2017

POLÍTICAS INSTITUCIONALES EN MATERIA DE INFORMÁTICA

INFORMATICA -AMP

AUTORIDAD MARÍTIMA PORTUARIA

DIRECCIÓN EJECUTIVA DE LA AUTORIDAD MARÍTIMA PORTUARIA: San Salvador, a los ocho días del mes de agosto de dos mil diecisiete.

CONSIDERANDO:

1. Que debido a la utilización de tecnología informática para el desarrollo de las actividades de la AMP, se debe proteger la información y el equipo tecnológico existente, procurando una administración oportuna y eficiente.
2. Que en función de los riesgos existentes en cuanto a pérdida de información por agentes infecciosos, es necesario tomar medidas que garanticen la protección de los recursos tecnológicos y evitar extracción de información por personas o entidades ajenas a la Institución.
3. Que en función de evitar el uso indebido de los equipos y herramientas informáticas, es necesario implementar controles y restricciones que garanticen el debido uso y cuido de la tecnología existente en la institución.
4. Que en función de cumplir con las Normas Técnicas de Control Interno que rigen a esta institución, en lo referente a poseer un Manual de Políticas en materia de Informática, que sea aplicable a todas las oficinas y puestos de trabajo de la AMP.

POR TANTO:

El Director Ejecutivo de la AMP **autoriza** y hace del conocimiento de todo el personal de las distintas dependencias de esta institución, las Políticas Institucionales para el uso de los Recursos Informáticos.

Objetivos

Aplicar normativa restrictiva sobre el uso de los Recursos Informáticos mediante controles en Administración, Procedimientos y Requerimientos, para asegurar la protección adecuada a la información contenida en los Equipos Informáticos instalados en la Institución.

Alcance

Las políticas están orientadas a todos los empleados de la Institución, ubicados en las diferentes áreas que utilicen o tengan acceso a equipos informáticos de cualquier tipo o clase, conectados a la red local a través de cualquier medio.

Políticas

Las políticas están orientadas a las áreas de acción que se detallan a continuación: Políticas de Administración, Políticas sobre el uso de Internet, Políticas sobre el uso de Correo Electrónico, Políticas sobre Desarrollo de Aplicaciones Mecanizadas, Políticas de Prevención, Manejo y Contención de Epidemias y Políticas de Contingencia.

1 Políticas de Administración

La administración de recursos informáticos de la red de la AMP es responsabilidad de la Unidad de Informática Institucional. Las funciones de administración incluyen: la administración de los Servidores de Internet, Correo Electrónico, Bases de Datos propias de la AMP, supervisión del tráfico de la red, la seguridad de accesos a la red y servicios, como Dominios, Active Directory, Servidores WINS, servidores DHCP, los Firewalls, Proxys y/o la instalación de nuevos enlaces y hardware de conectividad.

La Unidad de Informática puede quitar de la red y confiscar sin advertencia cualquier dispositivo sospechoso de violación de esta política.

1.1 Hardware

1.1.1 De la Adquisición de Equipo Informático

I. El área de Informática Institucional propondrá a la Dirección Ejecutiva la inversión necesaria para la adquisición o renovación de equipos, junto con las especificaciones técnicas para los casos de nuevas contrataciones,

obsolescencia de equipos o daños irreparables en los mismos.

II. La Dirección Ejecutiva, con apoyo del área de Informática y UACI, verificará la propuesta de Inversión, hará los cambios necesarios y autorizará para que se inicie el trámite de adquisición.

III. Todo Gerente o Jefe de área de la AMP que detecte necesidades específicas de adquisición o renovación de hardware, hará la consulta al área de Informática Institucional, para que a través de ésta se valide dicha necesidad y se hagan las consolidaciones de las áreas (si es el caso); para luego continuar con los procedimientos de compras establecidos por la UACI, según especificaciones técnicas dadas por el área de Informática Institucional.

