



## ÍNDICE

1. Propósito.....	2
2. Objetivo.....	2
3. Alcance.....	3
4. Políticas Generales relativas a los Servicios de Tecnologías de Información y Comunicaciones.....	3
4.1. De la asignación de equipo de cómputo.....	3
4.2. De la utilización de equipo de cómputo.....	4
4.3. Del mantenimiento preventivo y correctivo.....	8
4.4. Del uso de internet.....	9
4.5. Del correo electrónico.....	9
4.5.1. Uso del correo electrónico.....	9
4.5.2. Configuración del correo electrónico.....	11
4.5.3. Seguridad del correo electrónico.....	11
4.6. Del respaldo de información.....	13
4.7. Del servicio de telefonía.....	14
4.7.1. Asignación de extensiones telefónicas.....	14
4.8. Del acceso al sitio WEB institucional.....	14
4.8.1. Solicitud de publicación de información emitida por las áreas.....	14
4.9. De otros servicios.....	15
5. Sanciones.....	16

## **1. Propósito.**

Establecer las Políticas Generales relativas a los Servicios de Tecnologías de Información y Comunicaciones que deberán observar y aceptar los servidores públicos que hagan uso de servicios de tecnologías de información y comunicaciones, para proteger adecuadamente los activos tecnológicos y la información de la Auditoría Superior del Estado (ASE).

## **2. Objetivo.**

De conformidad con lo dispuesto en los artículos 3 y 17 apartado A fracción I, incisos q) y t) de la Ley de Fiscalización y Rendición de Cuentas para el Estado de Tamaulipas, estas políticas tienen como objetivo el uso racional de los servicios institucionales en materia de tecnologías de información y comunicaciones que se ofrecen a los usuarios de la ASE a fin de optimizar el desarrollo y cumplimiento de las funciones de la misma.

Los servicios institucionales que se prestan son:

- a) Asignación de equipo de cómputo.
- b) Mantenimiento preventivo y correctivo de equipo de cómputo.
- c) Acceso a internet y red institucional.
- d) Correo electrónico.
- e) Respaldos de información.
- f) Servicio de telefonía.
- g) Acceso al sitio WEB institucional.
- h) Otros.

### **3. Alcance.**

Las presentes políticas están dirigidas a los servidores públicos de la ASE que utilicen tecnologías de información y comunicaciones para el desarrollo de sus funciones, aplican a los equipos propios y ajenos los cuales deberán estar previamente autorizados por la Unidad de Tecnologías de la Información (UTI), conectados a las redes de la ASE.

Estas políticas son de observancia general, obligatorias para todos los usuarios y sustituyen cualquier otra emitida con anterioridad.

Su inobservancia será sancionada de acuerdo a su gravedad, de conformidad con lo establecido en el apartado de sanciones de este documento.

### **4. Políticas Generales relativas a los Servicios de Tecnologías de Información y Comunicaciones.**

#### **4.1 De la asignación de los equipos de cómputo.**

4.1.1. El equipo de cómputo será utilizado única y exclusivamente para apoyar las funciones que son propias de la ASE.

4.1.2. El equipo de cómputo será asignado a través de la UTI, atendiendo solicitudes signadas por los titulares de área.

4.1.3. Se asignará un equipo de cómputo a cada usuario de la ASE y solamente en los casos plenamente justificados y documentados se permitirá la asignación de otro equipo, bajo ninguna circunstancia se autorizará la asignación de equipo de cómputo al personal que por sus funciones, no lo requiera.

4.1.4. Toda asignación de equipo de cómputo debe estar amparada por el correspondiente Resguardo Interno de Equipo de Computo que entrega la UTI y debe ser firmado por el responsable directo de dicho equipo.

4.1.5. El firmante del Resguardo Interno de Equipo de Cómputo, es el responsable en todo momento del bien informático hasta que se cancele el mismo,

teniendo la obligación de mantener la integridad del equipo y cuidando su buen uso.

4.1.6. Los usuarios que tienen bajo su resguardo un equipo de cómputo, son responsables directos de su contenido, salvo el paquete de software básico correspondiente al perfil del equipo de cómputo respectivo.

