LINEAMIENTOS DE SEGURIDAD PARA LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES DEL ITAIH.

CONTENIDO

CAPITULO I
DISPOSICIONES GENERALES

Artículo 1. Los Lineamientos de Seguridad para los Sistemas Informáticos y de Comunicaciones, son directrices que tienen como objetivo promover el buen uso y cuidado de los recursos tecnológicos entre personal directivo y administrativo. Las disposiciones de los presentes lineamientos son de observancia general, para proteger los componentes de los recursos y sistemas informáticos y la confidencialidad de la información del instituto.

Los presentes Lineamientos norman la manera como el instituto previene, protege y administra los riesgos relacionados con tecnologías de información en las instalaciones, equipos, información, servicios y soluciones informáticas.

Artículo 2. Todo el personal terceras personas relacionadas con nuestra institución que hagan uso de nuestros servicios e infraestructura de cómputo y comunicaciones, deben de dar cumplimiento a los Lineamientos de Seguridad para los Sistemas Informáticos y de Comunicaciones; tanto en el interior de las instalaciones, como en el exterior; de manera física y lógica vía internet.

Artículo 3. El presente documento deberá ser revisado y actualizado cuando se considere necesario por la Dirección de Tecnologías de la Información.

Artículo 4. Para los efectos de los presentes Lineamientos, se entenderá por:

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

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.

DTI. - Dirección de Tecnologías de la Información.

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

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.

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

Firewall. - Software especializado de protección, también llamado cortafuegos, cuya función es prevenir y proteger un equipo de cómputo o a una red privada de intrusiones o ataques a través de una conexión de red, bloqueando el acceso no autorizado.

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

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

Información reservada y/o Confidencial. - La información clasificada como reservada es aquella que se encuentra temporalmente fuera del acceso público, debido al daño que su divulgación causaría a un asunto de interés público o seguridad nacional.

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

Malware. - cualquier tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento.

ITAIH. – Instituto de Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales del Estado de Hidalgo.

.

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

Privilegio. - Derecho de un usuario a realizar una tarea específica, que suele afectar a un sistema completo en lugar de un objeto determinado. Los privilegios los asignan los administradores a usuarios individuales o grupos de usuarios, como parte de la configuración de seguridad del equipo.

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

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

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.

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

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 institución.

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

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

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.

CAPITULO II
DEL BUEN USO DE LOS ACTIVOS INFORMATICOS

Artículo 5. 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.
Únicamente al personal adscrito a la institución se podrá asignar responsiva de activos informáticos, misma que deberá quedar bajo escrito.

Artículo 6. Toda movilización de activo informático dentro o fuera de las instalaciones de la institución es responsabilidad del usuario responsable del resguardo.
Para el caso de equipos de telecomunicaciones entre ellos switches, puntos de acceso, ruteadores, deberá ser bajo supervisión de la DTI.

CAPITULO III
CLASIFICACIÓN DE LA INFORMACIÓN

Artículo 7. El dueño de un servicio informático ofrecido por el ITAIH es responsable de la información que este servicio genera y procesa.

Artículo 8. 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 9. Todo usuario es responsable del resguardo de datos y debe vigilar 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 10. 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 11. Todos los usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas y se debe asegurar que se solicite un medio de autentificación para su acceso.

CAPITULO IV
INTERCAMBIO DE INFORMACIÓN Y PRESTACIÓN DE SERVICIOS

Artículo 12. Los usuarios que intercambien información que haya sido declarada reservada y/o confidencial, con personal del ITAIH o con terceras personas, deberán asegurarse de dejar el registro correspondiente de la entrega de la información que sea proporcionada, ya sea por medio físico o electrónico.

Artículo 13. Todo convenio del ITAIH con empresas, dependencias o 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. Se deberá asegurar que en el convenio se agreguen cláusulas de confidencialidad de la información.

Artículo 14. Todo proveedor que entregue o proporcione servicios y/o equipamiento informático al ITAIH 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 al instituto.

Artículo 15. Todo servicio y/o equipo 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, convenios o contratos del ITAIH.

CAPITULO V
PROTECCIÓN CONTRA CÓDIGO MALICIOSO (VIRUS Y MALWARE)

Artículo 16. Todo equipo de cómputo institucional debe contar con software antivirus y antimalware definido por la DTI, así como estar protegido por el firewall del sistema operativo. Si el software antivirus no cubre a la plataforma utilizada, el personal notificará a la DTI para buscar una alternativa de solución.
Los accesos a internet en cada unidad administrativa deberán tener activo un firewall, mismo que debe ser administrado por la DTI.

