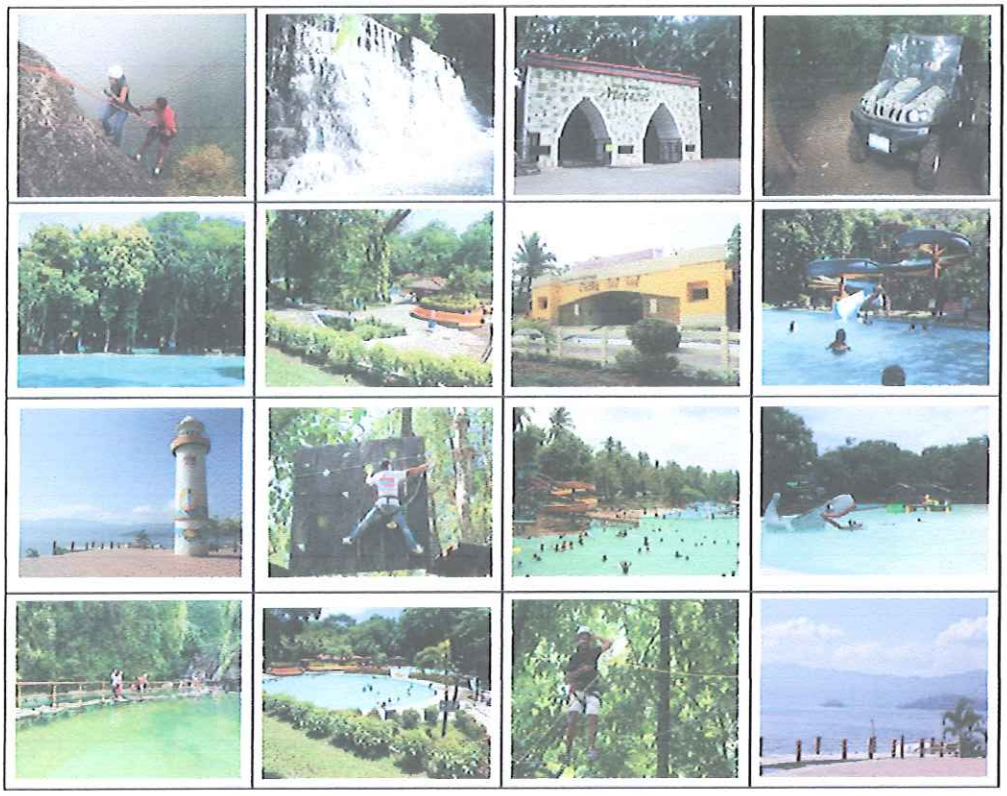
POLÍTICAS Y PROCEDIMIENTOS SOBRE CONTROLES DE APLICACIÓN DEL PROCESAMIENTO DE INFORMACIÓN Y MANTENIMIENTO DE APLICACIONES, DOCUMENTACIÓN Y LICENCIAMIENTO DEL SOFTWARE



SAN SALVADOR, EL SALVADOR, CENTRO AMÉRICA

HOJA DE AUTORIZACIÓN

REVISADO POR:

Nombre: Ing. José Mauricio Vásquez

Cargo: Jefe Unidad de Tecnología de Información y Comunicación

Autorizado por Junta Directiva de ISTU en Reunión Ordinaria 20/16, de fecha 30 de agosto de 2016, Punto Único: "Aprobación de Manuales, Instructivos, Políticas y Procedimientos Administrativos"

CONTENIDO:

ÍNDICE

1. OBJETIVO

Establecer el marco de referencia para la regulación de la actividad informática, su correcta administración, buen uso y aprovechamiento de todos los recursos informáticos del Instituto.

Con esto se proporcionará a las Dependencias de la Institución, infraestructura y servicios informáticos que les permitan mejorar y enriquecer sus procesos en el manejo de información, para incrementar la productividad en el desempeño diario de las funciones y actividades bajo su responsabilidad.

