Dirección de Planeación

Políticas para la Seguridad Informática
Instituto Nacional de Perinatología
"Isidro Espinosa de los Reyes"

Unidad Responsable:

Departamento de Tecnologías de la Información

Agosto 2018

Contenido

Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad en Informática comienza con establecer y difundir las políticas para su aplicación.

La Seguridad en Informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas que cubran las necesidades del Instituto en materia de seguridad.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

1. Seguridad de Personal
2. Seguridad Física y Ambiental
3. Seguridad y Administración de Operaciones de Cómputo
4. Controles de Acceso Lógico
5. Cumplimiento

En apego al Manual de Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, publicado por la Secretaria de Función Pública, el Departamento de Tecnologías de la Información del Instituto Nacional de Perinatología "Isidro Espinosa de los Reyes elaboró las presentes *Políticas para la Seguridad Informática* con la finalidad *de* proteger la infraestructura computacional y todo lo relacionado con ésta, la cual incluye la información contenida.

Objetivo

El presente documento tiene como finalidad dar a conocer las políticas para la seguridad informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información del Instituto Nacional de Perinatología Isidro Espinosa de los Reyes,

Marco - Jurídico Administrativo

La "Ley General de Responsabilidades Administrativas", en su Artículo 49 del Título Tercero de las faltas administrativas de los servidores públicos y actos de particulares vinculados con faltas administrativas graves Capítulo I De las Faltas administrativas no graves de los Servidores Públicos.

La "Ley Federal de Derechos de Autor", que tipifica como delito el que reproduzca, distribuya, venda o arriende un programa de computación sin autorización del titular de los derechos de autor; así como lo que establece el texto del artículo 103 "Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a éste" así corno lo establecido en el Artículo 105 "El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando: I.- Sea

indispensable para la utilización del programa, o II.- Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación".

Y en caso de incumplir las presentes disposiciones, el responsable o responsables se podrán hacer acreedores a una sanción, de acuerdo a lo establecido en el Artículo 231 Título XII, Capítulo II "Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:..." VII. Usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular" y en el Artículo 232 del Título XII, Capítulo II. De las Infracciones en materia de comercio de la mencionada Ley, y en materia de comercio previstas en la presente Ley, serán sancionadas por el Instituto Mexicano de la Propiedad Industrial como multa: I. De cinco mil hasta diez mil días de salario mínimo en los casos previstos en las fracciones I, III, IV, V, VII, VIII y IX del artículo anterior.

La Ley Federal de Transparencia y Acceso a la Información Pública", Artículo 186, Frac. IV, que señala la responsabilidad administrativa de los servidores públicos por "Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de manera indebida información que se encuentre bajo su custodia, a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión"

La "Ley General de Transparencia y Acceso a la Información Pública", Artículo 206, Frac. IV, que señala la responsabilidad administrativa de los servidores públicos por "Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, sin causa legítima, conforme a las facultades correspondientes, la información que se encuentre bajo la custodia de los sujetos obligados y de sus Servidores Públicos o a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión".

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Artículo 3 señala que "Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Así como demás normatividad aplicable en la materia.

Alcance

El documento describe las políticas de seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos del Instituto.

Justificación

El DTI está facultado de acuerdo a su objetivo y funciones, el definir normas y procedimientos para el uso, manejo y conservación del equipo de cómputo y comunicaciones.

Definiciones

Abreviatura:	Definición:
Instituto	Instituto Nacional de Perinatología "Isidro Espinosa de los Reyes"
DTI	Departamento de Tecnologías de la Información
Políticas	Políticas para la Seguridad Informática
Usuario (s)	Servidores Públicos que se encuentren laborando en las instalaciones del Instituto Nacional de Perinatología "Isidro Espinosa de los Reyes"

Sanciones por incumplimiento

El incumplimiento a las presentes Políticas podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Beneficios

Las políticas establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información del Instituto.

1. SEGURIDAD DE PERSONAL

Política

Todo usuario de bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información y de su uso adecuado de los recursos informáticos del Instituto.

Los usuarios deberán cumplir con lo señalado en estas Políticas las cuales fueron diseñadas para observancia y aplicación dentro de las instalaciones del Instituto.

Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir con las presentes Políticas para la Seguridad Informática establecidas para el buen funcionamiento en materia tecnológica.

Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos del Instituto deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información del Instituto, así como comprometerse a cumplir con lo establecido en las presentes Políticas.

Entrenamiento en Seguridad en Informática

Por medio del Departamento de Capacitación, Calidad y Desarrollo de Personal dependiente de la Dirección de Administración y Finanzas, en específico en su curso de Inducción, se solicitará hacer del conocimiento del

personal de nuevo ingreso que para conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento a los servicios informáticos, deberán consultar las Políticas para la Seguridad Informática, a través de la página web www.inper.mx o en la intranet institucional.