#### **4.2. De la utilización del equipo de cómputo.**

4.2.1. Los usuarios no podrán modificar la configuración de su equipo de cómputo y en caso de requerirlo, deberá justificarlo y contar con la autorización de su superior jerárquico, realizando la solicitud correspondiente a la UTI.

4.2.2. Todos los equipos de cómputo administrados por la UTI estarán configurados para imprimir en red, salvo en los que el usuario ya cuente con una impresora local.

4.2.3. Cuando el usuario requiera instalar dispositivos (scanner, cámaras, PDA's, etc.) que no formen parte de la configuración original de los equipos, será necesario solicitar a la UTI la validación de la compatibilidad de estos, sus controladores y software específico, previa autorización de su superior jerárquico.

4.2.4. Bajo ningún argumento o justificación se autorizará la instalación de software ajeno a las funciones que le han sido encomendadas al usuario, en caso de detectarse, el personal de la UTI estará autorizado para desinstalar la aplicación, previa notificación al usuario y a su superior jerárquico.

4.2.5. Los usuarios de los equipos de cómputo que sean detectados haciendo análisis de protocolos, barridos de puertos o descubrimientos, en las redes de datos de la ASE, se les suspenderá en forma inmediata el acceso a la misma, notificando este suceso a su superior jerárquico.

4.2.6. Los usuarios no podrán usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo propiedad de la ASE, sin el

consentimiento del Auditor Superior del Estado y en caso de hacerlo, se aplicarán las disposiciones legales vigentes para la protección y derechos de autor.

4.2.7. Los desarrollos de software internos estarán sujetos a las normas específicas para este entorno, no debiendo realizarse sin la autorización del Auditor Superior del Estado y el conocimiento de la UTI.

4.2.8. Cuando un usuario de equipo de cómputo desee instalar software cuya licencia de uso original sea adquirida por él, deberá solicitar la autorización a la UTI para su instalación, justificando plenamente el uso del software y realizando los trámites necesarios para la donación del mismo en favor de la ASE, incluyendo la factura original. El software debe ser previamente certificado por la UTI antes de su instalación.

4.2.9. Para los casos de migración, sustitución o respaldo de información en CD's, USB o cambio de equipo de cómputo se deberá observar lo siguiente:

4.2.9.1. Todos los archivos de trabajo de las computadoras a sustituir deberán encontrarse ubicados o respaldados en la carpeta llamada "mis documentos".

4.2.9.2. Las macros de las diferentes aplicaciones de Microsoft Office (Word, Excel u otros) se consideran como archivos personales y será responsabilidad del usuario su actualización o reformulación para que operen en el nuevo equipo de cómputo personal bajo la versión de Microsoft Office autorizada por la ASE.

4.2.9.3. Los archivos con extensiones MP3, AVI, WAV y en general cualquiera relacionado con música, video o juegos, no serán migrados al nuevo equipo de cómputo. El personal de la UTI está autorizado para borrar este tipo de archivos, ya que comprometen el proceso de migración o sustitución del equipo.

- 4.2.9.4. Los dispositivos de almacenamiento necesarios para respaldar la información de archivos guardada en la carpeta de “mis documentos” serán proporcionados por el área respectiva que corresponda al usuario.
- 4.2.9.5. Queda estrictamente prohibido la utilización de dispositivos de almacenamiento de información personal, tales como USB, CD, DVD, discos duros, memorias de teléfonos celulares, cámaras fotográficas, etc. para respaldar archivos que contengan información propia de las funciones del usuario.
- 4.2.10. Toda unidad de almacenamiento externo (memorias USB, CD, DVD, Disco Duro, etc.) deberá ser revisada con el software antivirus cuando se conecte a un equipo, para asegurar que no esté contaminada con algún virus informático.
- 4.2.11. La clave (user\_name) asignada al usuario así como la contraseña (password) para el acceso a los servicios proporcionados por la UTI es personal e intransferible, por lo que cada usuario es responsable de su uso y confidencialidad.
- 4.2.12. Los usuarios que cuenten con regulador, deben conectar únicamente el CPU, el monitor y en su caso, la impresora, está prohibido conectar otros dispositivos.
- 4.2.13. En caso de sacar de las instalaciones de la ASE, equipo de cómputo, componentes o periféricos del mismo sin autorización, previa investigación él o los responsables serán sancionados de acuerdo con la normatividad y legislación vigente y en su caso, la ASE se reserva el derecho de emprender acciones legales ante las autoridades correspondientes.
- Igualmente queda prohibido el ingreso a las instalaciones de la ASE, equipo de cómputo, así como de cualquier unidad de almacenamiento, tales como

