POLÍTICAS Y LINEAMIENTOS PARA EL USO DE EQUIPOS DE CÓMPUTO, SERVICIOS DE RED, INTERNET Y CORREO ELECTRÓNICO

El Plan de Desarrollo del Estado de México 2017-2023, publicado en el periódico oficial "Gaceta del Gobierno", el 15 de marzo de 2018, señala en el Eje 3: Conectividad y Tecnología para el Buen Gobierno, que en el siglo veintiuno, el rasgo de todo gobierno moderno y vanguardista debe ser el uso de la conectividad y las tecnologías para ser más eficaz en la atención ciudadana, darle mayor fuerza a la rendición de cuentas y a la transparencia, fortalecer la capacidad de respuesta gubernamental ante la demanda social, y darle mayor alcance a su comunicación con diversos actores.

La Secretaría de la Contraloría, conforme a lo previsto en los artículos 19, fracción XIV y 38 Bis, de la Ley Orgánica de la Administración Pública del Estado de México; es la dependencia del Ejecutivo Estatal encargada de la vigilancia, fiscalización y control de los ingresos, gastos, recursos y obligaciones de la Administración Pública Estatal y su sector auxiliar, así como lo relativo a la presentación de la declaración patrimonial, de intereses y constancia de presentación de la declaración fiscal; así como de las responsabilidades de los servidores públicos.

El Manual General de Organización de la Secretaría, establece como objetivo para la Dirección de Gobierno Tecnológico: Planear, regular, y proporcionar los servicios de soporte técnico a equipo de cómputo, seguridad informática y administración de la infraestructura de red a las unidades administrativas de la Secretaría; facilitando el desempeño de sus funciones, y promover las acciones en materia de gobierno digital y acceso libre a la información gubernamental en el ámbito de su competencia.

Asimismo, el Manual General de Organización y Reglamento Interior de la Secretaria de la Contraloría establece entre otras atribuciones para la Unidad de Tecnologías de la Información y Comunicaciones lo siguiente:

I. Autorizar lineamientos, políticas y controles de seguridad de las aplicaciones digitales, así como de la infraestructura informática que opera en la Secretaría.
II. Elaborar y aplicar los lineamientos, políticas y controles para garantizar la seguridad e integridad de la infraestructura tecnológica de la Secretaría.
III. Administrar los componentes de hardware que dan soporte a los servicios electrónicos de la Secretaría, a fin de mantenerlos en operación, así como prevenir, detectar o corregir las contingencias que se presenten.
IV. Atender las políticas y lineamientos que emita la Dirección General del Sistema Estatal de Informática de la Secretaría de Finanzas en materia de tecnologías de la información, en el ámbito de su competencia.

OBJETIVO

Establecer los lineamientos para el uso de equipos de cómputo, servicios de red, internet y correo electrónico al interior de la Secretaría de la Contraloría.

ALCANCE

Las políticas y lineamientos para el uso de equipos de cómputo, servicios de red, internet y correo electrónico, son de observancia general y obligatoria por los usuarios adscritos a la Secretaría de la Contraloría y usuarios externos que hagan uso de los mismos.

DISPOSICIONES GENERALES

PRIMERO. Las políticas y lineamientos constituyen las reglas de negocio emitidas por la Unidad de Tecnologías de la Información y Comunicaciones para el uso de la infraestructura tecnológica instalada en la Secretaría de la Contraloría, por lo anterior, todos los usuarios, deberán apegarse estrictamente a ellas derivado que son de observancia general y obligatoria.