IV. Todo hardware adquirido, independientemente del proceso que venga (compra, donación o producto de transferencia de tecnología), deberá ser recibido por el área de Informática Institucional acompañado de una copia de Acta de Recepción emitida por el área de Activo Fijo de la Gerencia Administrativa Institucional.

1.1.2 De la Instalación de Equipo Informático

I. Todo el equipo informático (computadoras, accesorios, etc.), que esté o sea conectado a la Red de Datos de la AMP, o aquel que en forma autónoma se tenga y que sea propiedad de la institución, debe de sujetarse a las normas y procedimientos de instalación que emita el área de Informática Institucional.

II. El área de Informática, en coordinación con el área encargada del control de Activos Fijos de la AMP, deberá tener un registro de todos los equipos informáticos que sean propiedad de la AMP.

III. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de seguridad física, condiciones ambientales, alimentación eléctrica y su acceso a la red de datos de la AMP.

IV. La protección física de los equipos informáticos corresponde a quienes en un principio se les asigna; a ellos también les corresponde notificar los movimientos en caso de que existan, al área de Informática y al área de

Activos Fijos.

V. Todos los Directores, Gerentes o Jefes de áreas de la AMP deberán notificar al área Informática Institucional el ingreso de cualquier equipo informático que no sea propiedad de la AMP y que se utilizará en la red de la Institución.

1.1.3 Del Mantenimiento de Equipo Informático

I. Corresponde al área de Informática Institucional, la realización del mantenimiento preventivo y correctivo de los equipos.

II. En caso de que a los equipos se les realice mantenimientos preventivos o correctivos por terceros, la coordinación al respecto será responsabilidad del área de Informática.

III. Se autorizará el mantenimiento preventivo y correctivo de bienes que sean propiedad de la AMP.

1.1.4 De la Reubicación del Equipo Informático.

I. Todos los Directores, Gerentes o Jefes de áreas de la AMP deberán solicitar al área de Informática Institucional reubicación, reasignación, y todo aquello que implique ubicación de los equipos informáticos.

II. En caso de existir movimientos (reasignación, traslado) de equipos de informática (computadoras, impresores, monitores, baterías de respaldo y otros), el área de Informática Institucional notificará a la unidad encargada del control de Activos Fijos de la AMP los cambios realizados.

III. El equipo de informática a reubicar o trasladar, sea de cualquier área, se hará únicamente bajo la autorización del área de Informática Institucional.

1.1.5 Del control de accesos
Del Acceso a Áreas Críticas.

I. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta el área de Informática Institucional.

II. El área de Informática deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

III. Bajo condiciones de emergencia o de situaciones de urgencia manifestadas,

el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

Del control de acceso al equipo informático.

I. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
II. Las áreas donde se tiene equipo de propósito general cuya misión es crítica, estarán sujetas a los requerimientos que el área de Informática dicte.
III. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el área de Informática Institucional tiene la facultad de acceder a cualquier equipo informático aunque no esté bajo su supervisión.

Del Control de Acceso Local a la Red

I. El área de Informática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
II. El acceso lógico a equipo especializado de tecnología (servidores, enrutadores, bases de datos, Switch, Racks, etc.) conectado a la red será administrado por el área de Informática Institucional.
III. Todo el equipo informático que esté conectado a la Red de Datos o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite el área de Informática Institucional.

Del Control de Acceso Remoto.

I. El área de Informática Institucional es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
II. Para el caso especial de los recursos de accesos remotos, acceso a bases de datos, sistemas de información y otros por parte de terceros, deberán ser autorizados el Director Ejecutivo de la AMP por medio de los mecanismos legales que se estime conveniente.
III. El acceso remoto, acceso a bases de datos, sistemas de información y otros

que realicen personas ajenas a la institución, deberá cumplir las normas que emita el área de Informática Institucional para el acceso a las Aplicaciones o Sistemas de Control Interno.

