Plan Institucional de Tecnologías de Información 2022

ÍNDICE

INTRODUCCIÓN

Actualmente los requerimientos de seguridad que involucran a las tecnologías de la información han cobrado gran auge de manera global sobre todo cuando se tiene conexión a internet y se deben erradicar los riesgos que amenazan a los sistemas computarizados.

Por lo anterior, el Instituto Tecnológico Superior del Occidente del Estado de Hidalgo en función con el área encargada de las Tecnologías que tiene la responsabilidad de gran parte de los recursos de TI y control de operaciones, se identificó la necesidad de normar el uso adecuado de estas destrezas tecnológicas para evitar su uso indebido y problemas en los sistemas informáticos y de comunicaciones del instituto.

De esta manera, estos lineamientos de seguridad para tratan sobre la seguridad desde un punto de vista general, contemplando, además de la propia información, aspectos tales como el hardware, el software, las redes, los datos y el personal que manipula o da soporte a esta Infraestructura de TI que servirán de instrumento y apoyo para dar a conocer la importancia y sensibilidad de la información.

Los presentes lineamientos deberán seguir un proceso de actualización cuando sea necesario sujetos a los cambios institucionales relevantes: crecimiento de la plantilla de personal, cambio en la infraestructura informática, desarrollo de nuevos servicios, entre otros.

OBJETIVOS

General

Establecer los lineamientos de trabajo con el fin seguir los procedimientos adecuados para proporcionar seguridad en el manejo y resguardo de información e infraestructura para la protección eficaz y eficiente, mediante un enfoque preventivo, defectivo, y operativo del uso de la información del instituto.

Específicos

- Dar a conocer al personal técnico sobre los procedimientos y normativas a seguir en el uso de sistemas informáticos y de comunicaciones.
- Exponer al personal operativo los lineamientos que se pueden y deben seguir para el manejo adecuado de software y hardware.

ALCANCE

Las políticas o lineamientos aplican para todos los servidores públicos, proveedores, sistemas informáticos, software, documentación o información, equipos y demás recursos de tecnológicos utilizados por los usuarios del Instituto.

POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad informática son reglas que deben cumplir los usuarios que tienen acceso a los activos de tecnología e información del instituto que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que puedan afectar el desarrollo de sus actividades.

Estas políticas no solo van destinadas a los equipos técnicos e informáticos de la organización, sino a todos los miembros del Tecnológico que sean susceptibles a producir algún error o descuido de seguridad.

Inventario de activos

Se debe llevar un inventario centralizado y actualizado de los recursos de Tecnología de Información de la institución, así como contar con mecanismos de control según el tipo de información que contienen, procesan, transfieren, transportan o almacenan.
Así mismo, los activos se deben clasificar según su naturaleza: activos físicos, activos de información, activos de servicios y activos personales.

Responsabilidades Administrativas

El encargado de TI debe determinar las responsabilidades explícitas para implementar, operar y administrar los controles de Seguridad Informática.

Capacitación del Personal en materia de Seguridad de la Información

El encargado de TI debe considerar en su plan de trabajo el proporcionar a los servidores públicos responsables de Tecnologías de la Información y Comunicaciones, programas de concientización, educación y capacitación adecuados en función de las necesidades, para que estos a su vez lo transmitan hacia los usuarios de los activos de información.

El personal debe recibir capacitación periódica al menos una vez al año para concientizar sobre los problemas de seguridad de la información.

Los usuarios deben recibir capacitación periódica una vez al año) para concientizar sobre la cultura de seguridad de la información.

Deben existir métodos que permitan afianzar la cultura de seguridad en el personal como:

- Correos electrónicos.
- Promover pláticas y vídeos de seguridad.
- Promover carteles o trípticos en materia de seguridad.

RESPONSABILIDADES DEL ÁREA DE SEGURIDAD INFORMÁTICA

Principios Generales

Todos los directivos y el personal del instituto tienen la responsabilidad de proteger la seguridad de los activos y de los recursos de TI bajo su control, de acuerdo con las instrucciones y la capacitación recibidas. Deben definirse responsabilidades expresas para la implementación, operación y administración de los controles de seguridad informática.

Responsabilidades

- Desarrollar, revisar y actualizar las políticas y normas se seguridad informática.
- Coordinar la implementación de las políticas y normas del Área de Seguridad Informática del instituto.

- Monitorear e informar sobre el trabajo de seguridad informática al encargado de TI.
- Dar asesoramiento sobre la seguridad física de todas las instalaciones del instituto.
- Investigar los aspectos penales de las violaciones de la seguridad informática, cuando sea necesario.
- Garantizar que la seguridad de todos los activos de informáticos y de comunicaciones.
- Garantizar que se le dé la prioridad correspondiente al trabajo de seguridad informática, de manera oportuna, en todos los proyectos de TI.

