

**POLÍTICAS DE USO Y SERVICIO DE BIENES  
INFORMÁTICOS  
DE LA SECRETARÍA DEL MEDIO AMBIENTE  
DEL GOBIERNO DEL DISTRITO FEDERAL**  
Agosto, 2009

**Preparó**

Dirección Ejecutiva de Administración  
Dirección de Monitoreo Atmosférico

**Responsables**

Lic. Antonio Efrén Parra Rivera  
J.U.D. Informática de la D.E.A.  
Ing. Alejandro Ríos Mejía  
Subdirector de Sistemas de la D.M.A.

## ÍNDICE

<b>INTRODUCCIÓN</b>	<b>3</b>
<b>OBJETIVO DE LA SEGURIDAD INFORMATICA</b>	<b>4</b>
<b>1. USO DE LOS BIENES INFORMÁTICOS</b>	<b>5</b>
<i>RESPECTO AL SOFTWARE:</i>	<i>5</i>
<i>RESPECTO AL HARDWARE E INFORMACIÓN</i>	<i>6</i>
<i>RESPECTO A LA IMPRESIÓN</i>	<i>6</i>
<b>2. SOPORTE TÉCNICO</b>	<b>7</b>
<b>3. USO DE LA RED DE CÓMPUTO</b>	<b>8</b>
<b>4. USUARIOS, CONTRASEÑAS, DATOS Y ACCESO A LA RED</b>	<b>11</b>
<b>5. ADMINISTRACIÓN DE LA RED</b>	<b>12</b>
<b>6. APLICABLES A CORREO ELECTRÓNICO</b>	<b>13</b>
<b>7. APLICABLES A INTERNET</b>	<b>17</b>
<b>8. MEJORES PRÁCTICAS EL USO DE LOS BIENES Y SERVICIOS INFORMÁTICOS</b>	<b>18</b>
<b>MEJORES PRÁCTICAS PARA EL CORREO ELECTRÓNICO</b>	<b>18</b>
<b>MEJORES PRÁCTICAS ANTE LAS AMENAZAS A TRAVÉS DE LA WEB</b>	<b>19</b>
<b>GLOSARIO DE TÉRMINOS</b>	<b>21</b>

## **POLÍTICAS DE USO Y SERVICIO DE BIENES INFORMÁTICOS**

### **DE LA SECRETARÍA DEL MEDIO AMBIENTE DEL GOBIERNO DEL DISTRITO FEDERAL**

#### **INTRODUCCIÓN**

La Secretaría del Medio Ambiente del Gobierno del Distrito Federal (**SMA**) cuenta en estos momentos con una importante infraestructura de medios informáticos integrada por equipo de cómputo de última generación; servidores de bases de datos y aplicaciones; una red estructurada de servicios de voz y datos con certificación, enlazados por diferentes tipo de medios de comunicación hacia Internet así como servicio de correo electrónico. Todo ello en cada una de las dependencias que la conforman, la cual está a disposición, con distintos niveles de acceso, del personal de la SMA y al público en general para compartir información en forma rápida y confiable.

Con el fin de proporcionar servicios informáticos y de comunicación con alto grado de funcionalidad, confidencialidad, integridad y disponibilidad de la información generada y utilizada por el personal de la SMA, así como administrar, controlar y aprovechar eficientemente los equipos de cómputo y comunicaciones con que cuenta la SMA, se requiere instrumentar procedimientos de organización y regulación de este sistema a fin de convertirlo en un instrumento eficiente y seguro.

Actualmente la diversidad de los ambientes distribuidos y su posible sobreposición (programas, sistemas operativos, etc.) hace que éstos corran bajo diferentes plataformas como Windows 95/98, NT, 2000, XP, 2003, Vista, Linux, Unix, Mainframes, etc., dando lugar, ya sea por descuido o falta de conocimiento a posibles huecos de seguridad que hacen vulnerables numerosos equipos o amplias áreas de trabajo que pueden ser utilizados por usuarios no autorizados (hackers), para visualizar, alterar, corromper o eliminar la información confidencial de Secretaría.

## OBJETIVO DE LA SEGURIDAD INFORMÁTICA

Los sistemas de información son fundamentales para cualquier compañía y deben ser protegidos; estos incluyen todos los datos de la organización, así como también los bienes y recursos informáticos que permiten a ésta almacenar y hacer circular estos datos.