SEGUNDO. Para efectos de las Políticas y Lineamientos, se entenderá por:

a) SECOGEM: Secretaría de la Contraloría del Gobierno del Estado de México.

b) UTIC: Unidad de Tecnologías de la Información y Comunicaciones, de la Secretaría de la Contraloría.

c) Usuario: Cualquier persona física o jurídica contratada por la SECOGEM que haga uso de la infraestructura tecnológica.

d) Dirección IP: Número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, laptop, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

e) Script: Archivo de órdenes, archivo de procesamiento por lotes.

f) Host: Computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella.

g) Peer to peer: (P2P, por sus siglas en inglés) protocolo de comunicación que permite el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

h) Infraestructura tecnológica: software, hardware, telecomunicaciones

i) Equipo arrendado: Equipamiento con que cuenta la SECOGEM bajo el No. Contrato: CS-A-15-2019, “SERVICIO DE ARRENDAMIENTO DE EQUIPO Y BIENES INFORMÁTICOS”

1. POLÍTICAS PARA EL USO DE EQUIPOS DE CÓMPUTO

1.1. DISPOSICIONES GENERALES

1.1.1. La Coordinación Administrativa asignará un equipo de cómputo a los servidores públicos que por sus funciones lo requieran, el cual deberán tener bajo su responsabilidad, utilizando los mecanismos de resguardo que establezca la normatividad vigente.

1.1.2. Posterior a la asignación o reasignación de equipos de cómputo, el usuario deberá solicitar a la UTIC el servicio de instalación y configuración correspondiente, a través del sistema de soporte técnico o mecanismo disponible en caso de falla del sistema.

1.1.3. Es obligación de los usuarios, mantener en buenas condiciones el equipo de cómputo asignado.

1.1.4. El equipo de cómputo asignado, únicamente deberá ser utilizado para actividades institucionales relacionadas con los objetivos y metas de la SECOGEM.

1.1.5. El usuario deberá firmar el resguardo por el equipo de cómputo, accesorios y licencias de software que lo acompañen, a través de los medios que la Coordinación Administrativa determine.

1.1.6. El usuario es responsable de la información y de los programas de software que tiene instalado el equipo de cómputo asignado.

1.1.7. Es responsabilidad de los usuarios realizar los respaldos de su información de manera diaria, semanal, mensual, anual etc. según las necesidades que se requieran por las funciones institucionales que desempeña, esto con el fin de preservar la integridad, disponibilidad y confidencialidad de la información que se encuentre alojada en su equipo, nube u algún otro dispositivo.

1.1.8. El usuario deberá abstenerse de consumir alimentos o ingerir líquidos, en el entorno de operación del o los equipos de cómputo.

1.1.9. El usuario deberá evitar colocar objetos encima del equipo de cómputo o cubrir los orificios de ventilación del monitor o del gabinete.

1.1.10. En caso de incidentes en equipos propiedad de la Secretaria de la Contraloría como robo, extravío, daño físico o lógico que afecten el funcionamiento de un equipo de cómputo, sus componentes o accesorios, el usuario debe notificar de inmediato de manera oficial a la Coordinación Administrativa.

1.1.11. En caso de incidentes en equipos arrendados que se encuentran instalados en la Secretaría de la Contraloría como robo, extravío, daño físico o lógico que afecten el funcionamiento de un equipo de cómputo, sus componentes o accesorios, el usuario deberá notificar y levantar el ticket correspondiente ante la empresa ALTUM al teléfono: 55-2347-0151 ó al Correo electrónico mesadeservicio@aluxen.com.mx.

1.1.12. Es obligación del usuario atender las solicitudes de la UTIC para revisión, mantenimiento y actualización de los equipos de cómputo, realizados de manera local o remota.

1.1.13. El usuario deberá apagar sus equipos de cómputo y no break, al finalizar su jornada laboral.

1.2. MANTENIMIENTO DE LOS EQUIPOS DE CÓMPUTO

1.2.1. La UTIC realizará los mantenimientos preventivos a los equipos propiedad de la Secretaría de la Contraloría cuando se identifique que dicho mantenimiento no se ha realizado en el último año o el equipo lo requiere y que no se encuentre en periodo de garantía por el fabricante, por lo cual, previo a su ejecución, se coordinará todo lo relativo al mantenimiento con los usuarios.