IV. Tendrá acceso a los sistemas o aplicativos de control solo el personal de la AMP que cuente con un usuario y contraseña y que el Director, Gerente o Jefe haya autorizado.

V. Tendrán acceso a información que se considere de uso restringido, únicamente los usuarios autorizados por la Dirección Ejecutiva de la AMP, con el objeto de garantizar su integridad.

VI. La instalación y uso de los sistemas de información se rigen por las normas y procedimientos establecidos por el área de Informática.

VII. Los servidores de bases de datos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal del área de Informática.

VIII. El control de acceso a cada sistema de información (aplicación) será determinado por la unidad responsable de generar y procesar los datos involucrados.

1.1.6 Software

<u>De la adquisición de software.</u>

I. En concordancia con la política de la institución, el área de Informática Institucional será la encargada de establecer los mecanismos para proveer de sistemas informáticos.

II. Del presupuesto que se le otorga al área de Informática se destinará una cantidad que deberá ser aplicada para la adquisición de programación con licencia.

III. Corresponderá al área de Informática emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

IV. De acuerdo a los objetivos globales el área de Informática deberá respaldar la adquisición y asesoramiento en cuanto a software de últimas versiones.

V. El área de Informática autorizará la instalación de software de dominio público que provenga de sitios oficiales y seguros.

De la instalación de software.

I. Corresponde al área de Informática emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
II. En los equipos tecnológicos únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde al cumplimiento de la Ley de la Propiedad Intelectual.
III. El área de Informática será la responsable de brindar asesoría y supervisión para la instalación de software informático.
IV. El software que desde el punto de vista del área de Informática pudiera poner en riesgo los recursos de la institución, no será instalado en ningún equipo de la Institución.
V. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, actualización, parches de seguridad, privilegios de acceso, y otros que se apliquen).
VI. La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier inconsistencia al área de Informática.

De la actualización del software.

I. La adquisición y actualización de software para equipo especializado informático y de telecomunicaciones se llevará a cabo de acuerdo a la programación anual definida por el área de Informática Institucional.
II. Corresponde al área de Informática solicitar la autorización de cualquier adquisición y actualización del software.
III. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por el área de Informática.

De la auditoria de software instalado.

I. El área de Informática es la responsable de realizar revisiones periódicas para asegurar que sólo licencias autorizadas estén instaladas en las computadoras de la institución.
II. Corresponderá al área de Informática programar y notificar de las visitas para realizar la auditoría a los equipos informáticos.

Del software propiedad de la Institución.

I. Todo software adquirido por la institución sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la Ley de Propiedad Intelectual le confiera.
II. El área de Informática en coordinación con el área de Activos Fijos de la institución deberá tener un registro de todos los Software propiedad de la AMP.
III. Todos los sistemas desarrollados o adquiridos a través de los recursos del área de Informática, se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.
IV. Los datos, las bases de datos, la información generada por el personal, que residen en los servidores deben estar resguardados en medios magnéticos, virtuales y otros que se estime conveniente y bajo la supervisión del área de Informática Institucional.
V. Corresponderá al área de Informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos, así como los sistemas.

Sobre el uso de software académico.

I. Cualquier software que requiera ser instalado para trabajar sobre la Red deberá ser evaluado por el área de Informática.
II. Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la AMP.

1.1.7 Infraestructura Física

El área de Informática Institucional en coordinación con la Gerencia Administrativa velará porque la infraestructura se mantenga de acuerdo a las políticas siguientes:

I. La información digital deberá estar protegida con las copias de respaldo guardadas en medios electrónicos o virtuales con diferente ubicación.
II. Las instalaciones de Informática no deben estar ubicadas cerca de tuberías de agua, y los techos no deben presentar ningún tipo de goteras.
III. En las instalaciones de Informática deben existir extintores de gas, instalados en las salas de Soporte Técnico y del cuarto de servidores.
IV. Se debe contar con control de temperatura en el cuarto de servidores, a fin de conocer con exactitud la temperatura del sitio para hacer las correcciones del caso.
V. La limpieza debe ser diaria, evitando toda la papelería innecesaria.
VI. Prohibición de fumar en las oficinas de Informática, a fin de prevenir un incendio.
VII. Debe existir detectores de humo en todas las instalaciones de Informática.
VIII. Los equipos centrales de Informática deben estar a una temperatura media de 15 a 25 grados centígrados, con un sistema de aire acondicionado independiente e ininterrumpido. El edificio debe contar con un sistema de aire acondicionado central que mantenga las instalaciones a 23 grados centígrados.
IX. Todo el sistema eléctrico debe ser diseñado con el tipo de cable adecuado, centralizando todas las conexiones en un tablero de seguridad ubicado en la Sala de Administradores. Los cables eléctricos se ubican en las partes bajas, y los cables de señal de información serán aéreos.
X. La corriente eléctrica que llega de las distribuidoras de electricidad nacionales, debe pasar por un transformador central y luego llegar al UPS, el cual debe abastecer de energía a los servidores centrales de la Institución.

XI. Con el fin de tener instalada una buena polarización en todo el piso del cuarto de Servidores, que garantice una disminución de la estática en dicho lugar, se debe poseer una instalación metálica unida al polo a tierra de la red del edificio. Por encima de esta red se coloca el doble piso, el cual también sirve para ocultar todos los cables que unen los Sistemas Centrales con los usuarios.

XII. El cuarto de servidores permanecerá constantemente cerrado, teniendo acceso solamente el personal autorizado por el área de Informática.

XIII. El cuarto de servidores es el lugar más privado, el cual es controlado por el Jefe de Informática. Por norma, nadie debe entrar al mismo. El Personal de Informática entrará únicamente para apoyar en casos especiales. Se excluye de esta política a los titulares y al personal de mantenimiento o servicio, siempre que sea para actividades propias de su cargo.

XIV. La autorización para el acceso del personal al equipamiento de conectividad y a los servidores de datos, debe ser gestionada ante el jefe del área de Informática Institucional, por el Jefe del área Interesada.

XV. Los usuarios no pueden acceder a ningún recurso informático mientras no sean autorizados debidamente.

XVI. La autorización de acceso a los recursos es exclusiva del usuario al que le es asignada y no es transferible a otros usuarios o dispositivos.

XVII. Las instalaciones que alberguen equipo de computación deberán estar correctamente polarizadas, y unidas entre sí para efecto de garantizar una red de polarización efectiva.

1.1.8 Infraestructura Red de PC's

1. Identificaciones de usuarios

I. Todos los usuarios que acceden a recursos informáticos de la red requieren de una única e intransferible identidad, normalmente llamado "username" para una persona, y un nombre de máquina para una computadora personal. Esta identidad se usa para representar un usuario o dispositivo en los ambientes informáticos de la red.

II. El área de Informática Institucional proporcionará este identificador como

parte del proceso de autorización. Los identificadores concedidos expiran cuando la Dependencia interviniente solicita expresamente al área de Informática Institucional las cesaciones de acceso para dicho identificador de usuario, o cuando se compruebe un uso indebido. Será obligación de cada Director, Gerente o Jefe informar la baja de los usuarios de su área que cesen en su función para que sea dado de baja el permiso de acceso existente.

III. A menos que por otra parte se especifique explícitamente, el puerto de red autorizado de un dispositivo está incluido como la parte del dispositivo. La desconexión de un dispositivo de su puerto autorizado y conexión a otro puerto de la red es una violación de este código. Laptops y computadoras móviles deben ser autorizadas para usar cualquier puerto de la red.

IV. El mal uso de la identidad de un usuario o un dispositivo constituye falsificación o falsedad. Las acciones que involucren accesos desautorizados, impropios o el mal uso de recursos informáticos de la red están sujetas a sanciones disciplinarias.

