

## **POLITICAS Y LINEAMIENTOS**

### **Índice**

	<b>Página</b>
<b>Introducción</b>	<b>2</b>
<b>Definiciones</b>	<b>3</b>
<b>Red interna de datos</b>	<b>4</b>
<b>Correo electrónico</b>	<b>5</b>
<b>Acceso a Internet</b>	<b>5</b>
<b>Monitoreo</b>	<b>7</b>
<b>Servicios a equipo de cómputo</b>	<b>7</b>
<b>Uso de equipo de cómputo y medios de impresión</b>	<b>8</b>
<b>Confidencialidad de la información</b>	<b>8</b>
<b>Observaciones generales</b>	<b>9</b>
<b>Cumplimiento y atención del presente reglamento</b>	<b>9</b>
<b>Derecho de los usuarios</b>	<b>10</b>
<b>Anexo 1</b>	<b>11</b>

## **Introducción**

La Administración Portuaria Integral Puerto Vallarta, S.A. de C.V. (API) proporciona servicios de tecnologías de la información con la finalidad de contribuir al buen desarrollo de las actividades y funciones de su personal, así como de las actividades administrativas sobre las que se apoyan las áreas, facilitando el intercambio y transformación de información. API da acceso a los servicios de cómputo a los miembros del personal administrativo y operativo que así lo requieran, para la realización de sus actividades administrativas, y provee a los usuarios con una red interna de datos, con acceso a Internet, así como con un servicio de correo electrónico. La instalación y el mantenimiento de estos servicios requieren de una cantidad significativa de recursos, y por lo tanto se espera que los usuarios mantengan una conducta responsable cuando los utilicen. El presente documento establece las políticas de uso aceptable de los servicios de TI (Tecnologías de la Información), a las cuales deben ajustarse los usuarios.

La utilización de estos servicios de cómputo conlleva la responsabilidad de aceptar las políticas de uso adecuado que se establecen en el presente documento.

## **Definiciones**

<b>CPU</b>	Unidad Central de Proceso (todos los componentes que integran el gabinete de la computadora)
<b>Hardware:</b>	Elementos físicos que conforman un equipo de cómputo. (cpu, monitor, teclado, mouse, impresoras y accesorios)
<b>Red:</b>	Conjunto de elementos, computadoras, impresoras y medios informáticos conectados entre si.
<b>Software:</b>	Conjunto de programas y herramientas informáticas para la operación de la computadora.
<b>TI</b>	Tecnologías de la Información.
<b>mp3, wav, wma,</b>	Formato de audio digital
<b>avi, mpg, wmv, mov</b>	Formato de archivos multimedia que contienen tanto imágenes como sonido
<b>Web</b>	abreviatura para World Wide Web: Red Mundial
<b>Chats</b>	Sistema para comunicarse (mediante texto) en tiempo real con personas que se encuentran en otros ordenadores conectados a la red.
<b>Internet</b>	Red mundial de dordenadores interconectados que utilizan un modo de intercambio de información llamado TCP/IP (Transmission Control Protocol)
<b>Firewall</b>	Mecanismo de seguridad en Internet frente a accesos no autorizados. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados.
<b>Firewall</b>	Mecanismo de seguridad en Internet frente a accesos no autorizados. Básicamente consiste en un filtro que mira la identidad de los paquetes y rechaza todos aquellos que no estén autorizados o correctamente identificados.
<b>IP</b>	(Protocolo de Internet). Es el número que identifica a cada dispositivo dentro de una red.