disco duro externo, CD, DVD, USB, cámaras fotográficas, grabadoras, etc. que no sean propiedad de la misma. Solo en los casos en que se justifique la necesidad de su ingreso, este deberá documentarse plenamente y ser supervisado por la UTI, con la autorización del titular del área donde se utilizará dicho equipo.

- 4.2.14. En caso de extravío, robo o siniestro de un equipo de cómputo, componentes o periféricos del mismo, el resguardante tiene la obligación de inmediatamente dar aviso a su superior jerárquico por escrito.
- 4.2.15. Solo está permitido el uso de papel tapiz (wall paper) o fondo de pantalla institucional que la UTI instalará en el equipo de cómputo respectivo. El personal de la UTI está autorizado para borrar cualquier otro papel detectado.
- 4.2.16. Al retirarse de su lugar de trabajo, salir a comer o terminar la jornada laboral, el usuario deberá salir de todas las aplicaciones con las que haya estado trabajando y apagar el equipo, salvo que el administrador de la red le indique que lo deje encendido para transmitir o actualizar algún software, para lo cual se tiene que salir forzosamente de las aplicaciones y apagar solamente el monitor.
- 4.2.17. Cualquier equipo de cómputo que se encuentre fuera de la administración de la UTI, no contará con los servicios que se detallan en el presente documento.
- 4.2.18. En caso de terminación de la relación laboral del usuario, el superior jerárquico deberá de comunicarlo a la UTI con la finalidad de revisar los bienes informáticos asignados, si todo está en orden, la UTI procederá a cancelar los resguardos correspondientes, en caso contrario, solicitará la reparación de los daños detectados.



- 4.2.19. Queda prohibido colocar sobre o cerca de los equipos de cómputo, componentes y sus periféricos, alimentos o bebidas, así como ingerirlos mientras trabajan o permanecen frente de éstos. En caso de registrarse algún siniestro por los motivos antes mencionados y ocasione un daño al bien informático, el usuario responsable del mismo deberá responder por el daño causado. Asimismo, queda prohibido colocar bolsas, cartapacios o cualquier objeto sobre el CPU.
- 4.2.20. Los usuarios deben cuidar que los conectores y cables de los equipos de cómputo bajo su resguardo, no sufran daño y se encuentren colocados de tal manera que eviten su deterioro o causen algún accidente.
- 4.2.21. El equipo de cómputo asignado al personal en calidad de préstamo temporal, ya sea, para utilizarlo en cursos de capacitación, por mantenimiento a su equipo, o en su caso, para realizar comisiones asignadas fuera del edificio de la ASE, entre otros, estarán sujetos a las mismas condiciones de uso y cuidado establecidas en el presente documento, mientras se encuentren bajo el resguardo del servidor público.

### **4.3. Del mantenimiento preventivo y correctivo.**

- 4.3.1. Este servicio preventivo se sujetará al Programa de Mantenimiento Preventivo a Equipos de Cómputo, Telefonía y Comunicaciones, en el cual se establecerá el calendario respectivo de la UTI, contemplando dos mantenimientos por año.
- 4.3.2. El usuario deberá brindar las facilidades al personal de la UTI para realizar dicha labor, en el entendido de que si dicho mantenimiento no es posible por su carga de trabajo, se podrá reprogramar de común acuerdo.
- 4.3.3. Cuando se requiera un servicio correctivo se solicitará a través del formato establecido, detallando específicamente la falla que se presenta en el equipo, sus componentes o periféricos o bien en el software instalado.



