad Orgánica del usuario, se permitirá el acceso y uso de mensajería instantánea.

e. Los usuarios no podrán transferir o publicar información de propiedad del Gobierno Regional de Loreto.

f. Los usuarios no podrán, bajo ninguna circunstancia utilizar el acceso a Internet para monitorear, interceptar información de otros usuarios a menos que hayan sido autorizados para hacerlo.

g. Los usuarios de datos deben asumir que ninguna conexión a Internet es segura a menos que este encriptado, y no deberían enviar información que consideren confidencial a través de este medio.

h. El acceso a cualquier recurso disponible a través de Internet que no sea el de navegación de sitios deberá solicitarse en forma justificada para su debida aprobación de su jefe inmediato.

i. Se permite a los usuarios acceder a Internet para los siguientes usos:

- ✓ Acceso a sitios sobre noticias (diarios, agencias, etc.)
- ✓ Acceso a Portales del Gobierno.
- ✓ Acceso a Sistemas de Pago Electrónico de servicios
- ✓ Acceso a Sistemas de información sobre transportes, mapas, turismo, hoteles, etc.
- ✓ Acceso a sitios de capacitación, educación, tecnología, etc.
- ✓ Acceso a sitios de clientes, proveedores, competencia, etc.
- ✓ Acceso a servicios de telefonía IP.

8.3. Respecto a las Responsabilidades del Administrador de Red

a. Definir los accesos por niveles Usuarios Permitidos, No permitidos, Restringidos, Solo Dominios, etc. que será utilizado para el Gobierno Regional de Loreto.

b. Definir los procesos de instalación y configuración del software de navegación web.

c. Disponer del mecanismo de control necesario para que el acceso a Internet sea solo a través de los proxy habilitados para tal fin.

d. Los administradores de redes, en sus diferentes categorías, deberán asegurarse que la configuración de todos los navegadores de Internet sea la recomendada por el Centro de Comunicaciones para el acceso óptimo al servicio.

e. Responsabilidades del Centro de Comunicaciones:

- ✓ El personal de redes deberá contar con mecanismo de control de utilización del ancho de banda para la lograr un uso lo más equitativo posible.
- ✓ Podrá monitorear la actividad de los enlaces para legitimar los propósitos con los cuales se utilizan.

8.4. Respecto al uso del Correo Electrónico

8.4.1. De la cuenta de correo electrónico

a. El nombre de la cuenta de correo electrónico institucional para cada usuario estará formado por la letra inicial del nombre del usuario seguido inmediatamente del apellido paterno y la inicial del apellido materno, ligado con el símbolo @ al nombre de dominio de la institución, en caso

de existir dos construcciones similares, el administrador de correo electrónico en coordinación con las personas involucradas, acordarán el nombre de la cuenta.

b. El único correo electrónico permitido a usarse es el correo institucional, para lo cual; los gerentes, directores y jefes de oficinas deberán hacer llegar la relación del personal que necesita correo electrónico.

c. Solo los gerentes, directores y jefes de oficina tendrán acceso a correos personales (Hotmail, Yahoo, etc.) además de trabajadores que ellos designen de acuerdo a la actividad que realizan.

d. Todos los trabajadores tienen derecho a contar con un correo electrónico institucional, pero solo podrán recibir y enviar correos dentro de la institución o dentro del dominio (regionloreto.gob.pe)

e. Los tipos de cuentas de correo electrónico institucional que podrán ser asignados son de 2 tipos:

- ***Correo Tipo 1.-*** Correo electrónico desde el cual se puede enviar y/o recibir mensajes con archivos adjuntos dentro de la institución, y que puede recibir mensajes con archivos adjuntos desde correos externos, pero no permite el envío de mensajes hacia correos externos a la institución

- ***Correo Tipo 2.-*** Correo electrónico desde el cual se puede enviar y/o recibir mensajes con archivos adjuntos dentro como fuera de la institución.

8.4.2. Del buen uso del Correo Electrónico

a. Uso de las contraseñas

- Es responsabilidad del usuario mantener la confidencialidad de su clave de acceso a la cuenta de correo electrónico, proporcionada por la institución.
- Cuando el usuario deje de usar su computadora deberá cerrar el software de correo electrónico, para evitar que otra persona use su cuenta de correo.

b. Lectura del correo electrónico

- Los usuarios de las cuentas de correo electrónico institucional deberán leer frecuentemente sus mensajes, así como depurar permanentemente los mensajes innecesarios para mantener espacio disponible de su cuenta de correo.
- Se recomienda no abrir correos electrónicos sospechosos, especialmente los que tienen archivos adjuntos, aunque el remitente sea conocido, así mismo tener especial cuidado con los correos electrónicos recibidos en otros idiomas