Medidas disciplinarias

Cuando el DTI identifique el incumplimiento a estas Políticas podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial del Instituto, o de que se le declare culpable de un delito informático consideramos entre algunos como:

- Falsificación informática mediante la introducción, supresión o borrado de datos informáticos.
- Fraude informática mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos

2. SEGURIDAD FÍSICA Y AMBIENTAL

Política

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Instituto.

Proteger el equipamiento de procesamiento de información crítica del Instituto ubicándolas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Instituto.

Implementar medidas para proteger la información manejada por el personal en las oficinas en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Adoptar controles adecuados de acceso para minimizar el riesgo de amenazas potenciales, como robos, sustracciones, etc. Por lo que solo personal autorizado del DTI tendrá acceso a las instalaciones y áreas restringidas del Instituto para salvaguardar algún bien o movimiento dentro del área o del Instituto.

Además de la protección de la información y la seguridad de los sistemas, tiene como objeto asegurar la continuidad de la información, que deben actuar coordinadamente evaluando y tratando los riesgos para implementar medidas con el fin de minimizar el impacto ante un incidente de seguridad de la información. Si bien los términos seguridad de la información tienen distintos significados, es necesario que converjan con el fin de proteger la Confidencialidad, Integridad y Disponibilidad de la Información

Resguardo y protección de la información

El usuario deberá reportar de forma inmediata al DTI, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

El usuario tiene la obligación de proteger los discos, disquetes, cintas magnéticas y CDROM que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad del usuario evitar en todo momento la fuga de la información del Instituto que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Es responsabilidad del usuario el mantener un respaldo actualizado de la información almacenada en el equipo de cómputo asignado.

Controles de acceso físico

Cualquier persona que tenga acceso a las instalaciones del Instituto, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del Instituto, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente en la Oficina de Activo Fijo cuya área de adscripción es el Departamento de Almacén, Farmacia e Inventarios.

Las computadoras personales, las computadoras portátiles, módems, y cualquier activo de tecnología de información, podrá salir de las instalaciones del Instituto únicamente con la autorización de salida del Departamento de Almacén, Farmacia e Inventarios, de acuerdo a lo establecido en el Manual de Procedimientos de dicho Departamento.

Seguridad en áreas de trabajo

El centro de cómputo (SITE) del Instituto es área restringida, por lo que sólo el personal autorizado por el DTI puede acceder a él.

Protección y ubicación de los equipos

Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del DTI, en caso de requerir este servicio deberá

notificarlo al mismo Departamento por escrito y con visto bueno de su Director de Área, con copia al Departamento de Almacén, Farmacia e Inventarios.

El área de Activo Fijo adscrita al Departamento de Almacén, Farmacia e Inventarios será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas en el Instituto.

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Es responsabilidad de los usuarios almacenar la información únicamente en la carpeta de disco duro identificado como "Disco local (D:)", para que en caso de que se dañe el sistema operativo no se pierda la información, ya que las otras están destinadas para archivos de programa y sistema operativo.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

Se debe mantener el equipo informático en un entorno limpio y sin humedad.

El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados por escrito con una semana de anticipación al DTI a través de un plan detallado de movimientos debidamente autorizados por el Director del área que corresponda.

Queda prohibido que el usuario abra o desarme los equipos de cómputo.

Mantenimiento de equipo

Únicamente el personal autorizado por el DTI podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

Pérdida de Equipo

El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

El usuario deberá dar aviso inmediato a las áreas de Asuntos Jurídicos, de Tecnologías de la Información, de Activo Fijo y de Servicios de la desaparición, así mismo levantará un acta del robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

Uso de dispositivos especiales

El uso de los grabadores de discos compactos y DVD es exclusivo para copias de seguridad de software que esté bajo contrato de licencia en el Instituto, para respaldos de información que por su volumen así lo justifiquen y para la generación de información para entregar a terceros institucionales.

El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

Queda prohibido el uso de módems, switches, routers externos en las computadoras de escritorio.

Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por su Director de área.

Los módems internos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones del Instituto para conectarse a ningún servicio de información externo.

Daño del equipo

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso el DTI determinará la causa de dicha compostura.

3. ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura tecnológica del Instituto. De igual forma, deberán proteger la información reservada o confidencial

que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del Instituto o hacia redes externas como Internet.

Los usuarios que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red, utilizando las herramientas que el Instituto le proporcione.

Uso de medios de almacenamiento

Toda solicitud para utilizar un medio de almacenamiento de información compartido (File Share), deberá contar con la autorización del área dueña de la información. El personal que requiera estos medios debe justificar su utilización. Dicha justificación deberá de presentarla al DTI firmada por el jefe inmediato superior del solicitante.