#### **4.4. Del uso de internet.**

- 4.4.1. El servicio de internet se prestará previa autorización por escrito del superior jerárquico del usuario, donde se justifique el uso y el dominio de las páginas web a que tendrá acceso.
- 4.4.2. En dicha autorización deberá señalarse si el acceso será por un periodo determinado o permanente.
- 4.4.3. Sólo se deberá utilizar el internet para actividades directamente relacionadas con el trabajo que se desempeña.
- 4.4.4. Queda estrictamente prohibido descargar archivos de entretenimiento (música, películas, juegos, etc.) aun comprándolas en forma legal.
- 4.4.5. El usuario no deberá ingresar a sitios en internet que sean inapropiados para las funciones de la ASE.
- 4.4.6. El usuario no debe descargar archivos ejecutables de internet a menos que sean parte de las funciones que le fueron asignadas.

#### **4.5. Del correo electrónico.**

##### **4.5.1. Uso del correo electrónico.**

- 4.5.1.1. Este servicio estará disponible para todo el personal de la ASE que tenga asignado un equipo de cómputo, será la UTI quien generará la clave de usuario conforme a la siguiente estructura: nombre.apellido@asetamaulipas.gob.mx, que será intransferible. Las claves de usuarios no podrán ser personalizadas.
- 4.5.1.2. El uso de este servicio será destinado únicamente para apoyar las funciones que son propias de la ASE y particularmente las encomendadas por el titular del área a la que pertenezca el usuario.



- 4.5.1.3. Está prohibido el envío de mensajes cuyo contenido sea nocivo o que atente contra las buenas costumbres, la moral y las leyes de derecho de autor, “cadenas” sin importar que tan plausible sea la causa, pornografía, obscenidades, correos discriminatorios de tipo racial, de género, social, culto, juegos, chistes, videos, audio, aquellos de proselitismo religioso, político o comercial, así como cualquier otro que no tenga relación con las actividades laborales encomendadas al usuario.
- 4.5.1.4. Está prohibido utilizar este servicio para insultar, agredir, intimidar, acosar o interferir en las funciones de los demás usuarios del servicio.
- 4.5.1.5. Queda prohibido realizar cambios en la configuración del software Outlook, referente a las reglas establecidas para el envío y recepción de correo electrónico.
- 4.5.1.6. La confidencialidad de la información remitida a través de correo electrónico es responsabilidad exclusiva de los usuarios.
- 4.5.1.7. Queda prohibido utilizar una identidad diferente a la propia (de otro usuario o ficticia) o actuar de forma anónima para enviar mensajes por este medio.

Es importante aclarar que el servicio de correo electrónico, está sujeto a verificaciones para salvaguardar la integridad del sistema, en las cuales no interviene personal directamente (revisión del contenido); estas se realizan como procesos de verificación automatizados con la finalidad de detener el correo no deseado (SPAM) y correo contaminado con virus informáticos. En caso de identificar que un correo válido no llegue a su destinatario, se deberá reportar a la UTI.

#### **4.5.2. Configuración del correo electrónico.**

- 4.5.2.1. La información del buzón de correo estará almacenada en carpetas personales localmente en el equipo de cómputo del usuario, se recomienda su depuración cuando exceda de 500 correos ya sea en la bandeja de entrada o salida para evitar saturación en el disco duro.
- 4.5.2.2. El tamaño máximo de un mensaje tanto para recepción como para envío será de 10 megabytes, lo anterior de conformidad con la capacidad de la infraestructura con que se cuenta actualmente en la UTI, por lo que todos los mensajes de correo que excedan de ese límite no se garantiza que puedan ser recibidos o enviados.
- 4.5.2.3. El número máximo de destinatarios simultáneos para un correo será de 20, considerando los rubros: Para, CC y CCO.

