POLÍTICAS DE CIBERSEGURIDAD DE LA SECRETARÍA GENERAL DE GOBIERNO DEL ESTADO DE MÉXICO

28 DE NOVIEMBRE DE 2024
VERSIÓN 2.0

PRESENTACIÓN

La política de ciberseguridad se define como una declaración de intenciones de alto nivel que cubren la seguridad de los sistemas informáticos y proporcionan las bases para la definición y la delimitación de las responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

La ciberseguridad es un proceso que, en conjunto con medidas y controles, pretenden asegurar la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que se procesa, almacena y comunica.

Antecedentes

El plan de ciberseguridad para la Secretaría General de Gobierno del Estado de México, es un proceso continuo que involucra a todo el personal de la Secretaría General de Gobierno, con el fin de cumplir con los requisitos de confidencialidad, integridad y disponibilidad de los activos de TI y de la información que se genera, se utiliza y se resguarda de manera digital en la infraestructura local y en el centro de datos estatal, ubicado en la Agencia Digital del Estado de México. Asimismo, ayuda a comprender, administrar y reducir los riesgos de ciberseguridad, así como proteger sus redes y datos.

Es importante destacar que, la información es un recurso que se debe valorar adecuadamente a pesar de ser un bien intangible.

Objetivos

1. Minimizar y gestionar los riesgos, así como detectar los posibles problemas y amenazas a la seguridad que comprometan la información que se almacena, genera y se utiliza dentro de la institución.
2. Garantizar la adecuada utilización de los recursos y de las aplicaciones de los servicios de TI.
3. Limitar las pérdidas de información y conseguir la adecuada recuperación de los servicios e información en caso de un incidente de seguridad.
4. Cumplir con el marco legal normativo (Ley y reglamento de Gobierno Digital del Estado de México).

Justificación

Las políticas de seguridad a servicios tecnológicos institucionales permitirán utilizar los recursos de forma efectiva, disminuyendo el riesgo y asegurando la entrega eficiente de los recursos de TI, tanto a las personas servidoras públicas, practicantes y cualquier persona interesada que tenga una relación con la Secretaría General de Gobierno.

Compromiso de la Secretaría General de Gobierno

La seguridad de la información y sus activos son esenciales para coadyuvar en el cumplimiento de los objetivos y funciones de esta Secretaría General, por lo que es importante contar con medidas y directrices que logren una implantación real de un sistema de seguridad de TI, siendo necesario que se disponga de los recursos necesarios para comunicarlo a todo el personal mediante una campaña de sensibilización sobre la importancia que hoy día tiene la seguridad en un entorno digital y las amenazas existentes.

Alcance

Las presentes medidas se deberán observar de manera obligatoria por las Unidades de Tecnologías de la Información y personal adscrito a la Secretaría General de Gobierno, que tengan acceso a servicios y recursos de Tecnologías de la Información proporcionados por la institución para el cumplimiento de sus funciones administrativas y operativas.

Estas políticas fueron elaboradas con base en la norma internacional ISO/IEC-27001, que es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información, agrupándolas en las siguientes áreas para su mejor comprensión:

1. Gestión de activos.
2. Gestión de recursos humanos.
3. Seguridad física y ambiental.
4. Gestión de comunicaciones y operaciones.
5. Control de acceso a servicios de TIC.
6. Gestión de cumplimiento de la política.

Políticas

GESTIÓN DE ACTIVOS

No.	Política	Descripción	Alcance
1	Inventario de infraestructura de TIC.	Integrar un inventario de activos de TI de la DGSyTI o de las Unidades de Tecnologías, que formen parte de algún servicio en producción.	• Personal técnico de TI
2	Clasificación de la Infraestructura de TIC	Identificar y clasificar los activos según su importancia y nivel de sensibilidad de TI de la DGSyTI o de las Unidades de Tecnologías, que formen parte de algún servicio en producción.	• Personal técnico de TI
3	Identificación y análisis de riesgos.	Llevar a cabo un análisis de riesgos del inventario de TI de la DGSyTI o de las Unidades de Tecnologías a fin de identificar amenazas, vulnerabilidades y el grado de riesgo que representa cada activo del inventario de infraestructura de TIC.	• Personal técnico de TI • Enlaces de TI
4	Control de mantenimiento de la Infraestructura de TIC	Llevar a cabo el registro y seguimiento del control de mantenimiento a la infraestructura de TIC.	• Personal técnico de TI • Enlaces de TI

GESTIÓN DE RECURSOS HUMANOS

No.	Política	Descripción	Alcance
5	Aviso de alta o baja de servidores públicos.	Se debe notificar a la DGSyTI cualquier movimiento de alta o baja del personal relacionado con servicios de TIC (internet, correo electrónico, sistemas	• Enlaces de TI • Recursos Humanos

		administrativos, etc.), a fin de modificar su información o cancelación de credenciales de acceso.	