2. ÁMBITO DE APLICACIÓN

CUMPLIMIENTO

Las presentes políticas aplican a todos los funcionarios, empleados permanentes, asesores, empleados temporales y terceros que usen equipos dentro del Instituto o accedan la Intranet del Instituto. En adelante la palabra "usuario" se referirá a cualquiera de estas personas.

APLICACIÓN

La Unidad de Tecnología de Información y Comunicación, será la responsable de velar por el cumplimiento de las presentes políticas. En adelante las siglas "UTIC" se referirán a esta Unidad.

ALCANCE

Las presentes políticas serán aplicables en todos los inmuebles propiedad del ISTU, en donde se cuente con equipo informático.

3. BASE LEGAL

Sustentan jurídicamente la emisión y aplicación de la presente Política Informática los siguientes ordenamientos:

- Constitución de la República de El Salvador.
- Ley del ISTU.
- Reglamento Interno ISTU.

- Ley de Fomento y Protección de la Propiedad Intelectual.
- Ley de Marcas y otros Signos Distintivos.
- Ley de Ética Gubernamental y su Reglamento.
- Ley de Acceso a la Información Pública.
- Ley Orgánica de Administración Financiera del Estado y su Reglamento.
- Ley de Adquisiciones y Contrataciones de la Administración Pública y su Reglamento.
- Código Tributario y su Reglamento.
- Contrato Colectivo de Trabajo.
- Reglamento de las Normas Técnicas de Control Interno Especificas del ISTU
- Otras disposiciones legales aplicables.

4. DEFINICIONES

ARCHIVO

Conjunto de información organizada localizada en el disco duro de una PC o un servidor

CORREO ELECTRONICO

Mensajes electrónicos enviados o recibidos a través de Internet o de una red local de computadoras mediante un servidor de correo electrónico.

DIRECCIÓN IP

Número de identificación único y numérico asignado a cada equipo conectado a una red de computo, de acuerdo con los estándares internacionales de la tecnología TCP, el cual es determinado por el administrador de la red en uso, por ejemplo, 191.31.140.115.

EQUIPO DE CÓMPUTO

Término genérico que se utiliza en este manual, para denominar a una computadora personal, impresora, scanner, disco duro, unidad de disquete, o cualquier otro componente de la computadora.

5. RESPONSABILIDADES

- Es responsabilidad del Jefe de la Unidad de Tecnología de Información y Comunicación, proponer modificaciones a este reglamento y mantener actualizado el

mismo.

- Es responsabilidad del Jefe de la Unidad de Tecnología de Información y Comunicación, revisar y velar por el cumplimiento de este reglamento y proponer mejoras al mismo.

- Es responsabilidades de los Jefes de las distintas unidades organizativas del ISTU, dar fiel cumplimiento a este reglamento y proponer mejoras al mismo.

- Es responsabilidad de las Unidades Organizativas del ISTU, cumplir lo dispuesto en este reglamento, en lo aplicable.

6. LINEAMIENTOS GENERALES

I. INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN.

1) Los Jefes de las Unidades Organizativas en coordinación con la sección de Inventarios y la Unidad de Tecnología de Información y Comunicación, llevarán un inventario centralizado de los recursos de tecnologías de información del ISTU, así como contar con mecanismos de control según el tipo de información que contienen, procesan, transfieren, transportan o almacenan.

2) Los Jefes de las Unidades Organizativas en coordinación con el Jefe de la Unidad de Tecnología de Información y Comunicación, serán los responsables de ejecutar el procedimiento de mantenimiento del inventario de los recursos de tecnologías de información.

3) El personal que solicite o tenga a resguardo una computadora de escritorio, estación de trabajo, portátil, servidor, impresora, etc., se compromete a resarcir el daño ocasionado por robo, perdida, maltrato o mal manejo del mismo o alguno de sus componentes.

