Contenido:

INTRODUCCIÓN. 2
ALCANCE. 2
NORMATIVIDAD. 2
LINEAMIENTOS. 3
01. Seguridad informática en la Institución. 3
02. Buen uso de los activos informáticos. 5
03. Clasificación de la información 5
04. Intercambio de información. 6
05. Prestación de servicios por terceros 6
06. Protección contra código malicioso (virus y malware). 6
07. Servicios informáticos en la red. 7
08. Uso de cuentas de usuario. 8
09. Monitoreo del uso de los servicios informáticos. 9
10. Uso de Internet. 9
11. Uso del correo electrónico. 10
12. Uso del software. 11
13. Vigencia. 11
14. Area responsible. 11

07/Enero/2022

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD PARA LOS SISTEMAS INFORMÁTICOS Y TELECOMUNICACIONES DE LA SECRETARÍA DE SEGURIDAD PÚBLICA

INTRODUCCIÓN.

Las políticas y lineamientos de seguridad informática y de comunicaciones, son directrices que tienen como objetivo promover el buen uso y cuidado de los recursos de tecnologías de información entre personal directivo, administrativo y terceros; mediante la notificación de las medidas y formas que deben cumplir y utilizar para proteger los componentes de los sistemas informáticos de la Secretaría de Seguridad Pública, sin menoscabo de los derechos humanos y la autonomía institucional.

Norman la manera como la Secretaría de Seguridad Pública previene, protege y administra los riesgos relacionados con tecnologías de información en las instalaciones, equipos, información, servicios y soluciones informáticas.

ALCANCE.

Todo el personal relacionado con la dependencia que hagan uso de nuestros servicios e infraestructura de cómputo y comunicaciones, deben de dar cumplimiento a las Políticas y Lineamientos de Seguridad Informática Institucional; tanto en el interior de las instalaciones de la Secretaría de Seguridad Pública de manera física y lógica vía internet.

NORMATIVIDAD.

Los ordenamientos jurídicos administrativos vigentes que regulan la operación de las actividades o tareas específicas a normar a través de las políticas y lineamientos de seguridad informática, entre otros, son:

- Ley de Responsabilidad de Servidores Públicos.
- Código de Conducta.
- Políticas de uso de internet.
- Reglamento de Centro de Cómputo.

POLITICAS Y LINEAMIENTOS.

01. Seguridad informática en la dependencia

Los términos y definiciones utilizados en el presente documento son:

Usuario. - Toda persona que haga uso de los activos o servicios informáticos de la dependencia, para el desempeño de sus funciones, consulta o servicio.

Activo informático. - Son recursos de sistemas informáticos o relacionados con este, que son necesarios para el desempeño de las funciones del usuario, tales como equipos de cómputo, impresoras, video proyectores, pantallas LED, teléfonos, equipos de telecomunicaciones, software, información, entre otros.

Equipo móvil. - Es todo activo informático físico que tiene la facilidad de movilidad, como laptops, tabletas, teléfonos inteligentes, entre otros.

Servicio informático. - Bien intangible que se proporciona para satisfacer los requerimientos de los usuarios, relacionado con el uso de activo informático.

Software. - Conjunto de programas y rutinas que permiten a la computadora realizar determinadas actividades diarias.

Hardware. - Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Software institucional. - Aplicación o programa informático con licenciamiento de uso propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la dependencia.

Software libre. - También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

Contraseña. - Palabra clave mediante la cual el usuario puede tener acceso a una aplicación, archivo informático o sistema de información.

Web, www (World Wide Web). - Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible.

Internet. - Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Antivirus. - Software especializado diseñado para detectar, eliminar y prevenir virus informáticos en los dispositivos de la Red.

Virus: Software creado para producir daño en un equipo informático.

Malware: cualquier tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento.
Correo Electrónico. - Servicio de la Red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos.

Equipo de Cómputo. - Dispositivo electrónico de uso personal capaz de almacenar información, procesar datos y entregarle al usuario los resultados de la información procesada.

Infraestructura. - Conjunto de bienes informáticos, cableado, equipos de cómputo, dispositivos de red, servidores y otros equipos de naturaleza tecnológica.

Servidor. - Equipo de cómputo de altas prestaciones, que forma parte de una red y provee servicios a otros equipos denominados clientes.

Sistema Operativo. - Programa o conjunto de programas informáticos que gestiona los recursos de Hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

Firewall. - Software especializado de protección, también llamado cortafuegos, sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, incluyendo malware y virus, bloqueando el acceso no autorizado.

02. Buen uso de los activos informáticos.

Artículo 1. Los usuarios que tengan activo informático asignado de manera personal para uso de sus funciones, son los únicos responsables de su utilización, así como también de la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

Artículo 2. Toda movilización de activo informático dentro o fuera de las instalaciones de la institución es responsabilidad del usuario resguardante.