## **1 Red interna de datos**

- 1.1 Para acceder a la red interna es necesario obtener una clave de usuario y una contraseña. Esta clave debe ser conocida solamente por el usuario y es intransferible. En caso de cualquier olvido la única persona autorizada para proporcionar una nueva clave y/o contraseña es el administrador de la red. Si el usuario sospecha que algún otro usuario está haciendo uso de su clave debe reportarlo al administrador de la red. En ocasiones una clave de usuario y su respectiva contraseña pueden ser compartidas por varios usuarios pertenecientes a un mismo grupo de trabajo. Es responsabilidad de los miembros de ese grupo no proporcionar su clave y contraseña compartida a ningún otro usuario.
- 1.2 Ningún usuario deberá permitir el acceso a la red interna de la empresa a personas externas al mismo o a personal no autorizado, mediante el uso de la cuenta que le ha sido asignada.
- 1.3 Los servicios de impresión en red deben ser utilizados únicamente para imprimir documentos relacionados con las labores administrativas del usuario.
- 1.4 Los usuarios podrán hacer uso de sus unidades de red para respaldar información de sus equipos, pero siempre dentro de sus cuotas de espacio en la red. Sin embargo, las unidades compartidas no podrán ser usadas para este propósito. Si los usuarios requieren de algún respaldo en particular del contenido en su computadora, deberá solicitarlo al área de sistemas.
- 1.5 Las unidades de red no se deberán utilizar para guardar archivos de música (mp3, wav, wma, etc.), o videos de uso personal (avi, mpg, wmv, mov, etc). Queda estrictamente prohibido tener imágenes o videos pornográficos, o software ilegal.
- 1.6 La información almacenada en las unidades de red se organizará en carpetas. Cada usuario tendrá una carpeta para su uso exclusivo, y cada grupo tendrá una carpeta para el uso compartido del grupo. Habrá un sistema de cuotas de espacio en estas unidades, y las cuotas serán fijadas por el departamento de informática, de acuerdo al espacio total de almacenamiento disponible en la red de datos.
- 1.7 Habrán también unidades de red para los diversos servicios y unidades administrativas de la empresa (Calidad, Nominas, SAP, Etc.), y estas también estarán sujetas al sistema de cuotas.
- 1.8 Habrá una unidad compartida, que será designada como la unidad “de Red”, a la que tendrán acceso todos los usuarios. Esta unidad tiene como propósito facilitar el intercambio de archivos e información entre los mismos usuarios de la red.

## **2 Correo electrónico**

- 2.1 Todos los usuarios Administrativos tendrán una cuenta de correo electrónico, que deberán solicitar al administrador del sistema, con el aval de su gerente de área. Los Trabajadores operativos también podrán tener una cuenta, con el aval de su jefe inmediato si así se requiere.
- 2.2 La cuenta de correo electrónico es personal e intransferible, por lo que la clave y contraseña para acceder al mismo deberán ser conocidas solamente por el usuario y no deberán ser compartidas con nadie, por lo que si se detecta que el servicio es utilizado por otra persona que no sea el titular se podrá cancelar el servicio.
- 2.3 El servicio de correo electrónico no deberá ser utilizado para enviar mensajes en forma masiva cuyo contenido sea ajeno a actividades relacionadas con la empresa, ni para enviar mensajes ofensivos o de hostigamiento a otras personas. Se prohíbe utilizar la cuenta de correo para enviar o reenviar mensajes que pertenezcan a “cadenas”. Queda estrictamente prohibido el uso de las cuentas para fines comerciales ajenos a las actividades de la empresa.
- 2.4 El usuario no debe utilizar la cuenta de correo para enviar o recibir archivos ejecutables que comprometan la seguridad del sistema. En caso de que sea necesario enviar o recibir datos adjuntos a un mensaje de correo electrónico el usuario tiene la responsabilidad de analizarlos para detectar la posible presencia de virus informáticos, y cualquier posible infección debe ser reportada de inmediato al administrador.