4) Toda la información generada, guardada y registrada en el equipo de computo es propiedad del ISTU y es responsabilidad del resguardarte el uso que se le dé, así como de su conservación.

5) La Unidad de Auditoria Interna tendrá acceso irrestricto a los archivos y documentos que sustentan la tecnología de información, cuando la naturaleza de la auditoria así lo requiera.

6) Todos los funcionarios y empleados del ISTU son responsables de etiquetar la información que se encuentre almacenada en papel o medios magnéticos y ópticos, indicando su tipo de clasificación para facilitar su control, manejo y cuidado, de acuerdo a los procedimientos que para el efecto se establezcan.

7) El ISTU representado por el personal de la UTIC, tendrá la facultad de administrar, controlar, auditar, desarmar, reubicar el equipo según los considere conveniente, para su mejor uso y aprovechamiento con la debida justificación.

8) Se prohíbe almacenar cualquier tipo de información ajena al trabajo del ISTU (Por ejemplo: archivos de música, imágenes, videos, etc.). En el caso de que el personal autorizado localice este tipo de archivos tendrá la facultad de eliminarlos sin la necesidad de consultar al usuario.

9) Los equipos informáticos tendrán configurado el modo de ahorro de energía cuando este se encuentre en inactividad (Apagado de monitor, modo suspendido, etc).

RESPECTO AL SOFTWARE.

1) Se prohíbe la instalación de Software, Programas y/o Aplicaciones que no cuenten con la licencia del producto otorgado a el ISTU.

2) Se prohíbe la instalación de Software, Programas y/o Aplicaciones Shareware, Freeware y Trial, que comprometan el uso eficiente de la red y los equipos de cómputo, o que resulten ajenos a los objetivos institucionales.

3) Se prohíbe los fondos de pantalla, colores de ventanas y letras que no sean los autorizados por la UTIC.

RESPECTO A LA IMPRESIÓN.

1) Las impresiones son de uso común y no personal.

2) Se prohíbe la impresión total o parcial de información ajena a los objetivos institucionales.

3) Para fomentar el ahorro de papel y otros recursos, se deberá imprimir solo el documento original, las copias de este se deberán enviar a través de un archivo digital a los interesados, vía correo electrónico o depositarlo en la Intranet de la Institución.

4) Utilizar la impresión a doble cara y calidad "Economo de" (Ahorro de tóner o borrador) cuando sea posible.

5) Solo el personal de la UTIC tiene autorización para la manipulación de los equipos de impresión que se encuentren en el ISTU (Propios o Arrendados).

6) La asignación de equipos de impresión será según las necesidades de las Unidades organizativas, así como por su ubicación y acceso.

SOPORTE TECNICO.

1) Únicamente el personal de Soporte Técnico autorizado por la UTIC podrá abrir, revisar, evaluar o reparar el equipo de cómputo. Por ningún motivo podrá hacerlo personal ajeno.

2) El mantenimiento Correctivo y/o Preventivo de Hardware y Software será única y exclusivamente para el equipo propiedad del ISTU y realizado por el personal de la UTIC.

3) Se establecerá un calendario de mantenimiento preventivo a los bienes informáticos de todas las áreas del ISTU, en este sentido se prevé realizar un mínimo de 1 revisión al año, por el personal de Soporte Técnico.

4) El equipo que requiera de mantenimiento correctivo de software o hardware será trasladado al área dedicada a estas actividades, este movimiento se realizará previa evaluación del personal autorizado.

5) El personal autorizado para evaluar las fallas del equipo deberá emitir un diagnóstico por escrito electrónico (archivo de texto) y éste deberá ser presentado o enviado vía correo electrónico al Jefe de área, para tomar la decisión correspondiente.

6) Todo periférico, tarjeta o aditamento que sea ajeno al equipo y que se pretenda incorporar a éste, deberá ser previamente autorizado por parte del personal de Soporte Técnico.

