ÍNDICE

I. OBJETIVO

Establecer la normatividad de aplicación general en el uso correcto de los recursos, bienes y servicios informáticos y de tecnologías de la información y las responsabilidades que debe de seguir los usuarios de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Yucatán.

II. ALCANCE

Aplica al personal de base, confianza, prestadores de servicios profesionales, servicio social y a todo el personal que haga uso de recursos, bienes o servicios informáticos y de tecnologías de la información de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Yucatán.

III. FUNDAMENTO LEGAL

Ámbito Federal

Artículo 113, Constitución Política de los Estados Unidos Mexicanos

Artículos 1, y 3, fracciones VIII y XIII de la Ley General del Sistema Nacional Anticorrupción.

Ámbito Estatal

Artículo 101 Bis de la Constitución Política del Estado de Yucatán.

Artículos 1, 30, 32, fracción III y 36 de la Ley del Sistema Estatal Anticorrupción de Yucatán.

Artículo 7 de la Ley de Responsabilidades Administrativas del Estado de Yucatán.

Artículos 4, fracción II, 26, 27 fracciones I, III, IV y VII, 32 fracciones II, XIV, XV y XVI del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción.

Artículos 8, primer párrafo y 51 primer y cuarto párrafo del Código de la Administración Pública de Yucatán.

Artículos 5, 22, fracción III y 26, fracción VI, incisos a, e y f de los Lineamientos para la implementación del Sistema de Control Interno Institucional en las dependencias y entidades de la Administración Pública Estatal.

IV. DEFINICIONES

Carpetas Compartidas: Espacio de almacenamiento de archivos de trabajo centralizado que pueden ser accedidos por múltiples usuarios de forma segura.

DTI: Departamento de Tecnologías de la Información.

RVDV: Red de Voz, Datos y Video.

Servidor de Archivos: Es un tipo de servidor que almacena y distribuye diferentes tipos de archivos informáticos entre los clientes de una red de computadoras. Su función es permitir el acceso remoto de otros modos a los archivos que almacena o sobre los que tiene acceso.

Servidor de Usuarios: Este servidor es propio de la Secretaría Ejecutiva y está destinado para el trabajo del personal adscrito.

Direcciones: Dirección de Administración y Finanzas, Dirección Jurídica, Dirección de Análisis y Políticas Públicas, Dirección de Vinculación Interinstitucional.

Secretario Técnico: Secretario Técnico de la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Yucatán.

SESEAY: Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Yucatán

V. POLÍTICAS

Políticas Generales:

1. Las presentes políticas son aprobadas por el Titular de la SESEAY en cumplimiento al Código de la Administración Pública de Yucatán.
2. Las presentes políticas son aplicables para todo el personal perteneciente a la SESEAY
3. Las situaciones no previstas dentro de las presentes políticas serán resueltas por el Director de Administración y Finanzas.
4. Cualquier modificación a las presentes políticas, deberá ser aprobada por el Director de Administración y Finanzas.
5. Las presentes políticas entran en vigor al día siguiente de su aprobación y será publicado en la página de la SEAY y dado a conocer a todo el personal de la SESEAY.

VI. DESCRIPCIÓN DEL PROCEDIMIENTO

Políticas Específicas:

1. Del Servicio de red y carpetas compartidas.

1.1. El servicio de red es una herramienta institucional que provee la SESEAY, mediante la cual los usuarios pueden compartir recursos de forma local y remota, estos servicios son utilizados para generar y compartir información entre las diferentes áreas, así como utilizar impresoras, multifuncionales, controles de acceso y cualquier otro equipo de comunicación y de ofimática.

1.2. Para acceder al servicio de red, carpetas compartidas y correo electrónico institucional se deberá contar con un usuario y contraseña valido y activo.

1.3. Para la solicitud de creación de cuentas de usuario de red y correo electrónico, las Direcciones deberán enviar por correo electrónico la solicitud correspondiente al Director de Administración y Finanzas, con la información necesaria para su creación: nombre completo, puesto, área de adscripción y tipo de contratación.