Personal

Todos los servidores públicos son responsables de:

- Cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad específicas documentadas.
- Mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados.
- Proteger la seguridad de los equipos de cómputo, así como de la información bajo su control directo.
- Informarle a la directiva inmediata o de seguridad cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de la misma, incluyendo sospechas de divulgación de contraseñas.

Terminación de Contrato

Al momento de notificar la terminación del contrato de un empleado por cualquier motivo y en cualquier circunstancia, el encargado de TI debe considerar:

- Eliminar los derechos de acceso a los sistemas informáticos, cuentas de correo electrónico, acceso a Internet, aplicativos y demás oportunidades en las que pueda existir un uso no autorizado de los sistemas del instituto.
- Se deben de remover los controles de acceso del empleado o terceros contratados como son: Remover el acceso a servicios de red.

- Verificar que los servidores públicos del y terceros contratados, regresen los activos propiedad de la organización utilizados durante su trabajo en el tiempo que duro su contrato, como: software, hardware, equipo de oficina, documentos corporativos, información en medios electrónicos y credenciales de accesos.

SEGURIDAD FÍSICA

Principios generales

Las instalaciones como site de comunicaciones y los IDFs que tienen fines específicos para albergar equipos que requieren mayor protección que la proporcionada a las oficinas comunes y deben considerarse como confidenciales y protegerse de manera acorde.

Construcción y emplazamiento de instalación de TI

Las instalaciones donde se alberguen los equipos de TI deben ser ubicadas y diseñadas de forma tal que se reduzcan los riesgos resultantes de desastres naturales, los inherentes a la zona circundante, y riesgos de otra naturaleza, y no deben llamar la atención innecesariamente sobre dicha finalidad.

Siempre debe solicitarse el consejo de los asesores en construcción, prevención de incendios y seguridad que correspondan, y cumplir con sus recomendaciones, incluyendo también los requerimientos legales y los códigos de prácticas correspondientes.

En la medida de lo posible, las instalaciones de TI deberán emplazarse y construirse a fin de reducir:

- El acceso directo público o el acercamiento directo de vehículos.
- El riesgo de inundaciones y otros peligros inherentes a la zona circundante y el medio ambiente.
- La cantidad de vías de acceso a las instalaciones, contando con áreas de entrega, carga y depósito controladas por separado.
- Los riesgos potenciales en el suministro de energía eléctrica, agua y de servicios de telecomunicación.

Protección contra incendio y explosión

Las medidas de prevención de incendios y explosiones deben incluir:

- Las medidas de prevención de incendios en los planos de las instalaciones tan pronto comiencen la construcción de las mismas.
- La implementación de las recomendaciones correspondientes hechas por los fabricantes de los equipos.
- Además de los dispositivos manuales esenciales, la instalación de sistemas
- automáticos de detección y extinción de incendios, los cuales deben ser supervisados las 24 horas del día siempre que sea posible.
- Capacitación adecuada en el uso de los equipos de extinción de incendios. Todo procedimiento relacionado debe ser documentado, evaluado, publicado y puesto en práctica.
- Eliminación de material inflamable, por ejemplo, papeles y artículos de papelería de desecho, de los centros de cómputos o equipos de computación, o de otros lugares que representen un peligro potencial de incendio, a menos que se lo requiera para el trabajo programado.

Protección contra daños provocados por el agua

Para proteger los equipos contra el agua se debe utilizar sistemas de alarma, contar con techos y pisos impermeables y un sistema de drenaje adecuado.

Control Ambiental

La temperatura, la humedad y la ventilación dentro de las instalaciones que albergan equipos de computación y de comunicaciones y medios de almacenamiento de información debe cumplir con las normas técnicas estipuladas por los fabricantes de los equipos. Cuando sea necesario, debe vigilarse la calidad ambiental y tomar las medidas correctivas pertinentes.

Suministros de energía eléctrica

Los suministros de energía eléctrica deben cumplir con las normas técnicas estipuladas por los fabricantes de los equipos. Cuando sea necesario, debe vigilarse la calidad del suministro de energía eléctrica y tomar las medidas correctivas pertinentes.

Debe proporcionarse a los sistemas críticos una fuente alternativa de energía eléctrica adecuada, por ejemplo, generadores de reserva, y si fuera necesario, una fuente ininterrumpida de energía eléctrica (UPS). Deben probarse periódicamente las fuentes alternativas de energía eléctrica.