7) Todo el equipo de cómputo contará con sello de seguridad para evitar la abertura del mismo, si por alguna circunstancia este sello es violado por personas ajenas al personal de Soporte Técnico, se procederá a levantar un acta para deslindar responsabilidades.

USO DE INTRANET (RED DE COMPUTO INTERNA).

1) Sólo el personal de la UTIC, está autorizado para cambiar la configuración física y lógica de la red, es decir cables, rosetas, direcciones IP, configuración de las impresoras compartidas en red, tipo de red, etc. Así como para asistir a los usuarios en problemas de comunicación.

2) Todo equipo deberá conectarse a la roseta de red con "cable de parcheo" certificado que tiene una longitud máxima de 2.13 metros (7 pies).

3) Por ningún motivo se podrá conectar el equipo con "cable de parcheo" no certificado y con longitud mayor a 2.13 metros.

4) Será responsabilidad total del usuario el uso de la información en su equipo u otros recursos al compartirlos en la red. Todo recurso compartido deberá tener contraseña o determinar que usuarios tendrán acceso, así como el tipo de permisos asignados.

5) En caso de requerir un mayor número de máquinas instaladas en un lugar donde sólo existe un nodo de red:

6) Solamente el personal de la UTIC está autorizado a instalar hubs, switches y Access point, previo estudio de factibilidad.

7) Todas las máquinas deberán quedar conectadas al switch con "cable de parcheo" certificado de 2.13 metros de longitud, en el caso de access point, con tarjetas de red inalámbricas que cumplan con los estándares internacionales de seguridad.

8) Está prohibida la instalación de programas ajenos al ISTU que utilicen los recursos de la red a menos que sean autorizados por la UTIC.

9) Está prohibido el acceso a los "Racks" ya que son áreas de equipamiento de redes, en los cuales se encuentra el cableado y el equipo de comunicación.

10) Los daños ocasionados al cableado y/o roseta de la red por negligencia del usuario serán directamente responsabilidad del mismo, comprometiéndose a cubrir el costo por la reparación de dichos daños.

II. CONTROL DE ACCESOS.

USUARIOS, CONTRASEÑAS, DATOS Y ACCESO A LA RED.

1) Las claves de acceso a la red constan de dos partes: una es la cuenta de usuario y la otra es la contraseña, por lo que las cuentas serán personales.

2) Todo usuario registrado en la red será responsable de proteger su nombre de usuario, contraseña y datos de cualquier acceso no autorizado.

3) Las cuentas de usuario registradas en la red son de carácter estándar, únicamente el personal de la UTIC, tiene los privilegios de modificar la configuración e instalación de aplicaciones adicionales a los equipos de cómputo.

4) Las claves de acceso serán habilitadas únicamente por el personal de la UTIC a funcionarios y empleados con base a sus roles o funciones y llevara un registro de los derechos de acceso de dichos usuarios.

5) El usuario es responsable de su clave de acceso. Ninguna contraseña debe ser divulgada, escrita, enviada por correo electrónico y compartida por cualquier otra persona ajena al usuario, ya que esto se considera una violación a la seguridad de la red y si es detectado, se suspenderá la cuenta y se enviará un oficio informativo al Jefe del área a la cual está adscrito el usuario.

6) El usuario es responsable por las acciones que se lleven a cabo con su cuenta personal, es decir, las modificaciones a las bases de datos, archivos recibidos o enviados por correo

electrónico, uso indebido de los recursos de la red.

7) Queda estrictamente prohibido el uso de un nombre de usuario distinto al propio, aun con el consentimiento del usuario original 44. El usuario es responsable de su clave de acceso. Ninguna contraseña debe ser divulgada, escrita, enviada por correo electrónico y compartida por cualquier otra persona ajena al usuario, ya que esto se considera una violación a la seguridad de la red y si es detectado, se suspenderá la cuenta y se enviará un oficio informativo al Jefe del área a la cual está adscrito el usuario.