1.4. No se elaborarán cuentas de usuario de red y correo electrónico, si la persona servidora pública aún no está dado de alta en recursos humanos, si es prestador de servicios profesionales sin haber suscrito contrato de prestación de servicios o bien si no se cuenta con la autorización del Director de Administración y Finanzas en casos excepcionales.

2. Carpetas compartidas en red.

2.1. Las carpetas compartidas en red se clasifican de acuerdo a su uso:

Carpetas Personales: Las carpetas personales, tienen como objetivo el almacenamiento de archivos de trabajo e información reservada, confidencial así como archivos, documentos y papeles de trabajo, revisión o actividades especiales, teniendo acceso únicamente los usuarios dueños de estas, así como su superior, por lo que es responsabilidad de cada usuario su constante actualización y depuración por lo cual tiene el compromiso de mantener este recurso, cumpliendo con la tarea de depurar cada 3 meses.

Carpetas de Comunes: Las carpetas de Comunes tienen como objetivo compartir la información de uso común dentro de la SESEAY y contendrá información específica de acuerdo a su clasificación para llevar un control integral de la misma. Dichas carpetas deberán tener una estructura definida para almacenar toda la información referente a la SESEAY.

2.2. Privacidad.

2.2.1. Todos lo archivos almacenados en los equipos de computo y en las carpetas compartidas en la red, son propiedad de la SESEAY y no de los usuarios. Por lo tanto, solo deben contener archivos con información relacionada con la actividad propia de la SESEAY.

2.2.2. Para otorgar permisos de acceso a las carpetas compartidas en red a usuarios que no pertenezcan a esa Dirección , se deberá realizar una solicitud por correo electrónico institucional al "DTI", con copia a director de área, solicitando el acceso a la información, de igual forma para eliminar los permisos el solicitante debe de enviar un correo electrónico institucional solicitando la eliminación del permiso concedido.

2.2.3. Los usuarios deben estar conscientes que en caso de baja de la institución voluntaria o involuntaria deberá entregar toda información contenida en sus equipos.

2.2.4. Para respaldos o resguardos de información que se pidan al "DTI", solo se ejecutará sobre información relacionada a sus labores en la institución, por lo

tanto, queda excluida toda información que no sea de carácter de trabajo o institucional.

2.2.5. Todo usuario de las carpetas compartidas y servicios de red deben asumir que los archivos, así como cada carpeta compartida de la red son privados, éstos no deberán ser observados, copiados, alterados ni utilizar aquellos que no sean de su autoría, relativos directamente a sus funciones o bajo consentimiento del propietario o de las Direcciones.

2.2.6. Los archivos almacenados en las carpetas compartidas y servicios de red pueden convertirse en evidencia para procedimientos legales, por lo que todo usuario autoriza a la "SESEAY" la revisión de cualquiera de ellos. Todos los archivos deben realizarse con el conocimiento de que pueden ser revisados y auditados.

2.2.7. No se debe permitir el acceso a la infraestructura de la red a equipos de cómputo, personas u organizaciones ajenas a la "SESEAY" sin autorización expresa por parte de la Dirección de Administración, la solicitud debe ser envia al "DTI" con copia al Director de Administración y Finanzas, indicando el motivo y tiempo de acceso.

2.3. Contenido de las carpetas y los archivos.

2.3.1. Los usuarios deben incorporarse a los estándares normales de comunicación, el servidor de archivos deberá ser usado únicamente para compartir información laboral.

2.3.2. El material explícitamente sexual, queda censurado y prohibido, por lo que a quien se encuentre este tipo de información serán sujetos a una acción disciplinaria, la cual se establece en la sección correspondiente.

2.3.3. No deberán existir en las carpetas compartidas archivos que no sean de carácter institucional, así como archivos y carpetas que contengan música, series televisivas, películas, juegos, programas o archivos ejecutables que no

sean de carácter institucional ya que serán borrados y para el caso de respaldos, éstos no serán considerados ya que no es información para uso laboral. Salvo por las personas autorizadas por la "Direcciones" correspondiente, justificando por medio de correo electrónico cuyas funciones laborales impliquen el uso de dichos archivos.