#### **4.5.3. Seguridad del correo electrónico**

- 4.5.3.1. En principio, toda la información que se envía por correo electrónico viaja “en claro” por internet, por lo que es susceptible de ser leída y modificada por “hackers”.
- 4.5.3.2. La información clasificada deberá cumplir con las medidas de seguridad definidas y aprobadas por la UTI.
- 4.5.3.3. La información que sólo deba ser accesible por personas autorizadas debe ser encriptada pudiendo tomarse medidas adicionales cuando el nivel de confidencialidad de la información así lo exija.
- 4.5.3.4. Sólo deberán utilizarse aquellas herramientas que proporcionen niveles de seguridad adicionales (como encriptadores, PGP o similares) que estén aprobadas por la UTI. Para la utilización de



nuevas herramientas de este tipo deberán ponerse en contacto con dicha área para obtener su autorización.

- 4.5.3.5. El usuario debe revisar con el antivirus todo el correo recibido aunque no esté visiblemente acompañado de archivos adjuntos, aun siendo un correo interno y de una fuente viable o confiable.
- 4.5.3.6. El usuario debe informar de inmediato a la UTI si detecta un virus en algún correo electrónico.
- 4.5.3.7. El usuario debe incrementar su cuidado al recibir un correo electrónico de fuentes desconocidas y más aún, si no se está esperando alguna información.
- 4.5.3.8. Queda prohibido el envío y respuesta a mensajes de tipo comercial cuyo contenido no fue solicitado por los destinatarios (SPAM), asimismo, aquellos mensajes cuyas características pudieran causar problemas de bloqueo en los servidores de red.
- 4.5.3.9. Ante la sospecha de que su cuenta esté siendo utilizada indebidamente, deberá cambiar de inmediato la contraseña de acceso a su equipo y notificarlo a la UTI.
- 4.5.3.10. Se debe evitar abrir archivos de datos adjuntos que provengan de un origen desconocido, ya que pueden contener "virus", los cuales pueden dañar la computadora o la información.
- 4.5.3.11. En caso de que alguien tenga necesidades de transmisión de mensajes que estén fuera de estas políticas, será necesario detallar sus requerimientos, obtener el visto bueno del titular del área y enviar su petición a la UTI para definir la mejor manera de atender su requerimiento.



4.5.3.12. Siempre que se reciban archivos vinculados a mensajes de correo deberán tomarse las medidas oportunas con el fin de evitar virus o cualquier otra amenaza.

4.5.3.13. En especial, se extremarán las precauciones cuando el correo sea de origen desconocido o no verificado, antes de abrirlos, se deberán aplicar los antivirus institucionales en todo caso.

4.5.3.14. Para cumplir con este apartado la UTI podrá proporcionar asesoría y capacitación al personal que así lo requiera.

#### **4.6. Respaldos de información.**

4.6.1. La UTI respaldará de manera automática y periódica a través del servidor de la ASE aquella información o base de datos que generen los sistemas institucionales.

4.6.2. Será responsabilidad del titular del área, solicitar a la UTI por escrito, el respaldo de aquella información que se genere en aplicaciones de Excel, Word, Power Point, etc. que considere necesaria para el desempeño de las funciones y responsabilidades de los usuarios a su cargo.

4.6.3. Queda a criterio del titular del área de cada usuario, determinar no solo la información a respaldar sino también la identificación, frecuencia, horarios, número de versiones, etc. así como métodos de compactación y/o cifrado de la información y de ser conveniente, de los respaldos a obtener.

4.6.4. Así mismo, será responsabilidad del usuario verificar regularmente que, a partir de los respaldos pueda restaurar su información apropiadamente.

4.6.5. El uso y aprovechamiento del dispositivo de almacenamiento para el respaldo de información, será destinado únicamente para apoyar las funciones que son propias de la ASE.

#### **4.7. Servicio de telefonía.**

##### **4.7.1. Asignación de extensiones telefónicas.**

4.7.1.1. La asignación de extensiones telefónicas estará sujeta a la solicitud por escrito del titular del área donde se requiera.

4.7.1.2. En dicha solicitud deberá señalarse el tipo de servicio que se requiere, si es solo para comunicación interna o tendrá acceso a llamadas locales, de larga distancia y/o celulares.