1.2.2. Para los equipos arrendados que se encuentran instalados en la Secretaría de la Contraloría el servicio de mantenimiento lo realizará la empresa conforme a las clausulas establecidas en el contrato correspondiente. Por lo que el personal de la UTIC, únicamente atenderá servicios relacionados con la información del usuario y algunos aspectos de configuración para acceso a la red de la SECOGEM.

1.2.3. El usuario deberá respaldar la información institucional previo a la realización de los mantenimientos preventivos correspondientes y otorgar las facilidades para esta actividad.

1.3. DISPOSITIVOS Y EQUIPOS EXTERNOS

1.3.1. Los titulares de las unidades administrativas, podrán solicitar el acceso de un equipo de cómputo ajeno a la SECOGEM a la red institucional, mediante oficio dirigido al titular de la UTIC, señalando de forma detallada el motivo por el cual se requiere el acceso, y para lo cual, el titular de la unidad administrativa solicitante, deberá especificar el nombre del usuario que tendrá acceso a la red institucional, así como, la información que se obtendrá o examinará mediante este acceso y el uso que de esto pueda derivarse.

La UTIC se reserva el derecho de configurar el acceso al equipo de cómputo que no cuente con licencia vigente de antivirus y del software instalado, así como con la última actualización del sistema operativo.

1.3.2. La UTIC no otorgará servicios de mantenimiento y soporte técnico a equipos de cómputo u otros dispositivos informáticos ajenos al inventario de bienes de la SECOGEM.

1.3.3 Para el equipo que se encuentra arrendado solo proporcionara servicios de soporte técnico a los usuarios en los casos que puedan ser resueltos por su personal (por ejemplo, configurar impresoras, conexión a Internet, etc.) mismas que serán determinadas al momento de la revisión, no se realizarán intervenciones mayores si el equipo lo requiere.

En caso que el equipo requiera una intervención mayor. el usuario del equipo, deberá levantar el ticket correspondiente ante la empresa ALTUM al teléfono: 55-2347-0151 ó al Correo electrónico mesadeservicio@aluxen.com.mx.

1.4. SEGURIDAD INFORMÁTICA

1.4.1. La UTIC es la responsable de configurar en los equipos de cómputo institucionales, el servicio de seguridad informática (que incluye: antivirus, firewall, IPS, antispam y antimalware), bajo ninguna circunstancia el usuario deberá deshabilitar, desinstalar o reconfigurar este servicio.

1.4.2. El usuario tiene la obligación de realizar el análisis de antivirus de los dispositivos de almacenamiento externo que conecte al equipo de cómputo asignado.

1.4.3. El usuario deberá mantener sus equipos informáticos con controles de acceso como contraseñas y protectores de pantalla, como una medida de seguridad cuando necesita ausentarse de su escritorio.

1.5. POLÍTICAS DE NO AUTORIZACIÓN (Restricciones en el servicio)

Queda estrictamente prohibido realizar lo siguiente:

1.5.1. Utilizar por si o a través de un tercero, los recursos informáticos para realizar actividades prohibidas por las disposiciones legales.

1.5.2. Realizar cambios a la configuración o modificaciones a la apariencia o funcionalidad de alguno de los componentes de software y hardware con la que se entrega el equipo de cómputo o de comunicaciones.

1.5.3. Abrir o desarmar los equipos de cómputo (sin previa autorización por escrito de la UTIC ó Coordinación Administrativa), propiciando además la pérdida de la garantía que proporciona el proveedor o fabricante.

1.5.4. Desagregar componentes de un equipo de cómputo, como ratones, memoria, monitores, teclados, etcétera, para incorporarlos a otro, ya sea interno o externo a la SECOGEM, de forma temporal o permanente, sin autorización previa de manera escrita de la Coordinación Administrativa.

1.5.5. Violar la propiedad intelectual de cualquier persona o institución. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso.