03. Clasificación de la información.

Artículo 3. El dueño de un servicio informático ofrecido por la institución es responsable de la información que este servicio genera y procesa.

Artículo 4. Los titulares de cada área, coordinación o departamento deben informar a sus colaboradores de la clasificación de la información a su cargo para su adecuado tratamiento.

Artículo 5. Todo usuario es responsable del resguardo de datos, debe confirmar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación. La información puede estar disponible de manera electrónica, impresa en papel, magnética, o bien, en algún otro medio.

Artículo 6. Todo usuario deberá hacer uso de la información a la que tenga acceso, únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales, absteniéndose de comunicarlos a terceros sin el consentimiento expreso de la persona a la que se refieren.

Artículo 7. Todos los usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

04. Intercambio de información.

Artículo 8. Toda persona que intercambie información reservada y/o confidencial con personal de la Secretaría de Seguridad Pública o terceras personas, debe asegurar la identidad de la persona a la que le es entregada la información, ya sea por medio físico o electrónico, dejando constancia que es procedente la entrega de información.

Artículo 9. Todo convenio de la Secretaría de Seguridad Pública con terceras personas para compartir información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales.

05. Prestación de servicios por terceros.

Artículo 10. Todo proveedor que proporcione servicios informáticos a la Secretaría de Seguridad Pública y que tenga acceso a información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique a la dependencia.

Artículo 11. Todo servicio informático otorgado por terceros debe ser monitoreado y revisado por la persona responsable de su contratación, para asegurar que se cumplan con los términos estipulados en los acuerdos o contratos de la Secretaría de Seguridad Pública.

06. Protección contra código malicioso (virus y malware).

Artículo 12. Todo equipo de cómputo de la dependencia debe contar con software antivirus y antimalware, así como estar protegido por el Firewall *(Fortinet o Microtik)*. Si el software antivirus no cubre a la plataforma utilizada, el personal notificará al personal asignado para buscar una alternativa de solución.

Artículo 13. Todo usuario que identifique una anomalía en su equipo de cómputo deberá reportarla de inmediato al personal de la Unidad de Informática para su inmediata atención.

07. Servicios informáticos en la red.

Artículo 14. Todo el personal y/o terceros son responsables del buen uso de los servicios informáticos alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones administrativas y laborales.

Artículo 15. Sólo el Personal de la Unidad de Informática queda facultado para acceder a los equipos de cómputo de la dependencia, para:

- Ejecutar las tareas del procedimiento de mantenimiento preventivo y correctivo.
- Realizar modificaciones al Sistema Operativo.
- Realizar una revisión de seguridad informática y descartar el uso indebido (daños intencionales a información o hardware) del equipo de cómputo.

Artículo 16. Todo titular del área o departamento, es responsable de autorizar el acceso al equipo de cómputo que tiene asignado, para que el personal a su cargo realice sus funciones.

Artículo 17. Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información, excepto en casos que se especifican en el artículo 15 del presente documento.

Artículo 18. Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información en la red de la Secretaría de Seguridad Pública, son personales, permitiéndose el uso bajo su responsabilidad, única y exclusivamente durante la vigencia de los derechos del usuario. La vigencia de las cuentas de usuarios es facultad de personal de la Unidad de Informática, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los usuarios.

Artículo 19. Toda utilización de herramientas tales como analizadores, escaneo y monitoreo de red, son permitidas únicamente para las funciones de administración de las tecnologías de información por parte de la Unidad de Informática.

Artículo 20. El equipo de cómputo (computadoras de escritorio y portátiles), será configurado solamente por personal de la Unidad de Informática para brindar acceso a la red de la Secretaría de Seguridad Pública. Todo usuario se abstendrá de realizar cambios en configuraciones de esta naturaleza, en caso de falla o error de acceso a internet por esta causa, será el único responsable.

Artículo 21. A toda persona que deje de laborar o tener relación con la Secretaría de Seguridad Pública, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. El Departamento de Personal comunicará a la Unidad de Informática, toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

Artículo 22. Todo hardware y software de uso que sea considerado de riesgo para la seguridad de los servicios informáticos institucionales, deberá ser utilizado en ambiente aislado.
Por ejemplo, analizadores de tráfico de red, herramientas de análisis y diagnóstico de equipos de cómputo, equipos de laboratorio de redes, entre otros.

08. Uso de cuentas de usuario.

Artículo 23. Toda persona que requiera acceder a servicios informáticos, tales como Correo Electrónico Institucional, requerirá de una cuenta de usuario y contraseña. Estos datos serán asignados por el responsable del servicio de la Unidad de Informática.

Artículo 24. Toda solicitud de alta, baja o cambio de privilegios de cuentas de personal administrativo de confianza o sindicalizado, para acceder a los servicios informáticos debe ser realizada por el jefe inmediato o jefe de área, debidamente justificado.