La seguridad informática consiste en garantizar que los bienes y los servicios informáticos de una organización se usen únicamente para los propósitos para los que fueron creados o adquiridos y dentro del marco previsto.

Generalmente la seguridad informática se resume en cinco objetivos principales:

- **Integridad:** Garantizar que los datos sean los que se supone que son, es decir, que sean los correctos o no estén corruptos.
- **Confidencialidad:** Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **Disponibilidad:** Garantizar el correcto funcionamiento de los sistemas de información, así como de las tecnologías de comunicación.
- **Evitar el rechazo:** Garantizar la no negación de una operación o acceso ya concedidos.
- **Autenticación:** Asegurar que los individuos que pretenden tener acceso a los recursos, sean quienes deben ser.

Además de los objetivos anteriores, la seguridad informática también planea e implementa todas las medidas necesarias para salvaguardar la información de vital importancia, así como evitar los accesos no autorizados a los equipos personales y principalmente a los servidores. Dentro de las medidas definidas se encuentran las siguientes:

- 1) Preparar procedimientos acordes al centro de datos.
- 2) Preparar y dar a conocer las políticas de seguridad.
- 3) Concientizar, tanto a los administradores como a los usuarios, de la importancia del tema.
- 4) Mejorar en forma continua la seguridad.
- 5) Ofrecer asesoría, a manera de sugerencia.
- 6) Registrar y dar seguimiento a los incidentes de seguridad, entre otros.

LAS POLÍTICAS AQUÍ EXPUESTAS SON APLICABLES A TODO EL PERSONAL QUE LABORE Y QUE SE ENCUENTRE DENTRO DE LAS INSTALACIONES DE LA SMA.

## 1. USO DE LOS BIENES INFORMÁTICOS

- 1.1. La SMA contará únicamente con un Centro de Datos (Site de cómputo) para atender las necesidades de las Direcciones Generales y Ejecutivas que la conforman, con el fin de optimizar en el uso de energía eléctrica, aire acondicionado, aprovechamiento eficiente de los servidores de cómputo, equipos de comunicaciones y servicios compartidos.
- 1.2. En el caso de los usuarios, para fomentar el ahorro de energía, los equipos no deberán mantenerse encendidos una vez terminado el horario laboral (impresoras, computadoras, monitores, UPS, bocinas, etc.).
- 1.3. Toda la información generada, guardada y registrada en el equipo de cómputo es propiedad de la SMA y es responsabilidad del resguardante el uso que se le dé, así como de su conservación.

### **RESPECTO AL SOFTWARE:**

- 1.4. Se prohíbe la instalación de Software, Programas y/o Aplicaciones que no cuenten con licencia del producto otorgada a la SMA o a sus diferentes áreas.
- 1.5. 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 fines relacionados con el desempeño de sus actividades de la SMA.
- 1.6. Es responsabilidad del resguardante, el buen uso del software instalado en su equipo.

### **RESPECTO AL HARDWARE E INFORMACIÓN**

- 1.7. 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, pérdida, maltrato o mal manejo del mismo o alguno de sus componentes.
- 1.8. La SMA representada por el personal de Informática de cada Dirección General y Ejecutiva, tendrá la facultad de administrar, controlar, auditar, desarmar, reubicar el equipo según lo considere conveniente, para su mejor uso y aprovechamiento con la debida justificación.
- 1.9. Se prohíbe almacenar cualquier tipo de información ajena al trabajo de la SMA (por ejemplo: archivos de música, imágenes, videos, etc.). En caso de que el personal autorizado localice este tipo de archivos tendrá la facultad de eliminarlos sin la necesidad de consultar al usuario.

### **RESPECTO A LA IMPRESIÓN**

- 1.10. Las impresoras son de uso común y no personal.
- 1.11. Se prohíbe la impresión total o parcial de información ajena a las actividades de la SMA.
- 1.12. Para fomentar el ahorro de papel y otros recursos, se imprimirá sólo el documento original, las copias de éste se deberán enviar a través de un archivo digital a los interesados, vía correo electrónico o, depositarlo en la intranet de la Institución.
- 1.13. Utilizar la impresión a doble cara y calidad "Economode" (Ahorro de tóner o borrador).