1.5.6. Instalar cualquier tipo de software en los equipos de cómputo proporcionados por la SECOGEM para la prestación del servicio, sin la previa autorización de la UTIC.

1.5.7. Difundir cualquier información institucional, sin previa autorización por escrito de la Unidad administrativa propietaria de la misma.

1.5.8. Utilizar los equipos de cómputo provistos por la SECOGEM para conseguir o transmitir material o información con fines de lucro o no institucionales.

1.5.9. Realizar actividades que contravengan la seguridad de los equipos de cómputo, sistemas, correo electrónico, red, etc. que generen interrupciones o degradación en el servicio que estos proporcionan.

1.5.10. Evadir los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, correo, etc.

1.5.11. Interferir, suplantar o negar el servicio a los usuarios con el propósito de lesionar la prestación del servicio o la imagen de la SECOGEM.

1.5.12. Modificar la configuración del sistema operativo, antivirus o firewall.

1.5.13. Compartir carpetas en la red de manera irrestricta, para lo cual deberá solicitar la autorización a la UTIC, quien asesorará del medio más adecuado para proveer el servicio requerido o atender una necesidad específica.

1.5.14. Queda prohibido ver, escuchar o descargar desde sitios de internet o guardar en los equipos de cómputo, gráficos, imágenes, videos, música o cualquier otro material que pueda ser percibido como obsceno, abusivo o que contenga humor inapropiado, lenguaje amenazante, de acoso u otra forma de lenguaje objetable dirigido a un individuo o grupo.

1.5.15 Los usuarios de equipos de cómputo arrendados o propiedad de la Secretaría de la Contraloría, no podrán intercambiar componentes (monitores, cpu, no break, etc.) que alteren los inventarios y resguardos establecidos, sin previa autorización por escrito de la Coordinación Administrativa.

2. POLÍTICAS DE USO DE LA RED DE DATOS

2.1. DISPOSICIONES GENERALES

2.1.1. La red de datos la SECOGEM, contiene elementos para ofrecer servicios de uso exclusivamente institucional.

2.1.2. La UTIC, podrá suspender la conexión a la red de datos, inhabilitación de servicio de internet o correo electrónico, cuando un equipo de cómputo, equipo de conectividad o cualquier otro elemento de la red de datos represente un riesgo de desempeño o de seguridad en la infraestructura tecnológica de la SECOGEM.

2.2. POLÍTICAS DE NO AUTORIZACIÓN (Restricciones en el servicio)

Queda estrictamente prohibido realizar lo siguiente:

2.2.1. Propagar archivos de entretenimiento como música, videos, fotos etc., que sean ajenos a las funciones de las unidades administrativas establecidas en el Manual de Organización de la SECOGEM.

2.2.2. Utilizar la infraestructura de la red de datos con el fin de cometer actos ilícitos, infringir la normatividad vigente del Estado de México o de cualquier otra entidad federativa.

2.2.3. Ejecutar software de escaneo y/o análisis de red (monitoreo) sin previa autorización de la UTIC.

2.2.4. Auto-asignarse una dirección IP.

2.2.5. Intercambiar cuentas y claves de acceso a la red de datos, sistemas de información, intranet o a cualquier otro recurso tecnológico.

2.2.6. Realizar modificaciones a la configuración de la red de datos.

2.2.7. Instalar dispositivos de interconexión o ampliación de nodos de red, ya sea alámbricos o inalámbricos (switches, repetidores Wifi, etc).

2.2.8. Realizar actividades que vulneren o generen interrupciones de la red o de los servicios.

3. POLITICAS DE USO DEL SERVICIO DE INTERNET

3.1. DISPOSICIONES GENERALES

3.1.1. La UTIC, tiene la facultad de suspender total o parcialmente el servicio de internet, cuando detecte un mal uso que ponga en riesgo o vulnere la infraestructura tecnológica de la red de datos de la SECOGEM.