8) El usuario es responsable por las acciones que se lleven a cabo con su cuenta personal, es decir, las modificaciones a las bases de datos, archivos recibidos o enviados por correo electrónico, uso indebido de los recursos de la red.

9) Queda estrictamente prohibido el uso de un nombre de usuario distinto al propio, aun con el consentimiento del usuario original.

ADMINISTRACION DE LA RED.

1) La UTIC, tiene la autoridad para controlar y negar el acceso a cualquier funcionario que viole las políticas o interfiera con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas así como a las jefaturas inmediatas.

2) La seguridad en la red estará a cargo del personal de la UTIC, el cual utilizará diferentes tipos de Hardware o Software para controlar los accesos a Internet y servidores que proporcionen los accesos a la red interna y administrar los recursos.

3) El personal de la UTIC no ejerce control sobre el contenido de la información que circula a través de la red, del origen y destino, esta queda bajo la responsabilidad del usuario. No lo anterior, el personal de la UTIC tiene en funcionamiento permanente herramientas de monitoreo y control que posibilitan analizar y detectar usos indebidos; por lo tanto se advierte que el contenido de la información que circula por la red, es monitoreada y sujeta a controles y reportes sobre su uso.

4) Corre por cuenta o riesgo del usuario cualquier información obtenida por medio del servicio

de Internet.

5) El incurrir en el incumplimiento de los siguientes puntos por primera vez, ameritará amonestación por escrito al usuario de la cuenta con copia al titular del área. En caso de reincidir se procederá a reportar a la Unidad de Auditoria Interna con copia a la Dirección Ejecutiva, y se procederá a la cancelación de la cuenta y sólo podrá reactivarse con previa autorización del titular del área.

6) Transmisión y circulación de materiales con derechos de propiedad intelectual, amenazantes u obscenos, ya sea en forma individual o masiva.

7) Acceso a páginas de Internet para obtener información no relacionada con el área de trabajo del usuario. Esto incluye sitios de pornografía, deportes, juegos, música, video, chistes, piratería informática, etc.

8) Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricas de redes y sistemas.

9) Monopolizar los recursos en perjuicio de los otros usuarios, incluyendo: el envío de mensajes masivos a todos los usuarios de la red, inicio o continuación de cadenas, creación de procesos innecesarios, generar impresiones voluminosas, uso de recursos de impresión no autorizado.

10) La exhibición de material pornográfico en cualquier lugar de la Institución utilizando el equipo de cómputo y/o los servicios de comunicación de la institución.

11) Cualquier usuario del ISTU que modifique la configuración de conectividad de red (IP, Gateway, DNS, etc.) se considerará como una amenaza a la seguridad de la información institucional. El personal de Redes suspenderá inmediatamente la cuenta de acceso a la red institucional y enviará un oficio informativo a Dirección Ejecutiva.

12) El personal de la UTIC atenderá a todos los usuarios que reporten un mal funcionamiento de su equipo de cómputo y de los servicios de red, Internet y correo electrónico, y presentará alternativas de apoyo al usuario. Asimismo, implementara

jornadas de capacitación permanentes para su uso óptimo.

APLICABLES A CORREO ELECTRONICO.

1) La creación de cuentas de correo electrónico deberá solicitarla el jefe de área respectivo por escrito a la UTIC.

2) La información enviada o recibida en el correo electrónico será responsabilidad total del usuario de la cuenta, dejando al ISTU fuera de cualquier responsabilidad penal o civil en la cual incurriera.

3) Los correos que se envíen serán de la completa responsabilidad del usuario que lo emite, y deberá basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos correos podrán emplearse en contra de los intereses de personas físicas así como del ISTU ni de cualquier otra institución.