Los usuarios deberán respaldar diariamente la información relevante y crítica que se encuentre en sus equipos de cómputo.

Los usuarios del Instituto deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita el Comité de Transparencia del Instituto en términos de la Ley General de Transparencia y Acceso a la Información Pública. y de Ley Federal de Transparencia y Acceso a la Información Pública.

Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información del Instituto son registradas y susceptibles de auditoría.

Instalación de software

Los usuarios que requieran la instalación que no sea propiedad del Instituto, deberán justificar su uso y solicitar su autorización al DTI, a través de un oficio firmado por el Subdirector de adscripción, indicando el equipo de cómputo, donde se instalará el software y el período de tiempo que permanecerá dicha instalación.

Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del Instituto, que no esté autorizado por el DTI.

Identificación de incidentes

El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de Seguridad en Informática deberá reportarlo al DTI lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de Seguridad en Informática.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar a su Subdirector de adscripción, quien notificará al DTI para lo conducente.

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del Instituto debe ser reportado al DTI.

Administración de la configuración

Los usuarios de las áreas del Instituto no deben establecer redes de área local, conexiones remotas a redes Internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del Instituto, sin la autorización del DTI.

Seguridad para la red

Será considerado como un ataque a la Seguridad en Informática y una falta grave, cualquier actividad no autorizada por el DTI, en la cual los usuarios realicen la exploración de los recursos informáticos en la red del Instituto, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Uso del Correo electrónico

El servicio de correo electrónico institucional, es un servicio gratuito, y no garantizable, se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al Instituto, a menos que cuente con la autorización de la Subdirección de adscripción.

Los usuarios deberán saber que la información de los correos electrónicos y archivos adjuntos son propiedad del Instituto.

Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando, de ser posible de manera codificada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

El Instituto se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado las políticas de seguridad o realizado acciones no autorizadas.

El usuario debe de utilizar el correo electrónico del Instituto única y exclusivamente a los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.

La asignación de una cuenta de correo electrónico, deberá solicitarse por escrito a la Dirección de Planeación, señalando los motivos por los que se desea el servicio, así como sus datos personales y el área adscrita que lo solicita. Esta solicitud deberá contar con el visto bueno del jefe inmediato del área que corresponda.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico, así como interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

El usuario deberá cuidar en todo momento la utilización de un lenguaje apropiado, evitando palabras ofensivas o altisonantes.

Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

Controles contra código malicioso

Para prevenir infecciones por virus informático, los usuarios del Instituto no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el DTI.

Los usuarios deben verificar que la información y los medios de almacenamiento, considerando al menos discos flexibles, CD's, cintas, cartuchos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el DTI.

Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

Ningún usuario debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas del Instituto. El incumplimiento de este estándar será considerado una falta.

Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea, redes de comunicaciones externas, sin la debida autorización del DTI.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al DTI para la detección del virus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el Instituto: Antivirus, Outlook, office, Navegadores u otros programas.

Debido a que algunos virus son extremadamente complejos, ningún usuario debe intentar borrarlos de las computadoras.

Internet

El acceso a Internet provisto a los usuarios es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

La asignación del servicio de Internet, deberá solicitarse por escrito al DTI, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del jefe inmediato del área correspondiente.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el Instituto, en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por el DTI.

Los usuarios de Internet tienen que reportar por escrito todos los incidentes de Seguridad en Informática al DTI inmediatamente después de su identificación, indicando claramente que se trata de un incidente de Seguridad en Informática.

El acceso y uso de módem en el Instituto tiene que ser previamente autorizado por el DTI.

Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización del DTI.
- La utilización de Internet es para el desempeño de su función y puesto en el Instituto y no para propósitos personales.

Uso de equipos ajenos al Instituto

El uso de equipos de cómputo que no son propiedad del Instituto en la red institucional deberá ser avalado y justificado por escrito por el responsable del área al que pertenece el usuario ante el DTI, quién autorizará siempre y cuando se cumplan los siguientes requisitos:

- Contar con sistemas operativos de acuerdo a las características que en su momento se determinen adecuadas para un buen servicio. (Linux, Windows 2000, Windows XP, Windows Vista, Windows 7).
- El equipo de cómputo deberá contar con todas las actualizaciones críticas de seguridad del sistema operativo.
- El equipo de cómputo deberá contar con un software antivirus actualizado con las últimas firmas virales.
- El equipo de cómputo no deberá tener instalado software de intercambio punto a punto (Kazaa, gnutella, emule, edonkey, imesh, napster, Ares, etc.) que pudieran comprometer la integridad de la red institucional.
- El equipo de cómputo deberá contar con accesorios de conectividad como cables de red, tarjetas de red y adaptadores, estos accesorios no serán proporcionados por el DTI.