## 2. SOPORTE TÉCNICO

- 2.1. Únicamente el personal de Soporte Técnico de cada Dirección está autorizado para abrir, revisar, evaluar o reparar el equipo de cómputo. Por ningún motivo podrá hacerlo personal ajeno.
- 2.2. El mantenimiento Correctivo y/o Preventivo de Hardware y Software será única y exclusivamente para el equipo propiedad de la SMA y realizado por el personal de Soporte Técnico.
- 2.3. Los equipos que no son propiedad de la SMA no recibirán soporte, salvo con la autorización explícita mediante un oficio por parte del Director General o Ejecutivo, justificando la solicitud.
- 2.4. El personal de Soporte Técnico tiene la facultad de revisar y evaluar periódicamente el equipo de cómputo en el momento que lo considere necesario y siempre en presencia del usuario, así como determinar la necesidad de su desplazamiento.
- 2.5. Se establecerá un calendario de mantenimiento preventivo a los bienes informáticos de todas las áreas de la Secretaría, en este sentido se prevé realizar un mínimo de 2 revisiones al año, por el personal de Soporte Técnico.
- 2.6. 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.
- 2.7. 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 Director del Área, para tomar la decisión correspondiente.
- 2.8. Todos los servidores, computadoras personales o portátiles propiedad de la SMA contarán con un password de hardware electrónico, cuya función será inhabilitar al equipo en caso de ser abierto por personal no autorizado. Dicha inhabilitación será de carácter temporal, hasta que el personal de Soporte Técnico determine las condiciones en las que se encuentre el equipo.

- 2.9. Únicamente el personal de Soporte Técnico tendrá acceso al password de hardware. Los usuarios no deben activar ni modificar ningún password de hardware o de BIOS en los equipos.
- 2.10. 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.
- 2.11. 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.

### **3. USO DE LA RED DE CÓMPUTO**

- 3.1. Sólo el personal de Redes, 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.
- 3.2. 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).
- 3.3. Por ningún motivo se podrá conectar el equipo con “cable de parcheo” no certificado y con longitud mayor a 2.13 metros.
- 3.4. El usuario no está autorizado para instalar cables o dispositivos de red. En caso de ser requerido cualquier tipo de dispositivo de comunicaciones (NIC, MODEM, Multipuertos, Ruterador, etc) el personal de Redes hará la instalación correspondiente con previa autorización del Director General o Ejecutivo.
- 3.5. Será responsabilidad total del usuario el uso de la información en su equipo u otros recursos al compartirlos en la red. Todo recurso compartido debiera tener contraseña o determinar que usuarios tendran acceso, así como el tipo de permisos asignados,

- 3.6. En caso de requerir un mayor número de máquinas instaladas en un lugar donde sólo existe un nodo de red:
- 3.6.1. Solamente el personal de Redes está autorizado a instalar hubs, switches y access point, previo estudio de factibilidad.
  - 3.6.2. 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.
- 3.7. Está prohibida la instalación de programas ajenos a la SMA que utilicen los recursos de la red a menos que sean autorizados por el personal de Redes correspondiente.
- 3.8. 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.
- 3.9. 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.
- 3.10. En el caso de los servidores:
- 3.10.1. El uso de los servidores es estrictamente para labores propias de la SMA por lo cual los usuarios que tengan acceso a ellos no deberán utilizar sus recursos para fines personales (tales como almacenamiento de archivos, ejecución de programas, etc.).
  - 3.10.2. Solamente el Director General, Ejecutivo o de Área, por medio de un oficio podrá hacer la petición del uso de los servicios para el personal que labore en su departamento, debiendo indicar los siguientes puntos.
    - 3.10.2.1. Servidor que será accedido.
    - 3.10.2.2. Nombre del personal autorizado.
    - 3.10.2.3. Recursos a accesar y justificación del mismo.

- 3.10.2.4. Privilegios a asignar.
- 3.10.2.5. El horario predeterminado de acceso a los servidores es de lunes a viernes de 8:00 a 21:00 hrs. En caso de necesitar un acceso diferente, deberá de ser especificado.
- 3.10.2.6. Tiempo que deberá permanecer activa la cuenta (por cuestiones de seguridad el máximo tiempo permitido será de 1 año, después de los cuales el usuario deberá renovar la petición de acceso).
- 3.10.3. Los servidores llevan un registro detallado de las operaciones ejecutadas en ellos, por lo cual el usuario será responsable totalmente del buen o mal uso de dichos recursos, así como pérdidas o cambios de información como resultados de errores de operación.
- 3.10.4. A cada servidor se le realiza un respaldo en cinta todos los días sábado, el cual es resguardado por un periodo de dos semanas de operación, siendo responsabilidad del personal de Redes dicho respaldo. En caso de requerir que el respaldo se realice con una frecuencia diferente o se requiera un periodo mayor de almacenamiento, deberá solicitarse por escrito al personal de Redes correspondiente.
- 3.10.5. El personal de Redes es responsable de la integridad de los datos que los usuarios depositen en los servidores, sin embargo no será responsable por penalizaciones civiles o legales derivadas de la información resguardada.
- 3.10.6. En caso de requerir el respaldo de información específica que no esté contemplada dentro de los servidores, el usuario tendrá la obligación de notificarlo al personal de Redes a través de un oficio signado por su Director General, Ejecutivo o de Área, indicando la periodicidad de dicho respaldo, a fin de que se incluya en el compendio de información a resguardar en cinta.