2.4. Capacidad y retención de archivos.

2.4.1. Las carpetas compartidas del Servidor de Archivos son responsabilidad de cada usuario por lo cual tiene el compromiso de mantener este recurso, cumpliendo con la tarea de depurar cada 3 meses, o en el caso de información de auditorías al concluir el periodo correspondiente de uso. Así también el "DTI" tiene la responsabilidad de mantener vigente dicha carpeta.

2.4.2. Las carpetas compartidas de red de las Direcciones están diseñadas para almacenar archivos de uso particular del personal del área, teniendo acceso único y exclusivo por él mismo; por lo que es responsabilidad de cada usuario mantener depurada esta carpeta para darle el uso adecuado.

2.5. Nomenclatura y nombres de Archivos y Carpetas.

2.5.1. Se prohíbe utilizar caracteres especiales (" ",.% (){}[ ]@¿i-4-/!:;&#') para nombrar archivos o carpetas ya que genera problemas cuando estos requieren ser respaldados, transferidos o incluso la probabilidad de NO poder abrir archivos que se encuentren bajo este esquema.

2.5.2. Los usuarios no deben de colocar nombres demasiado largos a los archivos creados ya que esto ocasiona inconvenientes con las tareas de respaldo.

2.5.3. Los usuarios no deben realizar más de 6 estructuras de archivos dentro de un mismo directorio debido a que esta clasificación no permite la realización de respaldo.

3. Del respaldo de Información.

3.1. De la información en equipos de los usuarios.

3.1.1. Por seguridad los archivos con información sensitiva y critica deberán ser respaldados y/o actualizados en las carpetas compartidas correspondientes, por lo que es responsabilidad del usuario realizar esta tarea antes de finalizar su jornada de trabajo y/o en el momento que lo considere necesario, a fin de asegurar que la información generada por las diferentes unidades administrativas, no se pierda y esté disponible en caso de desastre, o cualquier contingencia, como daño en los discos duros, o eliminación accidental de la Información o bien un caso de desastre fisico de los equipos personales.

3.1.2. El "DTI" no se hace responsable por la información que no se encuentre en el Servidor de Archivos al momento de realizar las copias de seguridad programadas.

3.1.3. Cuando ocurra una contingencia, es esencial que el usuario conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en caso de ser posible al "DTI" en el menor tiempo posible el proceso perdido.

3.1.4. En caso de que por el volumen de información se requiera algún respaldo en CD o DVD, este servicio deberá solicitarse por correo electrónico al "DTI" con copia o autorización del Director del área correspondiente.

3.1.5. Al realizar el mantenimiento preventivo o correctivo a los equipos de cómputo, es responsabilidad del usuario mantener toda la información de trabajo ordenada e informar al "DTI" para su correcto respaldo.

3.1.6. Es responsabilidad del "DTI" hacer un respaldo de la cuenta de correo electrónico al realizar el mantenimiento preventivo correspondiente, así también una vez que se requiera suspender la cuenta o se encuentre en proceso de baja al usuario, esto siempre y cuando se cuente con los are ST o OST. Para la restauración de los datos se debe solicitar directame e al Director de Administración y Finanzas con la justificación correspondiente indicando

la información qué se requiere. La solicitud debe hacerse mediante via correo electrónico.

4. De las copias de Seguridad y Restauración.

4.1. Copia de seguridad de la información: "DTI" deberá determinar la calendarización de los eventos y periodicidad de copias de seguridad y el tiempo que se conservaran disponibles dichos respaldos.

4.2. En caso de requerir realizar u obtener una Copia de seguridad de la información y de igual manera para solicitar la Restauración de archivos o carpetas que se encuentren en las copias de seguridad, los usuarios deberán proporcionar el nombre del archivo o carpeta, la ruta donde se encontraba, así como la última fecha que fue respaldado, esto mediante correo electrónico con copia al Director del área dirigido al Director de Administración y Finanzas.

4.3. Todas las copias de seguridad deberán realizarse en medios externos o independientes de donde se encuentra la información, por parte del personal del "DTI".

5. Del uso de internet y correo electrónico.

5.1. Correo electrónico.

5.1.1. La SESEAY, es la propietaria exclusiva de todas las cuentas de correo electrónico, así como de la información enviada, recibida. almacenada o creada bajo su dominio y es otorgada como herramienta de trabajo institucional.