4) Los nombres de las cuentas de correo estarán conformadas por la letra inicial de los nombre y las letras del apellido del usuario, en caso de que ya exista se utilizarán variantes con el nombre o usando el apellido materno. La clave o password será definida por el usuario y no debe proporcionarla al personal de la UTIC.

5) Está estrictamente prohibido el envío de información confidencial del ISTU a través del correo electrónico.

6) Está estrictamente prohibido el envío de correos "cadena".

7) Evitar abrir los correos en los que exista duda de su procedencia o no solicitados.

8) Al final de cada año se deberá confirmar a la UTIC la permanencia y uso de las diferentes cuentas de usuario. En caso de no recibir la confirmación al inicio de cada año las cuentas serán eliminadas.

9) El tamaño máximo para envío de correo será de 50 MB y el tamaño máximo para recibir correos será de 50 MB o menor de acuerdo al límite de espacio libre del servidor. (esto es vigente para todas las áreas) 54. La creación de cuentas de correo electrónico deberá

solicitarla el jefe de área respectivo por escrito a la UTIC.

10) La información enviada o recibida en el correo electrónico será responsabilidad total del usuario de la cuenta, dejando al ISTU fuera de cualquier responsabilidad penal o civil en la cual incurriera.

11) Los correos que se envíen serán de la completa responsabilidad del usuario que lo emite, y deberá basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos correos podrán emplearse en contra de los intereses de personas físicas así como del ISTU ni de cualquier otra institución.

12) Los nombres de las cuentas de correo estarán conformadas por la letra inicial de los nombre y las letras del apellido del usuario, en caso de que ya exista se utilizarán variantes con el nombre o usando el apellido materno. La clave o password será definida por el usuario y no debe proporcionarla al personal de la UTIC.

13) Está estrictamente prohibido el envío de información confidencial del ISTU a través del correo electrónico.

14) Está estrictamente prohibido el envío de correos "cadena".

15) Evitar abrir los correos en los que exista duda de su procedencia o no solicitados.

16) Al final de cada año se deberá confirmar a la UTIC la permanencia y uso de las diferentes cuentas de usuario. En caso de no recibir la confirmación al inicio de cada año las cuentas serán eliminadas.

17) El tamaño máximo para envío de correo será de 50 MB y el tamaño máximo para recibir correos será de 50 MB o menor de acuerdo al límite de espacio libre del servidor. (esto es vigente para todas las áreas)

18) Se recomienda crear carpetas para la mejor administración del correo y mantener la bandeja de entrada con la menor cantidad de mensajes.

19) En el caso de que un usuario desee enviar o recibir un correo electrónico cuyo tamaño sea mayor a 50MB, se deberá dirigir al personal de la UTIC, donde se le presentará alguna alternativa. Es preciso aclarar que este tipo de requerimientos serán considerados sólo si el correo a enviar o recibir será utilizado para fines laborales.

20) El personal de la UTIC se reservará el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad de la información institucional, detección de intrusos, propagación de virus, seguridad de la red del ISTU e inclusive podrá ir al lugar del usuario a verificar en su PC el uso que le esté dando a su correo institucional.

APLICABLES A INTERNET.

1) Cuando las necesidades del servicio así lo requieran, el Jefe de Área deberá solicitar por escrito al personal de la UTIC la habilitación del servicio de Internet para personal eventual, Auditoria externa y similares. Esta solicitud deberá ser enviada con copia a la Dirección Ejecutiva.

2) A continuación se detallan algunos programas y acciones que no deben ser usados para el buen desempeño del servicio de Internet:

3) Limitar el acceso a Chats, icq, bbs, irc, talk, write o cualquier programa utilizado para realizar pláticas en línea.

4) Cualquier programa destinado a realizar enlaces de voz y video, sin que esto sea previamente autorizado y justificado por la Dirección Ejecutiva o de Área.

5) Descargas de gran tamaño (mayores a 25 Mb) o uso de archivos de audio y multimedia.