3.1.2. El historial de navegación del servicio de Internet, está sujeto a revisión y/o monitoreo por parte de la UTIC, la cual podrá dar parte al Órgano Interno de Control.

3.1.3. El servicio de Internet, es para uso exclusivo de actividades institucionales.

3.1.4. El acceso a sitios web adicionales a los prestablecidos, podrá solicitarse a través de oficio dirigido al titular de la UTIC, debidamente autorizado y justificado por el Director General o equivalente.

3.2. POLÍTICAS DE NO AUTORIZACIÓN (Restricciones en el servicio)

Queda estrictamente prohibido realizar lo siguiente:

3.2.1. Uso, distribución o propagación de cualquier programa, script o comando diseñado para interferir con el uso, funcionalidad o conectividad de cualquier usuario, host, sistema o site dentro de Internet.

3.2.2. Navegar en sitios web que pongan en riesgo la seguridad de los servicios de comunicación o Internet.

3.2.3. Instalar programas de descarga masiva.

3.2.4. Acceso o participación en sitios Web relacionados con actividades de juego, apuestas, o actividades ilegales en general.

3.2.5. Acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía.

3.2.6. Acceso a sitios de juegos, videos, música u otros sitios de entretenimientos on-line.

3.2.7. Acceso a sitios Web de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, bromas de mal gusto, prejuicios, menosprecio, o acoso explícito.

3.2.8. Acceso a sitios de “hacking” o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información de la SECOGEM.

3.2.9. Descarga o instalación desde Internet de cualquier material (incluyendo software), ya sea de uso libre, demo o protegido bajo leyes de derecho de propiedad, para usos no relacionados con la actividad de la SECOGEM.

3.2.10. Publicación de cualquier tipo de información perteneciente a la SECOGEM, en sitios personales u otros, sin la autorización del propietario de la misma.

3.2.11. Publicación de comentarios no profesionales en foros públicos, sitios de chat, Weblogs (Blogs), correo electrónico, o cualquier otro medio de publicación en Internet.

3.2.12. Operación de negocios personales.

3.2.13. Obtención de acceso no autorizado sobre otras computadoras pertenecientes a cualquier otra organización o entidad.

3.2.14. Instalación y uso de programas de tipo “peer-to-peer”.

3.2.15. Instalación y uso de programas de mensajería.

4. POLÍTICAS DE USO DEL CORREO ELECTRÓNICO

4.1. DISPOSICIONES GENERALES

4.1.1. Las personas servidoras públicas adscritas a la SECOGEM con cargo de Secretario, Subsecretario, Directores Generales, Jefes de Unidad, Directores de Área, Contralores internos, Subdirectores, Jefes de Departamento, enlaces y personal operativo que por sus funciones lo requieran, podrán gestionar una cuenta de correo electrónico institucional previa autorización del director general o director de área, mediante oficio dirigido al titular de la UTIC.

Se podrá gestionar una cuenta de correo electrónico, para enviar y recibir información relacionada con las funciones institucionales de la SECOGEM.

4.1.2. Se entiende por cuenta de correo electrónico, la asignación por parte de la UTIC de:

a) Una dirección electrónica con la forma usuario@secogem.gob.mx

b) Un buzón (espacio en disco) para almacenar los mensajes.

c) Una palabra clave o password para acceder de manera privada a la cuenta.

d) La posibilidad de enviar y recibir mensajes dentro de la SECOGEM y hacia internet utilizando la dirección electrónica asignada.

Con el fin de realizar acciones encaminadas a que la información pueda estar disponible independientemente de la permanencia del titular en el cargo, las cuentas de correo que sean asignadas a la Unidad Administrativa o usuarios deberán seguir las siguientes recomendaciones:

Unidades Administrativas: se conformarán con el nombre de la misma y siendo necesario la cuenta tendrá un alias conformado por el nombre y primer apellido del titular (sin tildes ni signos propios de algunos idiomas).