Artículo 17. Todo usuario que identifique una anomalía en su equipo de cómputo deberá reportarla de inmediato al al DTI, según corresponda, para su inmediata atención.

CAPITULO VI
SERVICIOS INFORMÁTICOS EN LA RED

Artículo 18. Todo el personal y terceros son responsables del buen uso de los servicios informáticos alojados en las instalaciones de la DTI y en la nube, asignados para realizar sus funciones administrativas.

Artículo 19. Sólo el Personal del la DTI queda facultado para acceder a los equipos de cómputo institucionales, para:

- Ejecutar las tareas del procedimiento de mantenimiento preventivo y correctivo.

- Realizar modificaciones al Sistema Operativo.
- Realizar una revisión de seguridad informática y descartar uso indebido (daños intencionales a información o hardware) del equipo de cómputo.

Artículo 20. 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 21. 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 19 del presente documento.

Artículo 22. Los sistemas institucionales deberán ser accedidos con cuentas que permitan identificar al usuario y deberán estar protegidas con contraseñas seguras. El desarrollo, implementación y vigilancia del acceso seguro en los sistemas institucionales será responsabilidad de la DTI.

Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información del ITAIH, 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 la DTI, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los usuarios.

Artículo 23. 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 DTI.

Artículo 24. El equipo de cómputo institucional (computadoras de escritorio y portátiles), será configurado solamente por personal de la DTI para brindar acceso a la red institucional. 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 25. A toda persona que deje de laborar o tener relación con el ITAIH, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. La Dirección de Administración y Finanzas comunicará a la DTI, toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de acceso a los servicios de red y comunicación.

Artículo 26. Todo hardware y software de uso administrativo que sea considerado de riesgo para la seguridad de los servicios informáticos institucionales deberá ser utilizado en ambiente aislado.

Son considerados Hardware de riesgo, de manera enunciativa más no limitativa, los routeadores, switches, servidores, firewalls, balanceadores de carga y módems.

Son considerados softwares de riesgo, de manera enunciativa más no limitativa, los analizadores de tráfico de red, herramientas de análisis y diagnóstico de equipos de cómputo y los demás que determine la persona encargada de la DTI.

CAPITULO VII
USO DE CUENTAS DE USUARIO

Artículo 27. El acceso a los sistemas institucionales de información y correo electrónico será a través de una cuenta institucional, compuesto por nombre de usuario y contraseña

Artículo 28. Toda solicitud de alta, baja o cambio de privilegios de cuentas de personal administrativo, para acceder a los servicios informáticos debe ser realizada por el jefe inmediato o jefe de área, debidamente justificado.

Artículo 29. Todo usuario debe actualizar la contraseña de su cuenta de acceso a los servicios informáticos por lo menos una vez al año o cuando sospeche que pueda estar comprometida.

Artículo 30. Cuando se requiera acceder a información de un equipo de cómputo de una persona ausente, ya sea por cuestiones de salud, por estar comisionado en actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar al encargado de la DTI que, se brinde el acceso correspondiente para poder dar continuidad a algún proceso institucional. El personal encargado de la DTI 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, se ausenta en la Institución o cambia de puesto, el jefe inmediato podrá solicitar a la DTI el acceso al equipo institucional que ésta tenía asignado, el cual es concedido para que sustraiga la información pertinente.

CAPITULO VIII
MONITOREO DEL USO DE LOS SERVICIOS INFORMÁTICOS

Artículo 31. El personal de la DTI realizará periódicamente revisiones de hardware y software del activo informático institucional, para dar atención a problemas de obsolescencia y revisiones de licenciamiento. Además, monitoreará los servicios informáticos de red para administrar el uso del recurso de internet y solucionar cualquier problema detectado.

Artículo 32. 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 administrativas en el ITAIH.

Artículo 33. Todo responsable de área puede solicitar la restricción total o parcial de acceso a Internet de los equipos de cómputo asignados al personal a su cargo, considerando para ello las funciones laborales que éstos realizan.

Artículo 34. Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio, debe de omitir descargar archivos de páginas de internet de dudosa procedencia, que pongan en riesgo la información del equipo de cómputo de la persona, e incluso de la Institución derivado de virus o software malicioso.