2. ***Las contraseñas***

I. Los usuarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos con las contraseñas confidenciales que les fueron confiadas. Estas contraseñas deben construirse de manera que sean difíciles de suponer o adivinar por otros usuarios, deben expirar periódicamente y poseer una longitud mínima.

II. Todas las acciones realizadas bajo los auspicios de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular del identificador. Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente a la Unidad de Informática.

1.1.9 Seguridad

I. Toda la información que se encuentre contenida o circule en la red de computadoras de la Institución y que no ha sido específicamente identificada como propiedad de terceros, será tratada como parte de la información

perteneciente al de la AMP. Esta política se aplicará para prohibir el acceso, divulgación, modificación, cambio, destrucción, pérdida o abuso no autorizado de la información.

II. Adicionalmente, es política de la Institución, proteger aquella información perteneciente a terceros y que haya sido confiada al de la AMP en cumplimiento a los convenios establecidos, si lo hubieran, y a los estándares de la Industria.

III. La instalación y configuración de sistemas operativos, programas, aplicaciones y otras tareas administrativas de los equipos informáticos definidos en al alcance de la presente directiva, será realizado exclusivamente por personal técnico previamente autorizado para tal fin y de acuerdo a los estándares definidos por la Unidad de Informática. Para garantizar la uniformidad de las configuraciones, se elaborará la documentación de apoyo necesaria.

IV. El área de Informática continuamente evalúa otros productos, para la sustitución de los actuales, y de ofrecer ventajas sobre lo instalado, gestionará su adquisición ante la UACI para su implementación.

V. Con la puesta en marcha de esta y otras directivas para la utilización del recurso informático, además de las medidas de protección a la red como Firewall y otros, se trata de garantizar la Integridad de la información y el rápido acceso a la misma, así como su disponibilidad, por lo que la instalación de cualquier software adicional, deberá ser previamente autorizado. Debe resaltarse la frase "cualquier software", ya que en Internet existen disponibles copias de software en versiones Shareware, Freeware o Tríal (prueba por tiempo limitado) y de acuerdo a recientes advertencias de fabricantes de antivirus, algunos Hackers están incluyendo virus o troyanos que se instalan junto con el programa ofrecido, burlando de esta forma la seguridad del equipo.

1.2 Políticas de uso de Internet

Es política de la Institución, proporcionar acceso a la red local e Internet para optimizar la obtención de recursos e información necesarios para complementar el trabajo encomendado a los empleados autorizados. Por lo

que el área de Informática y los miembros del equipo de trabajo realizan monitoreo de seguridad y desempeño de la red, a partir de lo cual pueden establecerse restricciones o limitaciones a la utilización de estos privilegios.

Los usuarios deberán abstenerse de:

I. Visitar sitios de Internet cuyo contenido sea ilegal, obsceno u ofensivo.
II. Enviar o recibir material obsceno o difamatorio; o cuyo objetivo sea incomodar o fastidiar a cualquier otra persona.
III. Realizar instalaciones de accesos no autorizado, ya sea por Conmutación Telefónica (Dial-Up) o Conexión Dedicada (Red Lan), debido al riesgo implícito de intrusión o infección,
IV. Usar programas o aplicaciones potencialmente peligrosas para el rendimiento de la red, tales como uso inadecuado de servicios de mensajería instantánea pública (Messenger y variaciones), así como gestores de descarga Peer to Peer o basados en redes Gnutella (Kazaan, Limewire, Edonkay, etc.) debido al detrimento causado en la red,
V. Subir (upload), Descargar (download), o transmitir software o cualquier material protegido por derechos de autor perteneciente a terceros o a la Institución sin previa autorización del Área de Informática Institucional.