5.1.2. La información que cree, almacene, envíe o reciba el usuario en y desde su cuenta de correo electrónico podrá ser auditada por el "DTI" a petición de la "SESEAY".

5.1.3. Es responsabilidad del usuario, el uso de la cuenta asignada.

5.1.4. El uso de la cuenta se sujeta a las siguientes restricciones:

- No iniciar y contestar "cadenas de correo".
- No contestar correos con dominio sospechoso.
- No abrir archivos adjuntos de correos sospechosos.
- No podrá usarse con fines lucrativos ni con fines comerciales no institucionales.

5.1.5. Se asignará solamente una cuenta por usuario.

5.1.6. La cuenta de correo electrónico es personal e intransferible.

5.1.7. No está permitido el uso de papel tapiz o fondo (wallpaper o background) en el cuerpo del correo electrónica.

5.1.8. El Titular, Directores y la Jefatura de Comunicación y Vinculación son los únicos autorizados a enviar comunicados generales a todos los usuarios de la SESEAY. En caso de requerir enviar un comunicado toda solicitud deberá ser dirigida a la Jefatura de Comunicación y Vinculación y deberán acatarse sus recomendaciones y dicha jefatura determinará y en su caso realizará el comunicado correspondiente.

5.1.9. Se dará de baja una cuenta de correo electrónico cuando el servidor público deje de prestar sus servicios o por instrucción directa de las

Direcciones mediante correo electrónico dirigido al Director de Administración y Finanzas.

5.1.10. El 'nombre de usuario" de la cuenta dada de baja quedará reservado e inhabilitada durante el tiempo que el Director del área lo considere, a partir de la fecha de baja.

5.1.11. No se deberán "responder a todos" los comunicadas generales ni los enviados a grupos.

5.1.12. En caso de tener problemas con la recepción de correos de cierto dominio, deberá de reportarse al "DTI", para agregar el dominio a las listas seguras de envío y recepción.

5.1.13. Cada vez que su buzón llegue a su máxima capacidad el sistema administrador de correo le enviará un mensaje de advertencia de buzón lleno para que el usuario haga la debida depuración y eliminación de correos, si el usuario hace caso omiso del mensaje su buzón será bloqueado y no podrá recibir más correos únicamente liberando espacio del mismo.

5.2. Uso de Internet.

5.2.1. Toda actividad realizada con el servicio de navegación en Internet es de única responsabilidad del usuario, por tal motivo es responsabilidad del usuario proteger la identidad de su cuenta y su clave de acceso: login y password.

5.2.2. El servicio de navegación en Internet a través de la "RVDV" es para uso exclusivo de actividades institucionales. Por tal motivo el "DTI" establece permisos de navegación de acuerdo al puesto de los usuarios.

5.2.3. Se prohíbe el acceso a los sitios o páginas web que contengan materiales amanazadores, pornográficos, racistas, sexistas o cualquier otro que degrade calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

5.2.4. Los permisos de navegación por Internet únicamente se asignarán a cuentas de usuario institucionales personales. No serán asignados permisos de navegación por Internet a cuentas de usuario anónimas (por ejemplo: recepción).

5.2.5. Es responsabilidad del usuario la descarga de cualquier archivo por este servicio y las consecuencias que de ello resulte.

5.2.6. Cualquier deficiencia o funcionamiento anómalo del servicio de navegación en Internet que observe el usuario deberá comunicarlo a su responsable del "DTI".

6. Del Uso de equipos de cómputo de la institución.

6.1. El usuario tiene la obligación de hacer uso adecuado de los equipos de cómputo de la institución: cualquier daño en el hardware (equipo físico) o software (sistema operativo o programas) de los equipos deberá ser notificado al "DTI", para realizar el diagnóstico y hacer la reparación o uso de la garantía con el proveedor.

6.2. Todo usuario está obligado a cuidar y hacerse responsable del equipo que recibe como herramienta de trabajo de acuerdo al resguardo que firma obligándose a

cuidar de la conservación del objeto descrito y será responsable del valor de este, así mismo se obliga a dar aviso a su Dirección correspondiente por escrito en un término no mayor a tres días cualquier afectación o desperfecto que pueda recibir el bien recibido en resguardo.