LINEAMIENTOS DE CONTROLES DE ACCESO FÍSICO

Debe protegerse la seguridad física de las instalaciones y del personal de TI mediante los siguientes controles:

- Ningún usuario puede tener acceso al Centro de Datos sin previa autorización del área responsable.
- Se utilizará sistemas automatizados de control de acceso físico para que solamente el personal autorizado pueda acceder a las áreas de seguridad.
- Los usuarios autorizados deben portar una identificación visible dentro de las áreas de seguridad.
- Cuando corresponda, deben mantenerse en secreto los códigos de acceso de las cerraduras digitales, los cuales deben cambiarse periódicamente y cada vez que un miembro del personal ya no necesite tener acceso.

Visitantes

Los procedimientos aplicados para la recepción de todos los visitantes en las instalaciones u oficinas de TI deben:

- Confirmar y registrar efectivamente las identidades de los visitantes, las organizaciones a las que representen, y el objetivo de su visita antes de ser admitidos.
- Registrar las fechas y horarios de entrada y salida.

- Proporcionar a los visitantes gafetes distintivos, los cuales deberán portar durante su visita, y proporcionarles instrucciones básicas de seguridad y de prevención de incendios.
- Garantizar que los visitantes estén bajo observación y sean supervisados durante su Visita, en función de los riesgos.
- Minimizar el acceso de los visitantes a las áreas de seguridad.
- Deben firmarse los acuerdos de confidencialidad pertinentes que cubran a los individuos y a las organizaciones que los emplean.
- El acceso de los ingenieros a la Información confidencial debe ser el mínimo posible.
- Deben hacerse copias de resguardo de la información antes que los ingenieros tengan acceso a los sistemas o los equipos.

LINEAMIENTOS DE CONTROLES DE ACCESO A LA INFORMACIÓN

Principios Generales

El acceso a los sistemas e información importante debe estar restringido al personal autorizado, justificarse por requisitos y debe registrar identidad de usuarios.

Debe controlarse el acceso al sistema por medio de identidades de usuario y contraseñas secretas asignadas a usuarios autorizados.

El software de seguridad debe estar adecuadamente protegido contra acceso o modificaciones no autorizadas.

Esta norma aplica al acceso del personal del instituto a todos los tipos de sistemas y aplicaciones internas del mismo, incluyendo equipos de telecomunicación de información y voz, servidores, las PC y otras estaciones de trabajo.

Identidades de Usuarios

Las identidades de usuario deben identificar de forma única a un usuario individual.

Política para el uso de contraseñas

Se debe proporcionar el correcto diseño y uso de nombres de usuario y contraseñas dentro del instituto, así como establecer un estándar para la creación de contraseñas fuertes o robustas, su resguardo y la frecuencia de cambio.

Esta política incluye a todo el personal del tecnológico y responsables de las cuentas internas con acceso a herramientas o información confidencial, así

como para consolas de operación y servidores que se encuentren en las instalaciones.

Guías generales

Las contraseñas NO deben tener las siguientes características:

- Tener menos de 8 caracteres
- Ser palabras de diccionarios comunes
- Ser palabras comunes como:
    - Nombre de familiares, mascotas, amigos, compañeros, etc.
    - Nombre de marcas, compañías, hardware, software.
    - Cumpleaños, y otra información personal como dirección o teléfono.
    - No utilizar información personal, nombre de familiares, etc.
    - No utilizar el usuario como contraseña.
    - No escribirlas en papeles o agendas de fácil acceso, ni en archivos sin cifrar.
    - No habilitar la opción "recordar clave en este equipo ", que ofrecen los programas o navegadores.
    - No enviarla por correo electrónico

Las contraseñas robustas deberán seguir las siguientes características:

- Tener caracteres en mayúsculas y minúsculas
- Tener números y caracteres especiales.
- Utilizar al menos 8 caracteres alfanuméricos
- Las contraseñas No deberán ser almacenadas medios electrónicos.
- Las contraseñas deben ser creadas de tal manera que se puedan recordar utilizando algún tipo de algoritmo relacionado.

Resguardo de contraseñas

- No se deben compartir las contraseñas con ninguna persona, incluyendo asistentes o secretarias, todas las contraseñas deben ser tratadas como sensibles y confidenciales.
- Nunca revelar la contraseña a través de una conversación telefónica.
- Nunca revelar una contraseña a través de un correo electrónico.
- Nunca hablar de una contraseña en frente de otras personas
- Nunca revelar la contraseña a compañeros de trabajo en vacaciones, cada quien debe tener su cuenta propia.

Bloqueos por exceso de intentos fallidos

En donde la tecnología lo permita, se deberá implementar un control que límite a 3 intentos de acceso fallidos, después de los cuales se procederá a bloquear la cuenta en cualquiera de las dos formas siguientes:

- Por espacio de una hora con opción a restablecerla mediante la solicitud expresa al administrador, si la tecnología lo permite.
- De manera indefinida hasta que si el titular de la cuenta de acceso solicite el restablecimiento mediante el procedimiento autorizado.