6) Páginas que no tengan relación directamente con las labores propias del usuario en el trabajo.

7) Las paginas dedicados a la difusión personal o Sitios de interacción social (redes sociales) solo podrán accederse de 12MD a 1MP de Lunes a Viernes.

8) Cuando una unidad organizativa necesite acceso a los literales anteriores para el

desarrollo de sus actividades fuera del horario establecido deberá solicitarlo por escrito a la Dirección Ejecutiva.

9) También se prohíbe el acceso a las páginas del tipo:
   - Dedicadas a proveer juegos en línea.
   - Con información que no sea relevante al trabajo del área.
   - Con material para adultos.
   - Servidores de almacenamiento masivo

III. MEJORES PRÁCTICAS EL USO DE LOS BIENES Y SERVICIOS INFORMÁTICOS.

MEJORES PRÁCTICAS PARA EL CORREO ELECTRÓNICO

1) No enviar mensajes que violen los derechos de los destinatarios o de terceras personas.

2) Al elaborar un correo electrónico se deberá hacer uso de un lenguaje apropiado.

3) No intercambiar grandes volúmenes de información, a través de este servicio.

4) Eliminar de su buzón de correo aquellos mensajes que no necesite mantener almacenados.

5) No enviar mensajes con juegos, pornografía, obscenidades, virus, etc.

6) No iniciar ni continuar una cadena de mensajes.

7) Tenga cuidado con los ataques de phishing (robo de identidad), evite enviar cualquier tipo de información personal como: información de identidad, información sobre cuentas bancarias, nip o usuarios y claves de accesos. Esta información generalmente es solicitada con uso fraudulento por un atacante, nunca será solicitada por una empresa, institución o banco. La omisión a esta recomendación puede poner en riesgo su seguridad personal, familiar y su patrimonio.

8) Si un usuario sabe que dejará de revisar su correo durante un tiempo considerable (por viaje, enfermedad, vacaciones, etc.), deberá informar a la Subdirección de Sistemas para evitar que durante su ausencia el buzón se llene y pierda todos los e-mails que intenten llegar durante ese tiempo.

MEJORES PRÁCTICAS ANTE LAS AMENAZAS A TRAVÉS DE LA WEB

1) El uso global de Internet facilita de manera extraordinaria comunicaciones, sin embargo esto lo convierte en una fuente de vulnerabilidad de nuestra información personal e institucional. Por esto se recomienda cautela en el manejo de los servicios e información que existe en esta red.

2) Cuando en una página de un sitio web detecte alguna amenaza, como virus, gusanos, troyanos, addware, etc., que no pueda ser removido o eliminado por completo, notifique inmediatamente al personal de Redes. Nunca confirme una solicitud de estas páginas.

3) El usuario debe verificar periódicamente (se sugiere cada semana) su computadora personal.

4) Cada usuario es responsable y debe tomar medidas para evitar el contagio de virus, troyanos, gusanos, etc., en los archivos adjuntos que envía.

5) El usuario queda eximido de cualquier responsabilidad cuando su cuenta de correo sea afectada por la actividad de un virus, troyano o gusano, el cual envíe mensajes a nombre del usuario, siempre y cuando se compruebe que el usuario es ajeno a la intromisión del virus en la red institucional de la SMA, puesto que el virus utiliza de manera aleatoria las cuentas de usuarios para propagarse a otros equipos, esto puede ocurrir antes de que las versiones actualizadas de los antivirus detecten su presencia en la red.

7. VIGENCIA

El presente Reglamento entrará en vigencia a partir de la fecha de aprobación por parte de la Honorable Junta Directiva del Instituto Salvadoreño de Turismo.

8. CONTROL DE MODIFICACIONES

FORMATO PARA EL REGISTRO DE MODIFICACIONES

Fecha de Cambio de Edición:

N°	DESCRIPCION DE MODIFICACIONES
1	
2	
3	