6.3. Si en el dictamen realizado por el "DTI" se deduce que el daño es por mal uso, negligencia o descuido, el usuario deberá de pagar las reparaciones o la compra del bien. El desconocimiento del uso correcto tampoco será causa para justificar una descompostura.

6.4. Es responsabilidad del usuario de la SESEAY, cuidar y mantener los equipos de cómputo bajo su resguardo aún fuera de horario de trabajo, y cuando se utilizan para fines de educación u otro objetivo no laboral.

6.5. Está prohibido fumar, tomar bebidas o consumir alimentos cuando esté haciendo uso de cualquier bien informático de la institución computadoras, impresoras, proyectores, teléfonos, etc.) ya que en caso de un accidente al hacer uso el equipo mientras realiza alguna de estas actividades se le imputará fallas detectadas en diagnósticos posteriores a quien tenga la responsabilidad del resguardo.

6.6. Se le prohíbe al usuario tener equipo de cómputo de la SESEAY cerca de campos magnéticos, así como conectarlo a fuentes de energía inestables.

6.7. Está estrictamente prohibido el intercambio de computadoras, accesorios o aditamentos entre usuarios sin previo aviso a la Dirección correspondiente, ya que sin una previa

revisión de los mismos por "DTI" antes de un intercambio de equipos entre personal se le imputará fallas detectadas en diagnósticos posteriores a quien tenga la responsabilidad del resguardo.

6.8. Todos los equipos se les programa una configuración estándar de acuerdo al perfil de los usuarios y las aplicaciones que estos ocupen, por lo que queda prohibido modificar estas configuraciones sin previa autorización de la Dirección correspondiente, ya que puede ocasionar fallas en la funcionalidad del sistema operativo o de sus aplicaciones, si esto ocurre caerá en una incidencia siendo considerada como causa de una sanción.

6.9. En caso de los equipos portátiles tipo laptop, notebook o macbook, es una buena práctica el mantener los equipos conectados a la corriente de luz. El usuario debe tener la seguridad de no hacerles movimientos bruscos o golpes, así como evitar dejar su equipo encendida en el portafolio, mochila, cama, piso o sobre una manta, ya que el ventilador que enfría el procesador está localizado en la parte inferior del equipo y este puede bloquearse o recolectar polvo, pelusa que estorbarán a su buen funcionamiento y causará que el procesador se sobrecaliente y este se dañe.

6.10. Para evitar el daño de los adaptadores de corriente se recomienda evitar golpearlos, desconectarlos con cuidado, no tirar del cable y enrollarlo de la mejor manera; además de no cambiarlos por los de otra computadora, ya que de ser necesario tramitar alguna garantía esta no será válida si los números de serie de la computadora y del adaptador no corresponden.

6.11. Queda prohibido colocar, adherir o pintar cualquier tipo de etiqueta, leyen, publicidad, calcomanía o elemento ajeno al bien, o con excepción de la dentificación correspondiente de control patrimonial o control de inventarlos.

VII. INDICADOR

Indicador	Fórmula	Unidad de medida	Periodicidad	Meta
N/A	N/A	N/A	N/A	N/A

VIII. ANEXOS

Código	Nombre del anexo	Ubicación	AT*	AC*	PTC*	Disposición final
N/A	N/A	N/A	N/A	N/A	N/A	Eliminar

*AT= Archivo de trámite; AC= Archivo de concentración; PTC= Plazo total de conservación.

IX. CONTROL DE CAMBIOS

Fecha	Número de revisión	Actividad
01/12/2021	00	Generación del Documento para las Políticas de Seguridad para Sistemas Informaticos de la Secretaria Ejecutiva del Sistema Estatal Anticorrupción de Yucatán

X. FIRMA DE AUTORIZACIÓN DEL DOCUMENTO

Autorizó	**Vo Bo**
Lic. Edwin Manuel Rejón Pacheco **Secretario Técnico**	**C.P. Lauro Ismael Canché Cháves** **Director de Administración y Finanzas**