Rotación programada de contraseñas

- Todas las contraseñas a nivel sistema (root, administrador, enable y cualquier cuenta con privilegios de administración) deberán cambiarse al menos cada tres meses.
- Cualquier tipo de contraseñas de usuario (email, web, computadora personal) deberán cambiarse al menos cada cuatro meses.

Responsables.

- Todo el personal del instituto es responsable de cumplir con esta política y el encargado de TI de vigilar su cumplimiento para poder aplicar las sanciones correspondientes a las violaciones de la política.

Transportación de la Información

Se deben implementar los controles apropiados para proteger a las partes involucradas contra fallas de seguridad durante la transportación de unidades de almacenamiento de información.

- Debe considerarse además el dividir el envío en varias partes para proteger la información confidencial.

LINEAMIENTOS DE SEGURIDAD FÍSICA

Equipos

Debe protegerse la seguridad de los equipos mediante las siguientes medidas generales:

- Deben guardarse los equipos bajo llave y asegurarlos cuando sean dejados sin supervisión. Cuando sea posible y adecuado para el riesgo, deben adaptárseles dispositivos contra manipulación indebida para minimizar la posibilidad de que el equipo sea removido o manipulado, que se instalen equipos en el área.
- No deben ubicarse los monitores ni las impresoras cerca de las ventanas, ni colocarlos de forma tal que puedan ser fácilmente observados;
- Prohibido comer, beber y fumar, así como el uso de teléfonos móviles/celulares en los centros de cómputo y oficinas.
- Los procedimientos deben garantizar que el mantenimiento de los equipos se lleve a cabo de acuerdo con las recomendaciones de los fabricantes.
- No puede conectarse equipo alguno a los sistemas o redes del instituto sin aprobación previa y, cuando se considere apropiado, bajo la supervisión del área de TI.

Cables

Siempre que sea posible:

- Las líneas eléctricas y de telecomunicaciones deben ingresar en las instalaciones de forma subterránea, con instalaciones alternativas disponibles desde otra fuente y a través de una ruta de ingreso independiente.

- Los cables deben ser enrutados e instalados de manera que se evite cualquier interferencia o daños accidentales o deliberados.

Medios de almacenamiento de datos y software

Deben protegerse los medios magnéticos mediante controles de seguridad física adecuados que incluyan el almacenamiento de la información o el software importante en gabinetes o cajas fuertes a prueba de fuego.

Escritorio despejado y entorno de trabajo

Deben adoptarse las siguientes medidas a fin de proteger la seguridad de las áreas generales de oficinas:

- Debe cerrarse sesión en los equipos de las oficinas cuando ya no se esté utilizando un equipo para que no sea usado sin autorización.
- Al final de cada jornada deben apagarse todos los equipos portátiles para minimizar el riesgo de robo y la pérdida potencial de información personal o delicada, deben guardarse bajo llave y en un lugar seguro todos los equipos portátiles durante la noche.
- Deben guardarse en un lugar seguro las llaves de los escritorios, gabinetes, cajas fuertes y otras instalaciones de almacenamiento similares, y proceder de igual manera con los registros de las combinaciones de las cerraduras digitales y cualquier otra información delicada similar. Además, deben implementarse los procedimientos establecidos para la manipulación y el almacenamiento seguro de las llaves.
- Fuera del horario de trabajo y cuando no se los utilice, deben guardarse en cajones o gabinetes con llave los documentos, papeles, disquetes, equipos de cómputo portátiles y otros artículos similares.
- Los pisos deben mantenerse libres de cajas, paquetes, equipos excedentes, etc. Para reducir los riesgos para el personal durante una evacuación de emergencia.

Protección del equipo fuera de las instalaciones

Todo el equipo que sea sacado de las instalaciones del instituto, incluyendo computadoras portátiles, unidades de almacenamiento, otros dispositivos electrónicos deben ser protegidos contra robo y pérdidas en todo momento. Debe protegerse la información del instituto con los controles de cifrado de información que se acuerden con el área de seguridad informática local. La provisión y utilización de equipos del tecnológico fuera de las instalaciones del mismo debe ser autorizado por los responsables de TI, tomando en cuenta los riesgos involucrados. El personal a cargo de los equipos del tecnológico utilizados fuera de las instalaciones del mismo son responsables de:

- Proteger la confidencialidad de la información.
- La seguridad física de ese equipo. Debe cumplirse con las recomendaciones de los fabricantes para la protección y manejo del equipo.
- Garantizar que el equipo sea utilizado sólo para los propósitos autorizados y por personal autorizado.
- Utilizar los controles de seguridad provistos con el equipo, tales como cerraduras físicas y sistemas de cifrado de archivos.
- Desconectar el equipo de las redes de telecomunicaciones cuando no se esté utilizando.