4.7.1.3. Cada usuario será responsable de su clave de acceso para el uso del servicio de telefonía.

#### **4.8. Del acceso al sitio WEB institucional.**

##### **4.8.1 Solicitud de publicación de información emitida por las áreas.**

La publicación de información institucional, convocatorias, programas, información financiera, cursos, eventos, temas de interés y demás actividades inherentes a las funciones de la ASE estará sujeta a lo siguiente:

4.8.1.1. El sitio WEB institucional de la ASE posibilita la publicación y moderación de la información, la UTI asume la responsabilidad de la administración del sitio, dicha actividad se extiende al registro que fuese necesario para acceder a determinados servicios o contenidos.

4.8.1.2. El titular de la UTI designará al responsable de publicar información emitida por las distintas áreas de la ASE.

4.8.1.3. El responsable de publicar información en el sitio web institucional, contará con una contraseña proporcionada por el titular de la UTI, comprometiéndose a hacer un uso diligente y confidencial de la misma.



- 4.8.1.4. La asignación del servicio de un espacio en el sitio web institucional deberá solicitarse por escrito a la UTI por el titular del área respectiva con la autorización del Auditor Superior del Estado.
- 4.8.1.5. Una vez autorizado el espacio, el titular del área y el responsable de crear y subir la información, deberán de firmar de conformidad un ejemplar de la información publicada en el sitio WEB institucional, con el fin de comprobar si fuera necesario, que la información publicada es copia fiel y exacta del archivo entregado para dicho fin.
- 4.8.1.6. Si la información es de relevancia para la ciudadanía y se desea que se muestre en la página principal para que sea de fácil acceso, el responsable de crear la información deberá de:
- a) Solicitar por escrito dicha petición, en la cual, deberá especificar en qué parte de la página principal del sitio WEB desea que se muestre.
  - b) Previo a la publicación, la información será evaluada y autorizada por el Auditor Superior del Estado, tomando en cuenta la relevancia con respecto a las que se publiquen en ese momento y que no interfiera con ninguna de las mismas.
- 4.8.1.7. La UTI dará respuesta a las solicitudes de publicaciones manteniendo una coordinación con las áreas respectivas para cualquier inconveniente o retraso que pueda existir.
- 4.8.1.8. Sera responsabilidad de cada una de las áreas respectivas la actualización de la información publicada.

#### **4.9. De otros servicios.**

Cualquier otro servicio que se requiera en materia de tecnologías de la información y comunicaciones que no se encuentre detallado en el presente documento, la UTI dará respuesta previa evaluación de la solicitud respectiva, sus costos de



implementación y de las ventajas que ofrezca para un mejor desempeño de las funciones encomendadas.

## **5. Sanciones.**

El desconocimiento de las políticas para la utilización del servicio de tecnologías de información y comunicaciones, no exime al usuario de la responsabilidad administrativa por el mal uso del mismo, ni de la aplicación de las sanciones que correspondan a las faltas que en su momento se lleguen a determinar.

El incumplimiento a las anteriores disposiciones y de acuerdo a la gravedad del caso, se procederá a instaurar el procedimiento administrativo que establece la Ley de Responsabilidades de los Servidores Públicos del Estado de Tamaulipas y conforme a la misma, se podrán imponer sanciones que podrán ser:

1. Apercibimiento público o privado.
2. Amonestación pública o privada.
3. Suspensión de labores de tres días a tres meses.
4. Destitución.
5. Inhabilitación temporal.
6. Sanción económica en caso de daños ocasionados.

Las presentes políticas entrarán en vigor el día de su suscripción y se autoriza su publicación en el visualizador del Sistema de Gestión de Calidad de esta Auditoría Superior del Estado.

Cd. Victoria Tamaulipas; a 7 de noviembre de 2013.

**ATENTAMENTE  
“SUFRAGIO EFECTIVO. NO REELECCIÓN”  
AUDITOR SUPERIOR DEL ESTADO**

**C.P.C. MIGUEL VÍCTOR SALMÁN ALVAREZ, M.A.**