## **3 Acceso a Internet**

- 3.1 El acceso a Internet debe ser utilizado fundamentalmente para visitar sitios relacionados con actividades de la empresa.
- 3.2 El acceso a Internet contará con restricciones para sitios inseguros, y será particularmente importante que los usuarios tengan un comportamiento responsable en aquellos sitios que no queden restringidos, ya que un uso inadecuado puede comprometer seriamente la seguridad de los servicios de cómputo, así como afectar el trabajo de otros usuarios de la empresa.
- 3.3 Queda prohibido el uso de programas para “bajar” o copiar de Internet archivos de procedencia no segura o ilegal, Por estos motivos también queda prohibido instalar y ejecutar programas que permitan el intercambio de archivos (**anexo 1**). Queda también prohibido utilizar los recursos de cómputo para actividades que no estén vinculadas con su trabajo, como pláticas en línea o “chats”.

- 3.4 Se sugiere que se minimice o se evite la práctica de bajar e instalar programas gratuitos del Internet, tales como salvapantallas, pues estos frecuentemente instalan programas indeseables como espías, lo cual minimiza el rendimiento de los equipos.
- 3.5 Queda prohibida la instalación de servidores Web o páginas Web en las computadoras de la empresa, a excepción de aquellas que pertenecen al portal del API. Queda prohibido además utilizar los servicios de cómputo de la misma para realizar actividades comerciales.
- 3.6 Todas las conexiones al Internet tendrán que estar dentro del Firewall para seguridad del sistema de red, a excepción de aquellas expresamente autorizados por el área de sistemas. Toda máquina con IP fuera del Firewall a la que se detecte algún incidente de seguridad podrá ser desconectada físicamente de la red en tanto se corrija el problema, y deberá ser nuevamente autorizada por el área de sistemas para poder operar fuera del Firewall.
- 3.7 El Administrador de la red deberá configurar y certificar los equipos para que se puedan conectar a la red. Todo equipo que se vaya a conectar deberá contar con antivirus vigente y con las actualizaciones al sistema operativo que permitan asegurar que no existan vulnerabilidades que pongan en entredicho la integridad y seguridad de la red del Instituto.
- 3.8 Queda estrictamente prohibido cambiar la IP asignada o usar un IP que no haya sido asignado por el área de sistemas. También está prohibido configurar equipos y conectarlos a la red sin que hayan sido revisados y certificados por la misma. En caso de existir la necesidad de instalar puntos de acceso inalámbrico a la red, se deberá remitir una solicitud al Administrador de la red, para lleve a cabo las acciones necesarias para garantizar la seguridad de la red.
- 3.9 Las máquinas que estén dispersando virus deberán ser desconectadas de la red hasta que se resuelva el problema y los virus sean eliminados. Los usuarios que detecten virus en sus equipos deberán dar aviso al área de sistemas, que deberá darle máxima prioridad a la solución de este tipo de problemas.
- 3.10 El departamento de informática no se hace responsable de problemas de comunicación con servidores externos por problemas ajenos a la Red de la API.
- 3.11 Es responsabilidad del área de sistemas mantener actualizado tanto el sistema operativo con los parches de seguridad como el antivirus con las actualizaciones disponibles para este fin.
- 3.12 Cualquier excepción a los puntos anteriores puede ser válida siempre y cuando el usuario proporcione una clara justificación, excepto los puntos

de prohibición estricta que no deberán ser transgredidos por ningún motivo.

#### **4 Monitoreo**

- 4.1 El área de sistemas se reserva el derecho de monitorear el uso de los servicios con el fin de detectar el posible mal uso de los mismos. Durante el monitoreo se tomarán todas las medidas necesarias para garantizar la privacidad del usuario.
- 4.2 En caso de sospechas de abuso por parte de algún usuario se le pedirá una explicación sobre la actividad detectada, lo cual se hará en estricta confidencialidad.
- 4.3 En caso de abusos reiterados por parte de algún usuario se podrá negar al mismo el uso de los servicios de cómputo de la empresa, por acuerdo de la alta gerencia y se hará del conocimiento a la dirección general.