c. Envío de correo electrónico

- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.
- Evitar usar acuse la opción "Acuse de recibo", "confirmación de lectura o de entrega" ya que esto provoca demasiado tráfico en la red, a menos que sea un mensaje muy importante donde requiera el remitente saber que el destinatario tomó conocimiento del mensaje (y a su vez disponga de un cargo de entrega), y pueda buscar otras vías de comunicación en caso el mensaje no fuera leído en un tiempo razonable.
- Evitar enviar mensajes a listas globales.
- Escribir el nombre de la persona a la que va dirigido el mensaje, también debe incluirse el nombre del remitente del mensaje.
- Los usuarios que se ausenten de la institución (vacaciones u otro motivo) deberán habilitar la opción de respuesta automática de "fuera de oficina", que consigne además fecha de retorno y funcionario alterno de contacto, para que el remitente pueda oportunamente derivar su comunicación a otras instancias hasta su retorno.
- El contenido y documentación y/o información remitida por el correo electrónico institucional es de responsabilidad del usuario que la originó dicho envío.
- Los correos electrónicos dirigidos a personas y/o instituciones que no pertenezcan al Gobierno Regional de Loreto tendrán el siguiente párrafo como pie de página: "Este mensaje electrónico y sus documentos adjuntos, solo son para conocimiento y uso de la persona(s) y/o institución a quien va dirigido. Si usted no es el destinatario(s), agradecemos se abstenga de copiarlos, divulgarlos o usarlos, y borre de su equipo este mensaje y los documentos adjuntos en caso obtenga alguno. La lectura de este mensaje presupone que usted comprende y acepta los términos de este aviso".

d. Tamaño de los mensajes

- La oficina de Desarrollo institucional e Informática determinará la cuota del correo electrónico de los usuarios, sujetándose los mismos al tamaño de dicha cuota, y siendo estos responsables de depurar sus [illegible] para garantizar el adecuado funcionamiento de su [illegible]
- [illegible] cuando estos excedan la capacidad de la cuota del usuario en el servidor.

e. Vigencia de los mensajes.

- La vigencia de los mensajes será por dos meses. Para mantener los mensaje de forma permanente, éste debe almacenarse (archivarse) en carpetas personales de su computador.

8.4.3. Del mal uso del correo electrónico.

a. Se considera falta grave facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas, conforme lo señalado en la Directiva N° 005-2003-INE/DTNP del instituto Nacional de Estadística e Informática.

b. Se considera como mal uso del correo electrónico institucional las siguientes actividades:
   - Utilizar el correo electrónico institucional con fines ajenos a la institución.
   - Participar en la programación de mensajes encadenados o similares.
   - Distribuir mensajes con contenidos impropios y/o lesivos a la moral; o que afecten la imagen de terceros o de la institución u otras Entidades Públicas.
   - Falsificar las cuentas de correo electrónico.
   - El envío de mensajes a grupos de discusión (listas de distribución, listas de correo y/o "newsgroup") que comprometan la información de la institución o violen las leyes del Estado Peruano.
   - La inscripción a listas de correos, las cuales no estén relacionadas directamente con su trabajo, algunas listas de correo generan cantidades masivas de correos a los suscriptores por lo que se satura el correo institucional.

c. Queda prohibido acceder y utilizar una cuenta de correo electrónico institucional diferente a la asignada.

d. Queda prohibido el uso de otro correo electrónico distinto al de la institución, sin la autorización de la unidad orgánica del usuario y de la Oficina Ejecutiva de Desarrollo Institucional e Informática.

9. RESPONSABILIDADES

a. **El Titular de Pliego** es responsable de cumplir y hacer cumplir la escala de prioridades por los criterios optimización del Ancho de Banda, seguridad y adecuada administración de la información, conforme se establece en la presente directiva.

   Dar el visto bueno al informe de cumplimiento por el monitoreo, evaluación y seguimiento de las medidas adoptadas por los responsables de la Oficina de Informática.

b. **De los jefes de las Oficinas de Administración**, o los que hagan sus veces en los demás órganos dependientes; conforme a lo establecido en el punto 8 de la presente Directiva y a los gerentes, subgerentes, jefes así como los funcionarios responsables de la conducción del personal para que, en el ámbito de sus competencias, estimulen comuniquen y autoricen el cumplimiento de cada uno de los puntos expresados en el presente documento normativo.

c. **De los responsables de la emisión de Informe de monitoreo y evaluación:** la Gerencia General Regional en mérito a su competencia funcional tomará en cuenta las recomendaciones emitidas y dispondrá las acciones correctivas que estime conveniente en coordinación con la Oficina especializada. El mismo que será concordado con los informes de vulnerabilidad que se emite a nivel del Gobierno Nacional. Por lo que es de su competencia aplicar los criterios de racionalidad y de los principios de oportunidad y demás, estipulados en la Ley del Procedimiento Administrativo General y en los parámetros y criterios contemplados en la presente directiva.

d. **De los usuarios que acceden a Internet:** Los que en mérito a la presente norma darán cumplimiento indefectible a los principios, criterios y parámetros de configuración técnica que proponga la Oficina Ejecutiva de Desarrollo Institucional e Informática, siendo pasibles de sanción por su incumplimiento sin perjuicio de otras acciones de carácter administrativo o penal a que diere lugar por su incumplimiento ocasionando daño a los activos de la Institución.