#### **4. USUARIOS, CONTRASEÑAS, DATOS Y ACCESO A LA RED**

- 4.1. 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.
- 4.2. Todo usuario registrado en la red será responsable de proteger su nombre de usuario, contraseña y datos de cualquier acceso no autorizado.
- 4.3. Las cuentas de usuario registradas en la red son de carácter estándar, únicamente el personal de Redes, tiene los privilegios de modificar la configuración e instalación de aplicaciones adicionales a los equipos de cómputo.
- 4.4. Las claves de acceso serán habilitadas únicamente por el personal de Redes.
- 4.5. 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 de red y se enviará un oficio informativo al titular del área a la cual está adscrito el usuario.
- 4.6. 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.
- 4.7. Queda estrictamente prohibido el uso de un nombre de usuario distinto al propio, aun con el consentimiento del usuario original.
- 4.8. El personal de Redes definirá el número de usuarios con claves de acceso, este número podrá variar de acuerdo a solicitudes hechas por cada Dirección General o Ejecutiva y las capacidades técnicas de la red. El número máximo de usuarios dependerá de la capacidad de cómputo y direcciones IP disponibles en la red.

## 5. ADMINISTRACIÓN DE LA RED

- 5.1. La seguridad en la red estará a cargo del personal de informática de cada Dirección General o Ejecutiva, 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.
- 5.2. El personal de Redes 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 obstante lo anterior, el personal de Redes 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.
- 5.3. Corre por cuenta o riesgo del usuario cualquier información obtenida por medio del servicio de Internet.
- 5.4. 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 la cancelación de la cuenta y sólo podrá reactivarse con previa autorización del titular del área.
  - 5.4.1. Transmisión y circulación de materiales con derechos de propiedad intelectual, amenazantes u obscenos, ya sea en forma individual o masiva.
  - 5.4.2. 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.

- 5.4.3. Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricas de redes y sistemas.
  - 5.4.4. 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.
  - 5.4.5. 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.
- 5.5. Cualquier usuario de la SMA 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 la Dirección General o Ejecutiva correspondiente.
- 5.6. El personal de Redes 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.

## **6. APLICABLES A CORREO ELECTRÓNICO**

- 6.1. El usuario es responsable de respetar la Ley Federal de Derechos de Autor, no abusando de los recursos institucionales de computo, red y correo electrónico para distribuir o copiar de forma ilegal software licenciado o reproducir información sin conocimiento del autor.
- 6.2. El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión de la misma.

- 6.3. Todo personal adscrito a la SMA que sea previamente autorizado por la Dirección General, Ejecutiva o de Área, poseerá una cuenta de correo electrónico. La autorización deberá solicitarse por escrito a la Subdirección de Sistemas.
- 6.4. La información enviada o recibida en el correo electrónico será responsabilidad total del usuario de la cuenta, dejando a la SMA fuera de cualquier responsabilidad penal o civil en la cual incurriera.
- 6.5. 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 de la SMA ni de cualquier otra institución local o federal.
- 6.6. Los nombres de las cuentas de correo estarán conformadas por la letra inicial del 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 informática.
- 6.7. La persona que sea sorprendida o se descubra que hace mal uso del correo electrónico para emprender ataques a sitios externos, será sancionada de acuerdo a las normas y leyes vigentes en la materia.
- 6.8. Cualquier abuso o problema con el buen uso y manejo de las cuentas, deberá ser reportado a la Subdirección de Sistemas.
- 6.9. Está estrictamente prohibido el envío de información confidencial de la SMA a través del correo electrónico.
- 6.10. Está estrictamente prohibido el envío de correos "cadena".
- 6.11. Evitar abrir los correos en los que exista duda de su procedencia o no solicitados.
- 6.12. Queda estrictamente prohibido el envío a través del correo electrónico de información encriptada a menos que sea autorizado por la Subdirección de Sistemas.