1.3 Políticas de uso de Correo Electrónico

I. Como una herramienta de mejora a la productividad, la Institución impulsa la utilización del correo electrónico para la agilización de las comunicaciones. Todos los mensajes generados o conducidos por las redes de comunicación, serán considerados propiedad de la AMP y no propiedad de los usuarios de los servicios de comunicación.
II. Independientemente de las circunstancias, las contraseñas individuales de las cuentas de correo o de usuario de la red, no deberán compartirse o divulgarse a terceros sin la debida autorización de la Unidad respectiva; efectuarlo supone responsabilidad por las acciones de terceros al usuario autorizado
III. Si los usuarios necesitan compartir información de sus computadoras, pueden utilizar las ventajas de la mensajería electrónica supervisada, directorios

públicos en las redes de área local y cualquier otro medio que haya sido previamente autorizado por el área de Informática. Como una forma de prevención al acceso no autorizado de estos recursos compartidos, se deberán escoger contraseñas de un mínimo de seis caracteres y que sean difíciles de descifrar. No deberán ser palabras escogidas del diccionario, detalles personales o relacionados a la actividad que realiza.

IV. Los usuarios en general no deben interceptar o exponer, o ayudar a la interceptación o exposición de los mensajes electrónicos de la red Institucional. El área de Informática a través del Administrador de la Red tiene claro su compromiso respecto a los derechos de privacidad de cada usuario.

V. De acuerdo a la práctica aceptada por la Industria, el Administrador de la Red recopilará datos estadísticos relacionados con la mensajería electrónica. A manera de ejemplo se realiza de la misma forma en que las Compañías o encargados de las telecomunicaciones que reportan datos sobre la duración de los llamadas, los números marcados, las horas del día en que se registran el mayor o menor número de llamadas, etc. Esta información es utilizada para asegurar la disponibilidad del servicio y la mejora de los sistemas de comunicación.

VI. Se enfatiza que el usuario deberá evitar la distribución y propagación de mensajes no solicitados o envío de Archivos Anexos (Attachments) a un elevado número de destinatarios, lo cual sature el desempeño del Servidor de Correo.

VII. La cantidad máxima a transmitir de archivos adjuntos es de 10Mb. Se debe de utilizar una herramienta de compresión si el o los archivos son grandes, ejemplo: Winzip, freezip u otros que le proporcione la Unidad de Informática Institucional (Unidad de Informática). Considere usar la utilidad de anexar archivos, solo cuando sea necesario.

VIII. Cada cuenta de correo es personal y cada empleado es el ÚNICO responsable de su cuenta.

IX. El envío de correo a un Grupo que incluya "Todos los usuarios de la AMP", es de uso exclusivo de Director Ejecutivo, Gerentes y Jefes. Los mensajes que informan sobre virus, serán enviados solamente por el área de Informática. El

empleado a quien haya llegado o tenga alguna información al respecto, deberá informar al área de Informática Institucional.

X. Es prohibido utilizar los recursos de la Unidad para enviar correos con material que ofenda la moral y las buenas costumbres o que esté fuera de los objetivos de la AMP. Esto se considera una falta, por lo que el jefe del área de Informática lo informará al jefe inmediato del empleado para que haga la amonestación que corresponda según el Reglamento Interno de Trabajo.

XI. No está permitido enviar o remitir correos de tipo "Cadena"; que son aquellos que piden reenviar un mensaje a otras personas conocidas; el empleado deberá ignorarlos e informar al área de Informática.

XII. Cuando se reciba correo de un desconocido, no se debe abrir ningún anexo, sino que se debe eliminar, para evitar cualquier contaminación por virus.

XIII. El usuario deberá crear sus propios grupos de destinatarios frecuentes de correo, en su Libreta personal de Direcciones.

XIV. El empleado debe ser muy selectivo con los destinatarios de sus correos. Debe evitar el envío de mensajes "con copia" a personas innecesarias, ya que esto duplica la cantidad de mensajes, lo que se traduce en espacio en el disco magnético y en consumo de ancho de banda.

XV. Se debe dar a los mensajes un título claro, en el mismo campo "Asunto". Esto permite a quien lo recibe, hacerse una idea de lo que le llega, y evaluar si abrirá o no ese correo.

