MARINA

SECRETARÍA DE MARINA

Lineamientos y Políticas de Seguridad para el uso de Equipo de Cómputo y Servicios de Tecnologías de la Información

Índice

Introducción

La Administración del Sistema Portuario Nacional Puerto Vallarta (ASIPONA PV) 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. ASIPONA PV da acceso a los servicios de cómputo a los trabajadores de la misma que así lo requieran, para la realización de sus actividades administrativas/operativas, y provee a las usuarias/os 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 las usuarias/os 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).

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

CPU	Unidad Central de Proceso (los componentes que integran el gabinete de la computadora)
Hardware:	Elementos físicos que conforman un equipo de cómputo. (cpu, monitor, teclado, mouse, impresoras y accesorios)
Red:	Conjunto de elementos, computadoras, impresoras y medios informáticos conectados entre sí.
Software:	Conjunto de programas y herramientas informáticas para la operación de la computadora.
TIC	Tecnologías de la Información y Comunicación.
mp3, wav, wma,	Formato de audio digital
avi, mpg, wmv, mov	Formato de archivos multimedia que contienen tanto imágenes como sonido
Web	abreviatura para World Wide Web: (Red Mundial)
Chats	Sistema para comunicarse (mediante texto) en tiempo real con personas que se encuentran en otros ordenadores conectados a la red.
Internet	Red mundial de ordenadores interconectados que utilizan un modo de intercambio de información llamado TCP/IP (Transmission Control Protocol)
Firewall	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.
IP	(Protocolo de Internet). Es el número que identifica a cada dispositivo dentro de una red.

1 Red interna de datos y Sistemas

1.1 Para acceder a la red interna y a los Sistemas que la Entidad opera, es necesario obtener una clave de usuario/a y una contraseña, misma que será proporcionada por el departamento de informática a solicitud de la Gerencia, Subgerencia o Jefatura del área según corresponda. Esta clave debe ser conocida solamente por la usuaria/o a quien le fue asignada y es intransferible. En caso de olvido la única persona autorizada para proporcionar una nueva clave y/o contraseña es el administrador/a de la red. Si el usuario/a sospecha que alguien está haciendo uso de su clave debe reportarlo al administrador/a de la red. En ocasiones una clave de usuario/a puede ser compartida por una o más personas, pertenecientes a un mismo grupo de trabajo. Es responsabilidad de las miembras/os de ese grupo no proporcionar su clave y contraseña compartida a ningún otro usuario/a.

1.2 Ningún usuario/a deberá permitir el acceso a los sistemas o 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 usuarios/as podrán hacer uso de sus unidades de red para respaldar información. Sin embargo, las unidades compartidas no podrán ser usadas para este propósito. Si requieren de algún respaldo en particular del contenido en su computadora, deberá solicitarlo al área de sistemas. Toda la información en Red será respaldada diariamente, la información en las pc's será responsabilidad de cada usuario.

1.4 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.

1.5 La información almacenada en las unidades de red se organizará en carpetas. Cada usuario/a 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.

1.6 Habrán también unidades de red para los diversos servicios y unidades administrativas de la empresa (Calidad, Nominas, SAP, SOP, Facturación, Etc.), y estas también estarán sujetas al sistema de cuotas.

1.7 Habrá una unidad compartida, que será designada como la unidad "de Red SALA DE JUNTAS", a la que tendrán acceso los usuarios/as. Esta unidad tiene como propósito facilitar el intercambio de archivos e información entre los mismos/as integrantes de la red. Pero esta solo será de intercambio, no se resguardará el contenido de la misma, por lo que cada usuario deberá ser responsable de la misma y eliminar cuando ya no se comparta (es de uso solo para compartir en reuniones en sala de juntas).

1.8 Toda la información generada en los equipos de cómputo, es responsabilidad de cada usuario, su uso y distribución es responsabilidad del mismo. Ya que para el resguardo de la información se les asignará una carpeta de red, es decir, la información que graben directamente en la computadora NO SE RESPALDA, para eso tienen asignada su unidad de Red.

2 Correo electrónico

2.1 Todas/os los usuarios/as tendrán una cuenta de correo electrónico, que deberán solicitar al área de informática, con el aval de su Gerencia, Subgerencia o Jefatura del área según corresponda.

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 la usuaria/o 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 La usuaria/o 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 la usuaria/o tiene la responsabilidad de analizarlos para detectar la posible presencia de virus informáticos, y cualquier posible infección debe ser reportada de inmediato al área de informática.

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 las usuarias/os 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/as de la Entidad.

3.3 Queda prohibido el uso de programas para "descargar (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", Redes sociales, ver videos, películas, futbol, etc., salvo aquellos casos que por sus actividades en la empresa lo requiere y será solo con la autorización de la Gerencia o Jefatura correspondiente.

3.4 Queda estrictamente prohibida la práctica de bajar e instalar programas gratuitos del Internet, tales como salvapantallas, o cualquier otro, sin previa autorización, pues estos frecuentemente instalan programas ocultos como espías, spam, o virus los cuales minimiza el rendimiento de los equipos o peor aún, ponen en riesgo la información de la Entidad.

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 la ASIPONA PV. Queda prohibido además utilizar los servicios de cómputo de la misma para realizar actividades comerciales.