#### **5 Servicios a equipo de computo**

- 5.1 Toda solicitud de servicios de cómputo deberá hacerse a través del correo electrónico "jdinformatica@puertodevallarta.com.mx". Las cuestiones muy urgentes podrán ser atendidas mediante una llamada telefónica o una visita del interesado al área de sistemas, pero en esos casos se deberá enviar la solicitud de servicio a la brevedad posible al correo electrónico arriba mencionado, y se exhorta a los usuarios de los servicios de cómputo a no usar este mecanismo mas que en casos verdaderamente excepcionales y a respetar la programación de los servicios de cómputo.
- 5.2 El departamento de Informática podrá canalizar órdenes de servicio a proveedores externos siempre que lo considere conveniente, pero en todos los casos deberá revisar primero el equipo de cómputo para evaluar la necesidad de enviarlo a un taller externo.
- 5.4 Cada usuario se hará responsable de los programas que se instalen en los equipos de cómputo que les son proporcionados. El personal de informática solamente instalará programas de procedencia legal que cuenten con la licencia respectiva. Cualquier otro programa instalado en el equipo que no cuente con dicho licenciamiento, el responsable deberá sujetarse de acuerdo con los términos y obligaciones de la Ley Federal de Derechos de Autor.
- 5.5 El área de sistemas se reserva el derecho de desconectar equipos de la red y no realizar órdenes de servicio por mal uso de la computadora: equipo con programas inseguros de música o video, entrada repetitiva de

virus a través de correo no filtrado, equipos operando sin antivirus actualizados o con sistemas operativos sin los parches de actualización.

## **6 Uso de equipo de cómputo y medios de impresión.**

- 6.1 El equipo de cómputo deberá utilizarse como herramienta de trabajo a través de las distintas áreas destinadas para este propósito.
- 6.2 El uso del equipo de cómputo es exclusivo para los empleados de la API. Cualquier persona que no esté considerada como tal y que desee hacer uso del equipo de cómputo deberá notificar al área de sistemas para proporcionarle la inducción debida.
- 6.3 Todo usuario deberá dar uso adecuado al equipo de cómputo. En el caso de que algún equipo resulte dañado físicamente por alguna acción atribuible al usuario, éste será acreedor a una sanción y deberá cubrir el costo del daño ocasionado si la empresa así lo considera.
- 6.4 Los equipos (CPU, Monitores, impresoras) no deberán ser movidos de un lugar a otro o de un área a otra sin previa notificación al área de sistemas.
- 6.5 No utilizar los equipos computacionales como máquinas de juegos; esto incluye utilizar software de juegos o acceder a servicios que impliquen el uso de juegos interactivos.
- 6.6 Equipo de cómputo no deberá ser utilizado para desarrollar programas o proyectos ajenos al interés de la empresa.
- 6.7 No alterar o dañar las etiquetas de identificación de cualquier equipo de cómputo.
- 6.8 No Alterar software instalado en el equipo de cómputo.
- 6.9 No usar Memorias USB sin previa revisión por parte del área de sistemas.

## **7 Confidencialidad de la información**

- 7.1 Toda información almacenada en los servidores no hecha explícitamente pública, será tratada como confidencial, y se harán todas las adecuaciones posibles por garantizar la privacidad de ésta.
- 7.2 La API se reserva el derecho de consultar la información almacenada en equipos propiedad de la API cuando así lo juzgue conveniente.

- 7.3 El departamento de sistemas sólo podrá requerir el acceso a la información de un usuario cuando se presuma alguna falta que a juicio de la alta dirección de la API, amerite lo anterior.
- 7.4 Todo usuario del cual se requiera consultar su información tendrá el derecho de estar presente en el momento de la consulta de la misma, que sólo podrá ser llevada a cabo por personal del departamento de Informática.

## **8 Observaciones Generales**

- 8.1 El área de informática se reserva el derecho de utilizar los medios a su alcance para investigar posibles violaciones a este reglamento, siempre respetando la confidencialidad de la información.
- 8.2 El área de informática. Se reserva el derecho de suspender o eliminar el acceso en cualquier equipo de cómputo a cualquier usuario, sin previo aviso al mismo, si el hacerlo es necesario para mantener la disponibilidad, seguridad e integridad de las operaciones de los recursos de la API.