Eliminación de desechos y otros materiales

El material de desecho y los equipos excedentes de informática deben ser eliminados en forma segura. En particular:

- La papelería membretada del instituto y los papeles que contengan información confidencial del tecnológico y no deben ser reciclados como hojas de borrador fuera de las instalaciones.
- Debe borrarse toda información y software que permanezca aún en los equipos y dispositivos de almacenamiento de información, incluyendo las PC, los disquetes, CDROM, discos duros y USB antes que el instituto los deseche, incluyendo, si se le considera esencial, la destrucción física de las unidades de almacenamiento de datos.

- Los CD y demás unidades de almacenamiento que contengan información y software deben ser destruidos.
- Deben quitárseles todos los logotipos del tecnológico a los equipos y las unidades de almacenamiento de datos antes de desecharlos.

LINEAMIENTOS DE LA ADMINISTRACIÓN DE LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES

Principios Generales

La operación segura de los sistemas de información es fundamental
para la protección de los activos del instituto. Por lo tanto, los directivos de TI deben verificar que se haga uso correcto de los equipos y del software y que sólo se utilicen para los procesos autorizados.
Esta norma aplica para todos los tipos de sistemas y aplicaciones, incluyendo los equipos de telecomunicaciones de datos y de voz, los servidores, las PC y demás estaciones de trabajo.

Utilización de los equipos y sistemas

Los equipos y sistemas del tecnológico deben:

- Utilizarse solamente para los fines autorizados.
- Registrarse en inventarios actualizados.

Procedimientos y registros documentados

Deben documentarse los procedimientos para la operación de todos los sistemas informáticos y de comunicaciones, mismos que deben incluir:

- El inicio y el cierre de los sistemas.
- El mantenimiento, la depuración y el soporte técnico de los sistemas.
- La programación y operación de las tareas.

- El tratamiento de los archivos, los datos y la información de salida, incluyendo la protección de la información confidencial. Debe mantenerse un inventario de los archivos de datos más importantes.
- Las copias de resguardo de la información y los planes de contingencia;
- El registro y el monitoreo independiente del uso y operación de todos los equipos.
- La inspección periódica, ya sea por medios manuales o automáticos, del equipo de escritorio y cualquier otro equipo del que se considere que representan un alto riesgo (tal como el utilizado por los directores), para identificar todo software o dispositivos adicionados no autorizados, incluyendo módems no autorizados.
- La documentación debe ser guardada en forma segura y tratada como confidencial.
- Deben conservarse copias de resguardo de toda documentación esencial en un lugar aparte.

Resguardo de la Información

Los procedimientos de resguardo deben:

- Preparar la creación oportuna de copias de resguardo de toda la información y software que se requiera para respaldar las actividades esenciales y los planes de contingencia.
- Garantizar que todas las copias de resguardo de información y software sean documentadas correctamente, y que sean probadas con regularidad para garantizar que se puede contar con ellas en caso de emergencia.
- Ser integrados con los planes para garantizar la continuidad de las operaciones y los planes de contingencia de TI.
- Enviar la información de resguardo con prontitud y de forma segura a un lugar de almacenamiento remoto seguro.
- Retener suficiente información de resguardo generada para los requerimientos básicos, legales y regulatorios.

Administración de la capacidad

Deben planificarse y monitorearse los requerimientos de capacidad de los equipos servidores y equipos clientes a fin de evitar fallas debidas a una capacidad inadecuada de los sistemas informáticos y de comunicaciones.

Registro de fallas

Deben documentarse todas las fallas técnicas importantes detectadas en los sistemas informáticos y de comunicaciones. Los registros de fallas deben ser:

- Revisados por los encargados de TI a fin de garantizar que se diagnostiquen y resuelvan las fallas satisfactoriamente.
- Retenidos como evidencia para negociar una compensación y para otros fines similares con los vendedores de los equipos.

Deben revisarse las medidas correctivas, a fin de asegurarse que no se hayan comprometido los controles de seguridad y que se autorizó debidamente la medida correctiva adoptada.

Procedimientos en caso de incidentes de seguridad

Un incidente de seguridad es una falla en la confidencialidad, integridad o disponibilidad de la información que ha causado, o es probable que cause, algún daño material, financiero, de imagen o de cualquier otro tipo al tecnológico.

En caso de que se produzca una falla significativa en la seguridad informática, el directivo de TI debe:

- Registrar y documentar todos los hechos pertinentes respecto a la falla de manera tal que puedan ser aceptados como evidencia legal.
- Documentar en detalle todas las medidas de emergencia y recuperación del curso normal de las operaciones que hayan sido adoptadas.
- Revisar y fortalecer a la brevedad los controles de seguridad informática a fin de evitar la recurrencia de la falla.