SEGURIDAD FÍSICA Y AMBIENTAL

No.	Política	Descripción	Alcance
6	Acceso físico a los Centros de Datos Locales (Sites).	Permitir el acceso a los centros de datos únicamente a las personas autorizadas.	• Enlaces de TI • Personal técnico de TI
7	Control y monitoreo ambiental y de suministro de energía eléctrica en los Centros de Datos Locales (Sites).	Proteger la infraestructura de TIC mediante monitoreo continuo de energía, temperatura y humedad adecuados, de acuerdo con las normas internacionales (ISO/IEC 27002).	• Personal técnico de TI
8	Protección de equipos de cómputo y periféricos.	Contar con una instalación de tierra física, fuente de energía auxiliar y de regulación del suministro de esta para cada equipo de cómputo y periférico que se considere esencial para las actividades sustantivas de la Secretaría.	• Todos
9	Traslado de equipo de cómputo y periféricos para mantenimiento físico.	Manejar con precaución el equipo durante su traslado para evitar fallas en los dispositivos de almacenamiento. Antes de enviar el equipo de cómputo a mantenimiento la información debe estar respaldada por el usuario.	• Todos

10	Reubicación de equipo de cómputo y periféricos.	Notificar a los enlaces administrativos de cada unidad para que en conjunto con la DGSyTI o Unidad de Tecnologías para revisar la viabilidad técnica de las instalaciones eléctricas y de comunicaciones.	• Todos
11	Baja de equipo de cómputo.	Para los equipos de cómputo que se aplicará el movimiento de baja, realizar borrado físico de los dispositivos internos de almacenamiento.	• Personal técnico de TI
12	Seguridad en el cableado y nodo de voz y datos de la red local.	Los cables de la red y nodos deben estar plenamente distribuidos a fin de evitar fallas en los servicios de red. En caso de requerir un nuevo cable de red, se deberá determinar su viabilidad técnica.	• Enlace de TI • Todos
13	Trabajo en áreas seguras.	Todos los equipos de cómputo y periféricos deben estar instalados en lugares limpios, secos y en condiciones ambientales y de energía adecuadas.	• Todos

GESTIÓN DE COMUNICACIONES Y OPERACIONES

No.	Política	Descripción	Alcance
14	Gestión de cambios en la infraestructura o servicios de TIC.	Cualquier cambio a la infraestructura de TI o de algún servicio debe ser autorizado y validado por la DGSyTI.	• Personal técnico de TI
15	Separación de recursos de desarrollo, prueba y operación de sistemas.	Se debe contar con ambientes independientes para las actividades de desarrollo y producción de sistemas.	• Personal técnico de TI

16	Provisión y supervisión de servicios de terceros (proveedores).	Contar con un acuerdo de nivel de servicios y de confidencialidad con cualquier proveedor que opere o supervise un sistema de la SGG dentro o fuera de la propia infraestructura de TIC.	• Personal técnico de TI
17	Protección contra código malicioso en equipos de cómputo.	Cada equipo de cómputo debe tener activado y actualizado en su sistema operativo tanto el antivirus como su firewall (Corta Fuegos). Los equipos deben mantenerse actualizados con la última versión estable del sistema operativo, aplicaciones y navegadores webs soportados.	• Todos
18	Almacenamiento de documentos digitales en equipos de cómputo locales o en servidores de archivos.	Los archivos almacenados de manera local deben seguir las reglas mencionadas en la guía de buenas prácticas para la gestión de archivos digitales. https://dgsyti.edomex.gob.mx/buenas-practicas-archivos-digitales	• Todos
19	Respaldo de información en equipos de cómputo.	Contar con un respaldo de archivos oficiales en algún medio extraíble libre de virus o en la cuenta de correo institucional (nube).	• Todos
20	Protección contra código malicioso en la red de área local.	Cada red de área local debe contar con un software o hardware de identificación de intrusos e incorporar, de ser posible, mecanismos adicionales.	• Personal técnico de TI
21	Protección contra programas descargados y	Evitar la descarga e instalación de software no autorizado en los equipos.	• Todos