Artículo 25. Todo usuario debe actualizar la contraseña de su cuenta de acceso a los servicios informáticos de manera periódica (al menos cada 3 meses) o cuando sospeche que pueda estar comprometida supervisado por la Unidad de Informática.

Artículo 26. Cuando se requiera acceder a información de un equipo de cómputo y/o cuenta de correo institucional de una persona ausente, ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar a la Unidad de Informática que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso institucional. El personal de la Unidad de Informática únicamente proporcionará acceso al responsable del área correspondiente que lo haya solicitado a efecto de que sustraiga la información necesaria, dejando constancia de ello por escrito y con firma del solicitante.

Si una persona deja de laborar en la dependencia o cambia de puesto, el jefe inmediato podrá solicitar al Titular de la Unidad de Informática el acceso al equipo que ésta tenía asignado, el cual es concedido para que sustraiga la información pertinente.

09. Monitoreo del uso de los servicios informáticos.

Artículo 27. El personal de la Unidad de Informática realiza periódicamente revisiones de hardware y software del activo informático institucional, para dar atención a problemas de obsolescencia y revisiones de licenciamiento. Además, se monitorean los servicios informáticos de red para administrar el uso del recurso de internet y solucionar cualquier problema detectado.

10. Uso de Internet.

Artículo 28. El servicio de Internet a través de las redes institucionales se considera como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a sus actividades laborales en la Secretaría de Seguridad Pública.

Artículo 29. Todo responsable de área puede solicitar la restricción total o parcial de acceso a Internet del personal a su cargo, considerando para ello las funciones laborales que éstos realizan.

Artículo 30. Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio, debe de omitir descargar archivos de dudosa procedencia. Los archivos descargados de Internet pueden contener virus o software malicioso que pongan en riesgo la información del equipo de cómputo de la persona, e incluso de la dependencia.

11. Uso del correo electrónico.

Artículo 31. El correo electrónico institucional es para uso exclusivo del empleado activo administrativo y/o sindicalizado. Éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

Artículo 32. Los responsables de área o departamento deberán solicitar la creación de nuevas cuentas de correo electrónico para personal a su cargo al Titular de la Unidad de Informática.

Artículo 33. La Secretaría de Seguridad Pública no es garante de los contenidos expresados en texto, sonido o video, redactados y enviados mediante el correo electrónico institucional. Ante algún correo de naturaleza sospechosa, abstenerse de abrirlo y eliminarlo de inmediato, para evitar descargar algún tipo de amenaza para el equipo de cómputo asignado y para la red institucional.

Artículo 34. A toda persona que termine la relación laboral con la Secretaría de Seguridad Pública, una vez recibida la notificación de baja por parte del Departamento de Personal, se inhabilitará el servicio de correo electrónico. Transcurridos 30 días hábiles, el contenido de la cuenta de correo inhabilitada será eliminado definitivamente.

Artículo 35. Toda solicitud de alta, baja o cambio de un grupo de correo institucional, debe ser solicitado por el responsable del área solicitante.

Artículo 36. Queda prohibido utilizar el correo electrónico para envíos de correo basura, cadenas, mercadotecnia, religiosos, propaganda política, actos agresivos e ilegales y cualquier otro contenido no apropiado para el destinatario.

Artículo 37. Es responsabilidad de todo usuario del correo electrónico institucional notificar al Titular de la Unidad de Informática la sospecha del uso no autorizado de su cuenta.

Artículo 38. Es responsabilidad del usuario respaldar aquellos correos electrónicos que por su contenido considere relevantes. Así mismo, el usuario deberá depurar constantemente los mensajes y borrar aquellos que no le son de utilidad, para liberar el espacio asignado a su cuenta de correo y evitar problemas de saturación.

Artículo 39. Todo usuario del correo electrónico institucional, acepta que comprende y acuerda expresamente que la SSP, no es responsable directo e indirecto y sin limitación alguna, por pérdida de datos o de cualquier otra pérdida intangible en el servicio de correo electrónico.

12. Uso del software.

Artículo 40. En todos los equipos de cómputo de la Secretaría de Seguridad Pública, solo se permite la instalación de software con licenciamiento vigente, ya sea de uso libre o comercial. La Unidad de Informática es la única facultada para realizar la instalación del software.

Artículo 41. Todo elemento del personal que instale software sin licenciamiento vigente o malicioso en equipos de cómputo de la institución, se hace único responsable de las consecuencias que esto conlleve.

Artículo 42. Las licencias de uso de software propiedad de la Secretaría de Seguridad Pública, otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados, propiedad de la dependencia.

13. Vigencia.

Estas políticas y lineamientos surtirán efecto a partir de su publicación y hasta que sufran alguna actualización.

https://www.sspcoahuila.gob.mx/archivos/Politicas%20y%20Lineamientos%20de%20Seguridad.pdf

14. Área responsable.

Unidad de Informática de la Secretaría de Seguridad Pública