3.6 Todos los equipos de cómputo tendrán que estar dentro del Firewall para seguridad del sistema de red, a excepción de aquellos 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 Todo equipo Externo que se vaya a conectar a la red 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 de la Entidad y deberá ser autorizada por el área de TICs.

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 área de sistema, para lleve a cabo las acciones necesarias para garantizar la seguridad de la red.

3.9 Si se detecta de algún equipo que esté dispersando virus, este será desconectado de la red hasta que se resuelva el problema y los virus sean eliminados. Las usuarias/os que detecten virus en sus equipos deberán dar aviso al área de sistemas inmediatamente.

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 de los usuarios/as.

4.2 En caso de sospechas de abuso por parte de alguna usuaria/o 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 alguna usuaria/o 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 TI deberá hacerse a través del correo electrónico “sginformatica@puertodevallarta.com.mx y/o al correo de cinformatica@puertodevallarta.com.mx: Las cuestiones muy urgentes podrán ser atendidas mediante una llamada telefónica o una visita de la interesada/o 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 las usuarias/os de los servicios de cómputo a no usar este mecanismo más que en casos verdaderamente excepcionales y a respetar el procedimiento normal.

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 usuaria/o 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 Autora/or.

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 el personal de la ASIPONA PV. 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 Todos los usuarios/as deberán dar uso adecuado al equipo de cómputo. En el caso de que algún equipo resulte dañado físicamente por alguna acción atribuible al usuaria/o, éste/a 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.

6.10 Los servicios de impresión en red deben ser utilizados únicamente para imprimir documentos relacionados con las labores administrativas/operativas de la Entidad.

6.11 Cuando se tenga personal de prácticas o servicio social en la Entidad, las áreas requirentes deberán de enviarlos al área de sistemas para la inducción correspondiente.

7 Confidencialidad de la información

7.1 Toda información almacenada en los servidores, será tratada como confidencial, y se harán todas las adecuaciones necesarias para garantizar la privacidad de la misma.

7.2 La ASIPONA PV se reserva el derecho de consultar la información almacenada en equipos propiedad de la Entidad cuando así lo juzgue conveniente.

7.3 Toda usuaria/o 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 estos lineamientos, 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 usuarias/os 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 ASIPONA PV.

9 Cumplimiento y atención de los presentes lineamientos

9.1 Dada la naturaleza de los presentes lineamientos, su conocimiento y cumplimiento son obligatorios para todas/as las usuarias/os del equipo de

cómputo de la red de la ASIPONA PV. Su desconocimiento nunca podrá ser invocado como excusa.

9.2 Los presentes lineamientos entrarán 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 las usuarias/os

Todas/os las usuarias/os tiene derecho a:

- A recibir asesoría cuando la requiera
- Recibir la inducción necesaria para la buena operación del o los equipos
- Contar con una cuenta de correo
- Que se les notifique si se realizan cambios en los accesos a la red.

Elaboró

P.T.I. Eduardo Ortega Navarro
Subgerencia de Tecnologías de la Información

Autorizó

Alm. Ret. Víctor Francisco Uribe Arévalo
Director General

Puerto Vallarta, Jalisco a 30 de octubre de 2023

Anexo 1.

Lista de Programas restringidos (Transmisión 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 Satelite	Kast	Plebio
AudioGnome	Kazaa Lite	PornDigger
BadBlue	Kazaa Kontrol Leech	Private Peer to Peer
Bearshare	Killer	QtraxMax
BlackWindow	Kazaa Lite Advanced	QueerPeer
Blipster Fast Find	Kaza Lite Cracked	Rapigator
BlubsterBoDeTella	Kazaa Cracked K++	Razius Express
BuddyShare	Kaza Media Desktop	Renapster
CatNap	Kazearch	RiffShare
Dagsta	Kceasy	RighteousMP3
DC++	Limewire	Shareaza
DC:Pro	Limewire Sparky	ShareSniffer
DietKazaa	Locutus	SideKick
DirectConnectDBNapster	IPhant	SlavaNap
Dopeflish Satellite	Madster	Smirck
Earth Station	MediaSeek	SongSpy XE
eDonkey Client	Mercora	SoulSeek
eDonkey Server Spy	Mnet	SpookShare
eDonkeyboot Lite	Mojonation	Swapnut
eDonkey	Morpheus	Swaptor
ELF	MP3Mystic	Taxee
eMule pHoeniX	MXlinx	The Circle
eMule Plus	MyNapster	The PornTrader
eMule	Myster R8	The Qube
Evolution	NapAmp	ToadNode
Exware	Napigator	TrustyFiles
ExoSee	NapiMX	URLBlaze
FANtastic PLayer	Napshack	Varvar
File Freedom	Napster	VexTV
Filemaze	Natural Born Chatter	Wanafile
FIlenavigator	Neo Modus Direct	Wannafree
FIlerouge	Connect	WinMX
FIleShare Client	Neo Napster	Wippit
FIleSpree	Netbrilliant	WWW Filre Share Pro
Filetopia	NetMess	Xolox
Freewire	Newtella	Yaga Share
FTP++P2P	NTella	Yoink
	Nudester	youtube
	Nuzzly	

* Esta lista es enunciativa más no limitativa.