	aplicaciones permitidas a los usuarios.	En caso de requerirlo para el desempeño de sus funciones, solicitarlo a la DGSyTI para evaluar su factibilidad técnica.	
22	Uso de navegadores web.	Evitar la instalación de extensiones o complementos (plugins, addons). En caso de requerirlo para el desempeño de sus funciones, solicitarlo a la DGSyTI para evaluar su factibilidad técnica.	• Todos
23	Controles de seguridad en las redes de área local cableadas.	Cada red de área local debe contar con mecanismo (firewall) por software o hardware que filtre los accesos entre la red interna y el internet. Evitar la instalación de switches en la red local para ampliar los nodos, así como nodos de red adicionales. En caso de requerirse solicitarlo a la DGSyTI para evaluar su factibilidad técnica.	• Personal técnico de TI • Todos
24	Controles de seguridad en las redes de área local inalámbricas.	Evitar la instalación de puntos de acceso inalámbricos (access points) en la red local para ampliar los nodos. En caso de requerirse solicitarlo a la DGSyTI para evaluar su factibilidad técnica. Utilizar clave robusta para el acceso y habilitar en cada punto de acceso el cifrado.	• Personal técnico de TI • Todos
25	Protección y actualización de parches de seguridad en los sistemas operativos, navegadores web,	Debe mantenerse actualizado con la última versión estable tanto el sistema operativo como las aplicaciones,	• Personal técnico de TI

	servidores de bases de datos, servidores de aplicaciones de los servidores físicos y virtuales en producción.	siempre que sean soportadas por el equipo.	
26	Acceso remoto.	Solicitar autorización a la DGSyTI para evaluar su factibilidad técnica. Todo acceso a servicios de este tipo debe asegurarse, controlarse y encriptarse mediante el uso de firewall y software VPN.	• Personal de TI
27	Conexión de dispositivos móviles personales o de Internet de las cosas (bocinas inteligentes, controles de iluminación, etc) a las redes inalámbricas institucionales.	Se permite su conexión solo a través de la red de invitados. Esta red debe estar aislada de la red local, solo con conexión a Internet limitada en ancho de banda, servicios de descarga y streaming.	• Todos
28	Intercambio de información en medios extraíbles.	Utilizar dispositivos libres de virus solo en el caso de que no pueda utilizarse un medio a través de internet y que no contenga información sensible.	• Todos
29	Intercambio de información en mensajería electrónica.	Utilizar correos de cuentas institucionales y evitar compartir información sensible mediante cualquier software público de mensajería instantánea.	• Todos
30	Información puesta a disposición pública en sitios web institucionales.	Para cualquier publicación en sitios web institucionales, se debe apegar a la ley vigente en materia de transparencia y acceso a la información pública.	• Todos

CONTROL DE ACCESO A SERVICIOS DE TIC

No.	Política	Descripción	Alcance
31	Solicitar o cancelar acceso a sistemas administrados por la DGSyTI.	La Unidad Administrativa que requiera el acceso, debe solicitarlo a la DGSyTI a través de su enlace de TI especificando el nombre de la persona, el rol y permisos para servicio que se quiere utilizar.	• Enlace de TI
32	Solicitar la creación o cancelación de cuentas de correo institucional.	La Unidad Administrativa que requiera el acceso solicitarlo a la DGSyTI a través de su enlace de TI, especificando el nombre de la persona y el tipo de cuenta que se quiere utilizar.	• Enlace de TI
33	Solicitar o cancelar acceso a internet administrado por la DGSyTI o por un administrador de la red local de su inmueble.	La Unidad Administrativa que requiera el acceso, solicitarlo a la DGSyTI a través de su enlace de TI, especificando el nombre de la persona y el nivel de acceso al servicio de internet que se quiere utilizar.	• Enlace de TI
34	Responsabilidades de usuarios (contraseñas, puesto de trabajo y pantalla limpia).	Todas las personas servidoras públicas de la SGG que ingresan a la Institución deben utilizar los servicios de TIC provistos por la misma. Al momento de ingresar a los sistemas y aplicaciones institucionales, cada persona servidora pública está aceptando la responsabilidad y confidencialidad del uso y manejo de los servicios e información institucional, así como el manejo	• Todos