LINEAMIENTOS DEL SOFTWARE

Software

Todo uso de software debe contar con una autorización y en cumplimiento de las licencias vigentes cuando se requiera:

- Los servidores públicos no pueden escribir, ingresar o usar ningún software a menos que esto haya sido autorizado y aprobado por el directivo de TI;
- Para evitar dudas, se prohíbe el uso del software que se enlista a continuación, a menos que se cuente con la autorización explícita de los encargados de TI para circunstancias específicas:
    - Software de juegos y recreación de cualquier tipo, incluyendo aquellos que formen parte de paquetes de software autorizados.
    - Cualquier software no autorizado que haya sido obtenido de Internet.
    - Software no solicitado sin importar de que fuente provenga.
    - Software creado por un empleado actuando como individuo y que no haya sido aprobado por el instituto.
    - Copias sin licencia de software autorizado.
- Todo uso y administración del software comprado debe ser acorde con los contratos de licencia y copyright respectivos.
- Deben guardarse las copias maestras del software y sus licencias en lugar seguro y tenerlas disponibles para su inspección si fuera necesario.
- Debe protegerse el software contra accesos o modificaciones no autorizadas mediante la utilización de controles automatizados de procedimientos que abarquen la administración de cambios y problemas y las nuevas versiones de software.
- La administración debe garantizar que el software haya sido probado adecuadamente antes de confiarle el procesamiento de las operaciones de las áreas del instituto.
- Deben aplicarse los parches de seguridad más recientes con los que cuente el proveedor del software.

Controles Antivirus

Debe utilizarse un sistema estándar de detección de virus actualizado de la DGSEI automáticamente para:

- Escanear todos los archivos que ingresen en el entorno informático del instituto por email, medios extraíbles o cualquier otra fuente externa tal como el Internet para identificar, informar y, si se considera necesario, eliminar virus informáticos en la primera oportunidad que se tenga.
- Escanear y, si fuera necesario, corregir o mantener en cuarentena todos los archivos enviados a los usuarios, proveedores y otras contrapartes externas por e-mail u otros medios para asegurarse de que el tecnológico no esté distribuyendo virus sin saberlo.
- Actualizar el las definiciones antivirus por lo menos una vez a la semana.
- Ejecutar por lo menos una vez a la semana el antivirus instalado en el equipo de cómputo.
- El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
- Las carpetas compartidas, dentro de una Red, deben tener una clave de acceso, la misma que deberá ser cambiada periódicamente.
- El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca parches de seguridad, atractivos premios o temas provocativos.
- Verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.
- No instalar productos que se descargan de Internet, ya que son una potencial vía de propagación de virus.
- Evitar ejecutar o abrir archivo con doble extensión.
- Si el antivirus detecta un archivo infectado que no puede ser reparado, entonces debe ser eliminado.

- Realizar respaldos de seguridad de la PC al menos una vez por mes.

Los ataques de virus significativo deben ser considerados incidentes de seguridad y tratados en consecuencia.

LINEAMIENTOS DE LA UTILIZACIÓN DE RECURSOS DE REDES

Administración de redes

Los equipos de comunicaciones están sujetos a las mismas normas de seguridad que otros equipos y sistemas de TI. Deben utilizarse controles de acceso a la red de comunicaciones y de enrutamiento de mensajes para complementar los controles implementados en el equipo conectado a las redes de comunicaciones. En particular:

- Cada una de las conexiones entre los sistemas del tecnológico y servicios externos, incluyendo conexiones inalámbricas, LAN y de acceso telefónico, debe tener la autorización individual de los encargados de TI.
- Cuando se haga uso del acceso telefónico, debe identificar y validar a los usuarios remotos, la devolución de llamadas (*dial-back*), el acceso a los sistemas, los controles de pistas de auditoria y la utilización de SSH en lugar de telnet.
- No se permite la creación de cuentas de usuario locales dentro de los ruteadores.
- La contraseña de enable para el ruteador debe mantenerse cifrada.
- Deshabilitar el IP directed broadcast.

Conexiones de Internet

El área responsable de las Tecnologías de la Información del tecnológico, debe implementar un conjunto completo y autónomo de controles para proteger la seguridad de la información que se transmite a través de la Internet. Esta norma aplica a cualquier servicio externo que sea prestado utilizando el protocolo de Internet (IP).