Usuarios: se conformarán con el nombre y primer apellido del usuario (sin tildes ni signos propios de algunos idiomas).

En caso de presentarse coincidencias en la identificación de dos alias, se resolverá de acuerdo con el orden de procesamiento: el primer usuario recibirá la identificación antes mencionada, el segundo será modificado recurriendo al segundo apellido.

Las cuentas de correo electrónico definidas con anterioridad que no sigan la estructura antes mencionada, quedarán como un alias dirigido a la cuenta de correo de su unidad administrativa de adscripción.

En caso de presentarse alguna situación relacionada con la administración de las cuentas de correo institucionales, se resolverá de acuerdo a lo que considere necesario la UTIC.

4.1.3. Aunque la dependencia cuenta con un servicio de revisión de virus para los mensajes de correo entrante, los usuarios deberán verificar que los mensajes que se reciban o se envíen no incluyan virus, para lo cual su programa instalado para tal efecto, deberá estar activo y mantenerse actualizado. Es responsabilidad de cada usuario verificar lo anterior, en caso de duda deberá comunicarse al área de soporte técnico de la UTIC.

4.1.4. Es responsabilidad de cada usuario tener copias de respaldo (backup's) de los mensajes de sus carpetas de correo y de su agenda de direcciones electrónicas.

4.1.5. La UTIC se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para su seguridad.

4.1.6. Se eliminarán las cuentas de correo electrónico con un periodo de inactividad mayor a 2 meses.

4.2. POLÍTICAS DE NO AUTORIZACIÓN (Restricciones en el servicio)

Queda estrictamente prohibido realizar lo siguiente:

4.2.1. Enviar o contestar cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.

4.2.2. Usar la cuenta para fines comerciales o personales.

4.2.3. Transmitir virus o programas de uso mal intencionado.

4.2.4. Suscribirse a cualquier lista de correo que genere mensajes cuyo contenido no tenga que ver con las funciones de la SECOGEM.

4.2.5. Usar el correo electrónico con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil, sin importar el idioma, la periodicidad o tamaño del mensaje.

4.2.6. Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de la SECOGEM.

4.2.7. Usar comandos o programas o el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

4.2.8. Enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (e-mail spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).

4.2.9. Responder a todas las personas cuando se envíen comunicados generales o para un grupo específico de personas, a excepción de que ésta sea la finalidad de la respuesta.

4.2.10. Exceder los 25 MB. el tamaño de los archivos adjuntos, este tamaño puede ser verificado por medio de las propiedades de cada archivo, desde el Explorador de Windows o bien seleccionando el archivo y presionando ALT+ENTER.

4.2.11. Enviar mensajes masivos (que involucre a todos los usuarios de la SECOGEM), a menos que sea un asunto oficial. El usuario será el responsable por el contenido de los mensajes a efecto que cumplan la característica de ser mensajes oficiales y de carácter laboral.

SANCIONES

El incumplimiento de las "políticas y lineamientos para el uso de equipos de cómputo, servicios de red, internet y correo electrónico", dará lugar a la aplicación de sanciones administrativas previstas por la Ley de Responsabilidades Administrativas del Estado de México y Municipios, sin prejuicio de la responsabilidad penal en que pudieran incurrir los usuarios implicados.

La falta de conocimiento de las presentes políticas, no libera al usuario de las responsabilidades establecidas en ellos por el mal uso que hagan de los equipos de cómputo, servicios de red, Internet o correo electrónico institucional.

Las situaciones no previstas en las presentes políticas serán resueltas por la Unidad de Tecnologías de la Información y Comunicaciones en coordinación con el Órgano Interno de Control, cuando se considere que las faltas cometidas vulneran la seguridad de la infraestructura tecnológica y van en detrimento de la operación institucional, dichas faltas serán causal de la aplicación de sanciones administrativas correspondientes.