- 6.13. En caso de que el usuario no realice una consulta de su correo en un periodo no mayor a 60 días hábiles a partir de la última fecha de consulta de su correo, su cuenta será suspendida y todos los mensajes serán eliminados en forma automática y permanente del servidor de correo.
- 6.14. La contraseña del correo caducará automáticamente cada año por lo cual se deberá de reasignar y no podrá ser el mismo durante 3 cambios.
- 6.15. Al final de cada año se deberá confirmar a la Subdirección de Sistemas 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.
- 6.16. El espacio de almacenamiento disponible en el servidor-mail es limitado, motivo por el cual se recomienda que el usuario con cuenta de correo, consulte diariamente de su correo (de esta forma el usuario descarga el correo almacenándolo a su equipo de cómputo).
- 6.17. El tamaño máximo para envío de correo será de 20 MB y el tamaño máximo para recibir correos será de 20 MB o menor de acuerdo al límite de espacio libre del servidor. (esto es vigente para todas las áreas)
- 6.18. Es deber de todo usuario de correo electrónico, la buena administración del espacio asignado a su cuenta de correo y por lo tanto, es su responsabilidad, cualquier anomalía que se presente, derivada de la mala administración del espacio asignado para su cuenta.
- 6.19. Se recomienda crear carpetas para la mejor administración del correo y mantener la bandeja de entrada con la menor cantidad de mensajes.
- 6.20. Se recomienda no mantener almacenados en el correo archivos que ocupen demasiado espacio. Si éstos son necesarios para el usuario deberá almacenarlos en el equipo de cómputo.

- 6.21. El usuario será responsable del perjuicio que pueda ocasionarle el no poder recibir o enviar más correos en caso de que se agote el espacio que tiene asignado 100 MB para usuarios de webmail y 1 GB en el equipo, a través de Outlook, Thunbderbird, Eudora o similar.
- 6.22. Es obligación de cada usuario, mantener su recipiente de elementos eliminados, continuamente vacío, ya que esto representa espacio de correo utilizado innecesariamente, debido a que implica la saturación de la capacidad de almacenamiento del servidor o el equipo de cómputo.
- 6.23. En el caso de que un usuario desee enviar o recibir un correo electrónico cuyo tamaño sea mayor a 20MB, se deberá dirigir al personal de Informática, 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.
- 6.24. El personal de Redes 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 de la SMA e inclusive podrá ir al lugar del usuario a verificar en su PC el uso que le esté dando a su correo institucional.

NOTA: El envío de mensajes masivos de correo electrónico deberá ser validado por el personal de la Subdirección de Sistemas esto con el fin de asegurar que cumplan con las reglas establecidas en los RFC-2476/RFC-4409 para el buen uso del correo electrónico. Los mensajes masivos no deberán ni podrán ser enviados desde una cuenta estándar ya que esto pone en riesgo el servicio al ser identificado como Spammer (creador de correo basura) y catalogarlo dentro de las "listas negras" empleadas para el el bloqueo del dominio completo por otros servidores de correo.

## 7. APLICABLES A INTERNET

- 7.1. Todo el personal de estructura de la SMA tendrá acceso al servicio de Internet.
- 7.2. Cuando las necesidades del servicio así lo requieran, el Director General, Ejecutivo o de Área deberá solicitar por escrito al personal de Redes la habilitación del servicio de Internet para personal eventual, de honorarios, código CF y base. Esta solicitud deberá ser enviada con copia a la oficina de la Secretaría del Medio Ambiente y a la Dirección Ejecutiva de Administración.
- 7.3. A continuación se detallan algunos programas y acciones que no deben ser usados para el buen desempeño del servicio de Internet:
  - 7.3.1. Chats, icq, bbs, irc, talk, write o cualquier programa utilizado para realizar pláticas en línea.
  - 7.3.2. Cualquier programa destinado a realizar enlaces de voz y video, sin que esto sea previamente autorizado y justificado por la Dirección General, Ejecutiva o de Área.
  - 7.3.3. Descargas de gran tamaño (mayores a 10 Mb) o uso de archivos de audio y multimedia.
  - 7.3.4. Sitios de interacción social (redes sociales), páginas personales o aquellas que no tengan relación directamente con las labores propias del usuario en el trabajo en la SMA.
  - 7.3.5. También se restringe el acceso a las páginas del tipo:
    - Dedicadas a proveer juegos en línea.
    - Con información que no sea relevante al trabajo del departamento.
    - Con material para adultos.
    - Dedicados a la difusión personal (Redes Sociales).
    - Servidores de almacenamiento masivo.