XVI. El área de Informática Institucional velara por el cumplimiento de estas disposiciones, e informará mensualmente al Director Ejecutivo del mal uso que se haga de esta herramienta.

1.4 Políticas de Desarrollo de Aplicaciones Mecanizadas

I. Todo nuevo desarrollo de sistemas será solicitado al área de Informática Institucional y será su representante quien lo analice y exponga al Director Ejecutivo para su debida aprobación, cuando se tratare de una aplicación que afecte a varias áreas de la AMP o afecte el plan de trabajo anual previamente aprobado; caso contrario, es deber del área de Informática dar el seguimiento correspondiente a fin de satisfacer a la unidad solicitante.

II. La Unidad de Informática previa autorización del Director Ejecutivo, deberá priorizar el sistema que se va a desarrollar, de acuerdo a la importancia y necesidades de las áreas de la AMP. La opción de tercerizar una aplicación o de desarrollarla internamente, será propuesta por el área de Informática junto con el área solicitante. Una vez se decida la conveniencia de tercerizar una aplicación, el área solicitante trabajará conjuntamente con el área de Informática en la elaboración de los términos de referencia para ser enviados a la UACI; después que se realice el contrato, será el área solicitante la responsable de administrar la ejecución del proyecto, apoyada por el área de Informática Institucional.

III. Todo nuevo desarrollo de sistemas a realizarse por el área de Informática Institucional, deberá contemplar los estándares establecidos.

1.5 Políticas de Prevención, Manejo y Contención de Epidemias

Para evitar la pérdida de información Institucional, minimizar intrusiones y preservar el rendimiento de las redes informáticas, es necesario realizar un esfuerzo por parte de usuarios y administradores para eliminar amenazas de virus y contener la propagación de infecciones.

1.5.1 Por parte del Usuario

I. El usuario deberá permitir los procesos de búsqueda de virus que los programas instalados efectúen y por ningún motivo deberá interferir o desactivar las aplicaciones de seguridad vigentes.

II. Evitar el uso, descarga o instalación de software o aplicaciones inseguras o no autorizada por el área de Informática.

III. Abstenerse de modificar los parámetros de configuración de red de los equipos informáticos.

IV. El uso de acceso Telefónico Conmutado será configurado por el área de

informática con autorización previa de la Dirección Ejecutiva.

V. Se deberá prestar atención a cualquier funcionamiento irregular o anómalo de los equipos informáticos, como son: tiempo excesivo de carga de sistema operativo o aplicaciones, retraso exagerado en comunicaciones de red local o Internet, surgimiento de iconos desconocidos en el escritorio y tráfico de red elevado aun cuando la máquina no realiza ningún proceso en red. Estas anomalías deben informarse inmediatamente a la Unidad de Informática.

VI. Al detectar cualquier situación anómala el usuario deberá desconectar el equipo de la red local y evitar la conexión telefónica o sustracción de datos mediante disco flexible a otro medio removible.

VII. El usuario estará sujeto a las disposiciones y/o recomendaciones hechas por la Unidad de Informática en cuanto a la estandarización del uso de protectores de pantalla, escritorios y utilitarios diversos.

1.5.2 Por parte del área de Informática Institucional

I. Velará por la puesta al día de aplicaciones antivirus y obtención de actualizaciones de seguridad de los Sistemas Operativos y aplicaciones en uso.

II. Se realizará verificaciones periódicas de equipos en sectores que históricamente hayan sido afectados por infecciones, para deducir procedimientos inadecuados o mal uso por parte de los usuarios,

III. Al encontrarse infectada una computadora o red, se aislará del resto de la red y se procederá a la limpieza o restauración del equipo. Durante este proceso, se deberá informar al usuario sobre la fuente de infección y se ofrecerán alternativas de solución para la continuidad del trabajo desempeñado en el equipo en cuestión,

IV. El administrador tendrá identificado la clasificación de los usuarios, los cuales estarán sujetos a las restricciones según las atribuciones asignadas a cada uno de ellos.