Todos las demás normas y principios de control aplican de igual manera para las aplicaciones de Internet, y en particular:

- Todas las conexiones de computadoras del instituto a servicios de Internet deben estar justificadas por las necesidades del área y contar con la aprobación de esta última y

el acceso a las mismas debe estar restringido a usuarios autorizados para fines autorizados;

- Está prohibido utilizar servicios de Internet que no cuenten con el permiso expreso del área de TI.
- Está prohibida la navegación en sitios de contenido pornográfico, juegos, chats, ocio y todo aquellos que no sea justificable para el buen desempeño de las labores del Servidor Público.
- El área de Tecnologías de la Información inhabilitará todas las direcciones de Internet que cumplan con lo expuesto en el punto anterior, a medida que estas sean consultadas.
- No debe transmitirse información confidencial o referida a valores a través de la Internet sin antes aplicar controles adicionales (cifrado, por ejemplo);
- Los equipos de la DGSEI conectados a servicios de Internet deben ser autónomos o bien estar ubicados en una zona DMZ protegida por *firewalls* autorizados;
- Es responsabilidad del área de Tecnologías de la Información o en su caso de los proveedores de internet mantener un dispositivo firewall entre la zona DMZ y la Internet.
- Todos los servidores que se encuentren en el centro de datos y aquellos que se pretendan ingresar al mismo y conectar a la red de la DGSEI deben:
    - Ejecutar sólo los procesos mínimos necesarios para llevar a cabo sus funciones. Mismos que serán notificados por parte del responsable del equipo para poder adecuar los controles de acceso al mismo.
    - Toda administración remota deberá realizarse a través de canales cifrados.
    - Todo servidor ubicado en la zona DMZ debe tener los registros apropiados en el DNS (al menos un registro A).
    - La operación de controles de firewall debe estar sujeta a pruebas con regularidad, así como a monitoreo automatizado.
    - Todo cambio en la configuración del firewall, elementos como switches, ruteadores, y concentradores debe ser notificada al Área responsable del tecnológico.

- Cualquier cambio en la configuración de los servidores deberá notificarse al Área de TI.

Uso de Internet:

El acceso a y el uso de Internet se suministra personalmente a individuos dentro del tecnológico como una herramienta con fines laborales.

El acceso a internet y al correo electrónico no debe ser utilizado para los siguientes propósitos expresamente prohibidos:

- No tienen el fin de ser usado para correspondencia externa de naturaleza personal.
- Mensajes ilegales, difamatorios u ofensivos, prejuicios u hostigamiento ya sean raciales, sexuales o de cualquier otro tipo,
- Acciones perjudiciales, su reputación o su acceso a Internet (insulto, difusión abusiva, etc.) para la baja de pornografía, juegos
- de software u otro material lascivo o frívolo,
- Para obtener o comprar software ejecutable (.exe) sin aprobación previa específica o material de vídeo, audio o musical, salas para charlas, tampoco para emisión de cualquier aviso comercial no autorizado formalmente.
- Compromiso legal asumido por correo electrónico a favor de cualquier miembro de la organización, ni para la conclusión de cualquier forma de acuerdo contractual de trabajo.

LINEAMIENTOS DE DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Principios Generales

Los requisitos de seguridad informática de sistemas de aplicaciones deben ser administrados por los desarrolladores de sistemas a lo largo de todas las etapas del desarrollo del sistema como parte de todos los demás requisitos y sobre la misma base que estos, para optimizar la efectividad y el costo de los controles de seguridad.

Delimitación de actividades

Deben separarse las responsabilidades y funciones de desarrollo y mantenimiento de sistemas de aplicaciones de aquellas destinadas a la operación de sistemas de producción.

Análisis y especificaciones de los requisitos de seguridad

Los requisitos del área para controles de seguridad informática, así como las soluciones seleccionadas, deben ser claramente documentadas por todos los proyectos de desarrollo de sistemas. Esta información debe ser ordenada en un documento por separado para todos los proyectos de tecnológico.

Los proyectos que implementen paquetes de software comprados deben incluir los requisitos de seguridad para la selección de los productos y el proceso de obtención del mismo. El diseño de los sistemas debe tomar en consideración los requisitos de las aplicaciones para:

- Los controles específicos de acceso de las aplicaciones basados en contraseñas de sistema e identidades de usuario, y la estructura y presentación de los menús de las aplicaciones.
- El cifrado de extremo a extremo u otra información de control de seguridad.
- El cumplimiento con la legislación y regulación correspondiente, incluyendo la relacionada con la protección y privacidad de la información, y otras regulaciones, incluyendo la utilización de pantallas de terminal al momento que el usuario inicie la sesión ("*banners* de inicio de sesión").
    - Alimentación automática de datos y archivos de datos.
    - Identificación y autenticación de los usuarios.
    - Autorización de transacciones.

Pruebas

Deben probarse los controles específicos de seguridad informática de las aplicaciones como parte integrante de los planes de prueba de proyectos, y deben estar sujetos a la aceptación por escrito al igual que a otros requerimientos de los sistemas.