- 7.4. Para hacer mejor uso de los recursos informáticos de la SMA, serán deshabilitados los MODEMs y los acceso por ADSL (infinitem, cablemodem, etc) de las computadoras de los departamentos que ya tengan acceso al enlace de Internet, a menos que por razones operativas sean necesarios y deberán ser evaluados por el personal de Informática, previa autorización del Titular de la Dependencia.

## **8. MEJORES PRÁCTICAS EL USO DE LOS BIENES Y SERVICIOS INFORMÁTICOS**

### **MEJORES PRÁCTICAS PARA EL CORREO ELECTRÓNICO**

- No enviar mensajes que violen los derechos de los destinatarios o de terceras personas.
- Al elaborar un correo electrónico se deberá hacer uso de un lenguaje apropiado.
- Revisar el buzón de su correo con frecuencia, especialmente si está suscrito a listas de interés.
- No intercambiar grandes volúmenes de información, a través de este servicio.
- Eliminar de su buzón de correo aquellos mensajes que no necesite mantener almacenados.
- No enviar mensajes con juegos, pornografía, obscenidades, virus, etc.
- No iniciar ni continuar una cadena de mensajes.

- 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.
- 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**

- 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.
- 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.
- El usuario debe verificar periódicamente (se sugiere cada semana) su computadora personal.
- Cada usuario es responsable y debe tomar medidas para evitar el contagio de virus, troyanos, gusanos, etc., en los archivos adjuntos que envía.
- 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

Cualquier punto no establecido será evaluado y añadido a estas políticas por la Secretaría del Medio Ambiente.

“El desconocimiento total o parcial de estas políticas no es justificación para el mal uso de los bienes y servicios informáticos. Es responsabilidad del usuario tener conocimiento de ellas.”

ACEPTO.

FIRMA DEL USUARIO: \_\_\_\_\_

NOMBRE DEL USUARIO: \_\_\_\_\_

AREA DE ADSCRIPCION: \_\_\_\_\_

## GLOSARIO DE TÉRMINOS

Archivo	Conjunto de información organizada localizada en el disco duro de una PC o un servidor.
BIOS	<b>Basic Input-Output System</b> , Sistema Básico de Entrada/Salida, es un código de software instalado en la placa base, en el cual se guarda la configuración de hardware y opciones de arranque de la computadora.
Correo electrónico	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 cómputo, 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 PC, impresora, scanner, disco duro, unidad de disquete, o cualquier otro componente de la computadora.
Firewall	Protección del uso de las redes de computadoras con el que se impide o autoriza el acceso a distintas redes de cómputo, con las que se tiene comunicación.
Freeware	Software de libre distribución y uso.
Ftp (file transfer protocol)	Protocolo de transferencia de archivos por medio de una red de computadoras con tecnología TCP.
Internet	Es una red mundial de computadoras interconectadas. Internet es la red de redes. Integra redes de área local (lan's, local área network) ubicadas en escuelas, bibliotecas, oficinas, hospitales, agencias federales, institutos de investigación y otras entidades, en una única red de comunicaciones extendida por todo el mundo.
Intranet	Es una red interna en un servidor web exclusivo y seguro, que le da al personal de una institución o compañía, la posibilidad de compartir

información, sin que ésta sea expuesta a la comunidad web en general.

Password o contraseña	Es una cadena de caracteres que se usa para autenticar la identidad de un usuario. Cada contraseña está asignada a una cuenta o nombre de usuario para la autorización de acceso a la red.
Trial	Software de libre distribución que cuenta con un período de pruebas.
Usuario	Persona de cualquier área de la Secretaría del Medio Ambiente que requiere de un servicio o solución por parte del Área de Informática, para aprovechar las ventajas tecnológicas a favor de su trabajo.
World Wide Web (WWW)	Un sistema de servidores de internet que soportan especialmente documentos con formato. Los documentos son formateados en un lenguaje llamado html (hyper text markup lenguaje) que soporta ligas a otros documentos, así como gráficas y archivos de audio y video. No todos los servidores de internet son parte de la World Wide Web.