1.6 Políticas de Contingencia

Con la finalidad de contar con alternativas de actuación ante situaciones imprevistas se establece las siguientes políticas:

I. Contactar y construir una relación de cooperación con empresas o instituciones que posean PC server con las mismas características de las que posee el de la AMP, para obtener apoyo en caso de imposibilitarse el ingreso a las instalaciones donde se encuentra el cuarto de servidores, ya sea por motivos de desastres naturales u otras causas.

II. Establecer mecanismos de comunicación para contactar inmediatamente a cada miembro del área de Informática. Debe disponerse de las direcciones de residencia, números telefónicos fijo y/o celular, correo electrónico, etc. Toda esta información debe ser compartida por las personas antes señaladas y por el Director Ejecutivo de la AMP.

III. Definir un área específica en una de las oficinas que pertenecen a la AMP y que se encuentre fuera de la oficina central (Ej.: Delegaciones Locales, etc.), para que en caso de emergencia se pueda trasladar en forma inmediata el área de Informática.

IV. Mantener capacidad instalada en la Gerencia Administrativa, para atender los requerimientos de servicios de emergencias de energía eléctrica, telefonía, transporte, etc.

V. Instalar una planta eléctrica que suministre energía al área de Informática, para ponerla en funcionamiento cuando las circunstancias lo demanden.

VI. Poseer en existencia repuestos básicos de funcionamiento de PC para atender necesidades urgentes.

2 Sitio Web

I. Con el objetivo de tener un sitio WEB para brindar un espacio informativo de las principales actividades realizadas y por realizar por parte de la Autoridad Marítima Portuaria, debe existir un servidor dedicado para esta misión y la dirección de la página web debe ser: www.amp.gob.sv

II. El diseño y mantenimiento del sitio WEB corre a cargo del área de Informática; La parte creativa y administrativa, es controlada por el área de Comunicaciones Institucional.

III. Son funciones del área de Comunicaciones Institucional establecer el "Arte" o presentación que lleva el sitio, así como su contenido.

IV. La periodicidad con que se cambia dicho "arte", para evitar una monotonía visual, debe ser como mínimo seis meses y el contenido debe ser actualizado como mínimo cada semana.

V. Para recopilar la información a ser actualizada, cada gerente de área debe nombrar a un responsable de su Gerencia, quien la enviará al área de Comunicaciones Institucional; con el objeto de depurar la información y darle el visto bueno, antes de publicarla en la página web.

3 Responsabilidades Generales

El área de Informática Institucional deberá verificar el cumplimiento de los estándares de seguridad proporcionados en este documento, incluyendo el hardware, software y respaldo de la información con los encargados de cada área. El respaldo de la información debe responder a procedimientos previamente establecidos por la Unidad de Informática Institucional.

4 Sanciones

Todo empleado que tenga asignado o utilice equipo informático deberá conocer las Políticas y Estándares Institucionales en Materia de Informática, por lo cual no existirá motivo para no cumplirlas. El área de informática informará al Director Ejecutivo de los usuarios que no respeten dichas políticas. Si esta conducta persiste, se iniciará el procedimiento sancionador previsto en el Reglamento Interno de Trabajo de la AMP.

5 Vigencia

Este documento entrará en vigencia a partir de la aprobación del mismo por el Director Ejecutivo de la Institución.

6 De las reformas al documento

Este documento de Políticas será revisado anualmente por la Unidad de Informática Institucional. Toda propuesta de reforma se presentará al Director Ejecutivo con una exposición de motivos y la justificación correspondiente, para que él decida lo que considere pertinente.

7 De la divulgación

Las presentes Políticas se divulgarán a todos los usuarios de la red por medio impreso, correo electrónico u otros medios digitales.

COMUNÍQUESE,

MARIO GUILLERMO MIRANDA
DIRECTOR EJECUTIVO