Siempre que sea posible, la información en tiempo real no debe ser usada para fines de pruebas y capacitación. En caso de ser utilizada, entonces:

- Los procedimientos de prueba deben garantizar que los riesgos asociados no sean mayores que los aceptados por los sistemas de producción;
- Debe contarse con el consentimiento previo de la Dirección.
- Todos los vaciados de memoria de almacenamiento y las salidas de datos para fines de diagnóstico o pruebas que pudieran contener información confidencial deben ser eliminados de forma segura.

Seguridad de la información y la documentación del proyecto

Durante todo el proceso de desarrollo:

- El software, la información y la documentación del desarrollo de los sistemas debe ser considerada confidencial.
- Deben ejercerse la administración de cambios y los controles de acceso apropiados para la información y la documentación del proyecto.
- Deben aplicarse procesos documentados de administración de configuración y cambios a la transición entre los proyectos de desarrollo y la puesta en marcha de la producción.

Copyright del software

El software está sujeto a la ley del derecho de propiedad intelectual, diseños y patentes. Por lo general, para los fines de la ley del derecho de propiedad intelectual el software es considerado como obra literaria, con las obligaciones de titularidad y propiedad intelectual respectivas. No se debe copiar, modificar o utilizar el software en contravención de las condiciones de la licencia.

La política del Instituto estipula que es el titular de todo el software y los programas diseñados por los servidores públicos en el desempeño de sus funciones, debiendo incluirse en el código de dichos programas las declaraciones correspondientes referidas al derecho de propiedad intelectual.

Todos los titulares de los programas, así como las etiquetas de los medios de almacenamiento que contengan software de la organización deben llevar la siguiente leyenda:

LINEAMIENTOS DE SISTEMAS DE COMUNICACIONES

Principios generales

Los sistemas de envío y recepción de mensajes se utilizan no sólo para las comunicaciones internas, sino también para las comunicaciones externas dirigidas a las demás dependencias del Tecnológico, proveedores y otras organizaciones. La información guardada en los sistemas de envío y recepción de mensajes es una parte importante de los registros del instituto. Por lo tanto, debe protegerse la seguridad de la información almacenada en dichos sistemas por medio de controles coherentes.

Sistemas telefónicos

Los sistemas telefónicos, los intercambios privados entre dependencias y los conmutadores respectivos son sistemas informáticos que deben protegerse en consecuencia.

Un aspecto que preocupa en particular es la protección de la información confidencial y otros tipos de información personal. En particular:

- Deben protegerse los equipos de control telefónico mediante controles de acceso físico.
- Debe regularse el mantenimiento y soporte administrativo mediante controles de acceso con contraseñas y, cuando corresponda, controles adecuados sobre las comunicaciones para mantenimiento en las redes.
- No deben utilizarse teléfonos celulares para transmitir información confidencial.

Correo electrónico (e-mail)

Los Servidores Públicos sólo podrán utilizar el servicio de correo electrónico interno de los servidores mail.itsoeh.edu.mx para los siguientes propósitos:

- Anunciar eventos, actividades, reuniones o seminarios de interés general y que estén relacionados directamente con la institución educativa.
- Enviar y recibir documentos de índole laboral, los cuales faciliten las actividades diarias de los Servidores Públicos.
- El envío de mensajes masivos a través de correo electrónico debe ser realizado sólo con aprobación de un superior.
- Se obtendrán copias impresas de cualquier mensaje de correo electrónico que deba ser retenido con fines reglamentarios u otros propósitos legales,
- Los Servidores Públicos **NO** podrán utilizar los servicios de correo electrónico para los siguientes propósitos:
    - Enviar mensajes donde se suplante la identidad del remitente del mensaje.
    - Evitar contestar mensajes no solicitados o de fuente desconocida, ya que al hacerlo se reconfirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos (Hoaxes), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.
    - Consultar y distribuir información privada, sin la debida autorización del dueño de la cuenta.
- La información confidencial no debe ser transmitida por correo electrónico, a menos que se ha autorizado, en cuyo caso los archivos deben viajar en forma encriptada.
- Los servidores públicos no deben enviar mensajes de correo electrónico con contendidos hostiles que molesten a los receptores del mismo, como comentarios sobre sexo, raza, religión o preferencias sexuales, así mismo cuando un empleado reciba este tipo de mensajes deben comunicarlo a su jefe inmediato y al área encargada de personal.
- El sistema de correo electrónico de la entidad debe ser usado únicamente para propósitos de trabajo. Todos los mensajes enviados por este medio pertenecen a la entidad y ésta se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.

Elaboró	Revisó	Autorizó
Lic. Noé Israel Azpeitia García Soporte Técnico	Lic. Eliel Olvera Gómez Encargado de la Subdirección de Planeación	Mtro. Luis Armando Officer Arteaga Director General