		responsable de su usuario y contraseña. Se debe tener instalado en cada equipo el fondo de pantalla institucional, de acuerdo con las políticas de imagen institucional vigentes. En caso de ausentarse momentáneamente durante el horario laboral, cerrar la sesión activa a fin de volver a reactivar el equipo con su contraseña. No manipular el sistema de arranque (BIOS) del equipo.	
35	Control de acceso a la red de área local.	La DGSyTI debe establecer controles de administración para proteger el acceso y servicios de red locales.	• Personal técnico de TI
36	Control de acceso Internet a través de la red de área local.	La capacidad de descarga de cada usuario final debe ser limitada y controlada. Dentro de la red de datos institucional se restringirá el acceso a: • Descarga de archivos de sitio peer to peer o repositorios no autorizados. • Conexiones a sitios de streaming no autorizado. • Acceso a sitios de pornografía. • Violencia contra niños, niñas y adolescentes.	• Todos

		• Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma. En caso de requerir un servicio sin restricciones será necesario que la unidad administrativa lo solicite a la DGSyTI, a través de su enlace, especificando el nombre de la persona servidora pública que lo utilizará, anexando justificación y autorización de su jefe inmediato superior.	
37	Gestión de contraseñas.	La generación de contraseña del usuario debe cumplir una complejidad media y alta que consiste en la utilización de letras mayúsculas, minúsculas, con caracteres especiales con una longitud mínima de 8 caracteres. • La asignación y cambio de contraseñas se deberá controlar a través de un proceso formal de gestión de contraseñas. • Cada usuario/a deberá cambiar o solicitar el cambio de su clave cada 60 días. • Las contraseñas no deben estar escritas y expuestas a que otras personas las vean. • Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).	• Todos

		• No guardarlas en medios de fácil acceso, ni en archivos sin cifrar. • No habilitar la opción "recordar clave en este equipo ", que ofrecen los programas. • No enviarla por correo electrónico. • Nunca guardar las contraseñas en ningún tipo de papel, agenda, etc. • Las contraseñas se deben mantener confidenciales en todo momento. • No compartir las contraseñas, con otros/as usuarios/as. • Cambiar la contraseña si sospecha que alguien más la conoce y si ha tratado de dar mal uso de ella. • No utilizar la opción de almacenar contraseñas en Internet.	

GESTIÓN DE CUMPLIMIENTO

No.	Política	Descripción	Alcance
38	Protección de datos personales.	Para cualquier base de datos que contenga información de datos personales, notificar al área de transparencia para su registro de acuerdo con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ley del Estado de México.	• Todos • Enlace de TI

39	Inventario de sistemas	La Unidades Administrativas que cuenten con personal de desarrollo, deberán enviar periódicamente el inventario de los sistemas que administran a la DGSyTI a través de su enlace de TI para el control de los sistemas en producción o baja.	• Enlace de TI
40	Uso de Software libre para desarrollo	Se deberá dar prioridad al uso de software libre para el desarrollo de sistemas. En caso de requerir software licenciado para el desarrollo, se deberá informar a la DGSyTI para evaluar su factibilidad técnica.	• Enlace de TI
41	Manuales de Usuario y Capacitación	Se deberán realizar los manuales de usuario de los sistemas desarrollados en conjunto con el área que administra el sistema; y además las capacitaciones a los usuarios finales.	• Personal técnico de TI
42	Contratación de sistemas externos	La Unidad Administrativa que utilice sistemas contratados externamente deberá notificar a la DGSyTI a través de su enlace de TI, especificando el nombre del sistema y proveedor del sistema. El proveedor deberá proporcionar un Acuerdo de Nivel de Servicios (SLA) en caso de ser un Software por Servicio. El proveedor deberá entregar la documentación técnica del sistema, código fuente en caso de que el	• Enlace de TI

		desarrollo pase a propiedad de la unidad administrativa.	
43	Directorio de Personal de desarrollo de sistemas.	La Unidad Administrativa deberá notificar a la DGSyTI a través de su enlace de TI, el nombre y perfil del personal que desarrolla sistemas para su dependencia.	• Enlace de TI
44	Revisión, Mantenimiento y Pruebas de Seguridad de Sistemas.	Asegurar que los sistemas sean probados para detectar y corregir vulnerabilidades antes de su implementación. Todo cambio debe ser analizado previamente en los ambientes de desarrollo y prueba	• Personal técnico de TI