## **9 Cumplimiento y atención del presente reglamento**

- 9.1 Dada la naturaleza del presente reglamento, su conocimiento y cumplimiento son obligatorios para todos los usuarios del equipo de cómputo. Su desconocimiento nunca podrá ser invocado como excusa.
- 9.2 El presente reglamento entrará en vigor a partir de la fecha de su publicación y se revisará al inicio de cada año para su adecuación si fuese el caso por el responsable del departamento de informática.

## **10 Derecho de los usuarios**

Todos los usuarios tiene derecho a:

- A recibir asesoría cuando la requiera
- A contar con equipo de cómputo que funcione adecuadamente
- Recibir la inducción necesaria para la buena operación del o los equipos
- Contar con los programas necesarios para facilitar sus actividades administrativas
- Contar con una cuenta de correo
- Que se les notifique si se realizan cambios en los accesos a la red.

Todas las sugerencias o inconformidades con respecto a las instalaciones o el comportamiento del personal del área de sistemas, deberán ser enviadas al responsable del área de sistemas.

Elaboró

---

P.T. Eduardo Ortega Navarro  
Jefe del departamento de Sistemas e Informática

Autorizó

---

Ing. Francisco Martínez Narváez  
Director General

Revisó

---

C.P. José Ramón Flores García  
Titular del Órgano Interno de Control

**Última actualización: 04 de Agosto de 2009**

## Anexo 1.

### Lista de Programas prohibidos para Intercambio de audio y video

3ECS	Gnucleus	OpenCola
Adult Media Swapper	Groskter	OpenNap
AppleJuice	iMesh	Overnet PeerGenius
Ares	Inoize	Phex
Atomwire	intelliMP3	Phosphor
AudioGalaxy	Jungle Monkey	Piolet
AudioGalaxy Satellite	Kast	Plebio
AudioGnome	Kazaa Lite	PornDigger
BadBlue	Kazaa Kontrol Leech Killer	Private Peer to Peer
Bearshare	Kazaa Lite Advanced	QtraxMax
BlackWindow	Kaza Lite Cracked	QueerPeer
Blipster Fast Find	Kazaa Cracked K++	Rapigator
BlubsterBoDeTella	Kaza Media Desktop	Razius Express
BuddyShare	Kazearch	Renapster
CatNap	Kceasy	RiffShare
Dagsta	Limewire	RighteousMP3
DC++	Limewire Sparky	Shareaza
DC:Pro	Locutus	ShareSniffer
DietKazaa	IPhant	SideKick
DirectConnectDBNapster	Madster	SlavaNap
Dopefish Satellite	MediaSeek	Smirck
Earth Station	Mercora	SongSpy XE
eDonkey Client	Mnet	SoulSeek
eDonkey Server Spy	Mojonation	SpookShare
eDonkeyboot Lite	Morpheus	Swapnut
eDonkey	MP3Mystic	Swaptor
ELF	MXlinx	Taxee
eMule pHoeniX	MyNapster	The Circle
eMule Plus	Myster R8	The PornTrader
eMule	NapAmp	The Qube
Evolution	Napigator	ToadNode
Exware	NapiMX	TrustyFiles
ExoSee	Napshack	URLBlaze
FANTastic PLayer	Napster	Varvar
File Freedom	Natural Born Chatter	VexTV
Filemaze	Neo Modus Direct Connect	Wanafile
Fillnavigator	Neo Napster	Wannafree
Fillerouge	Netbrilliant	WinMX
FileShare Client	NetMess	Wippit
FileSpree	Newtella	WWW Filre Share Pro
Filetopia	NTella	Xolox
Freewire	Nudester	Yaga Share
FTP++P2P	Nuzzly	Yoink