Si se detecta que el equipo de cómputo del usuario genera conflicto con otro equipo le será suspendido el servicio inmediatamente.

El propietario del equipo será responsable de instalar el software y hardware que utilizará dentro del Instituto; el DTI no proporcionará software con Licencia comercial (MICROSOFT OFFICE, SPSS, etc.) y demás fuentes que violen la Ley de Derechos de Autor.

Con el fin de evitar la propagación de virus a otros usuarios, el propietario del equipo deberá reportar al DTI a la brevedad posible cualquier sospecha de virus en su equipo. Se le indicará el día y la hora para analizar su computadora y verificar que sea eliminado el virus; en caso de ser posible erradicarlo será responsabilidad del propietario del equipo realizar los procesos necesarios para eliminar por completo el virus de su sistema.

Queda prohibido utilizar programas que no sean requeridos para los procesos institucionales tales como juegos, chats (IRCL hackers, brekers y similares; así como para realizar copias de CD o DVD de video, audio, juegos o software con licencia comercial).

Queda prohibido cambiar los parámetros de configuración de red asignados por el DTI.

No se permite la instalación, descarga o visualización de imágenes o textos en el equipo de cómputo o sus periféricos que puedan resultar ofensivos a terceros y que puedan perturbar el orden en las áreas institucionales.

El uso de los servicios de la red institucional es monitoreado por lo que el uso incorrecto de la misma resultará en la suspensión del servicio.

El Instituto no se hace responsable por daños físicos a los equipos o por pérdida de información ya sea por fallas de energía eléctrica, virus informáticos, robo o extravío de los mismos.

El servicio de red local estará sujeto a disponibilidad y ubicación de los equipos de comunicaciones, salidas de red y energía eléctrica.

4. CONTROLES DE ACCESO LÓGICO

Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y password necesarios para acceder a la información y a la infraestructura tecnológica del Instituto, por lo cual deberá mantenerlo de forma confidencial,

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica del Instituto, debe ser proporcionado por el dueño responsable de la información, con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus actividades

Controles de acceso lógico

El acceso a la infraestructura tecnológica del Instituto para personal externo debe ser autorizado al menos por un Subdirector de Área del Instituto, quien deberá notificarlo al DTI quien lo habilitará.

Está prohibido que los usuarios utilicen la infraestructura tecnológica del Instituto para obtener acceso no autorizado a la información u otros sistemas de información del Instituto o instituciones externas.

Todos los usuarios de servicios de información son responsables por el UserID y/o password que recibe para el uso y acceso de los recursos.

Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Instituto, a menos que se tenga la autorización del responsable dueño de la información y del DTI.

Cada usuario que acceda a la infraestructura tecnológica del Instituto debe contar con un identificador de usuario (UserID) único y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios.

Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (UserID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el UserID de otros usuarios.

Administración de privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del Instituto, deberán ser notificados al DTI, con el visto bueno del Subdirector correspondiente.

Equipo desatendido

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso con passwords y protectores de pantalla (screensaver) previamente instalados y autorizados por el DTI.

Administración y uso de Password

La asignación del password debe ser realizada de forma individual, por lo que el uso de password compartidos está prohibido.

Cuando un usuario olvide, bloquee o extravíe su password, deberá levantar un reporte al DTI para que se le proporcione un nuevo password y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.

La obtención o cambio de un password debe hacerse de forma segura, el usuario deberá acreditarse ante el DTI como empleado del Instituto.

Está prohibido que los passwords se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

Sin importar las circunstancias, los passwords nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su password de todas las acciones que se realicen con el mismo.

Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus passwords:

- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10), estos caracteres deben ser alfanuméricos.
- Deben ser difíciles de adivinar, esto implica que los passwords no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y caracteres de control.
- No deben ser idénticos o similares a password que hayan usado previamente.

El password tendrá una vigencia de 90 días, finalizando este periodo el usuario deberá realizar el cambio de contraseña.

Todo usuario que tenga la sospecha de que su password es conocido por otra persona, deberá cambiarlo inmediatamente.

Los usuarios no deben almacenar los password en ningún programa o sistema que proporcione esta facilidad. Los cambios o desbloqueo de password solicitados por el usuario al DTI serán notificados con posterioridad por correo

electrónico al solicitante con copia al jefe inmediato correspondiente, de tal forma que se pueda detectar y reportar cualquier cambio no solicitado.

Control de accesos remotos

Está prohibido el acceso a redes externas vía dial-up, cualquier excepción deberá ser documentada y contar con el visto bueno del DTI.

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Departamento de Tecnologías de la Información.

5. CUMPLIMIENTO DE SEGURIDAD EN INFORMÁTICA

Política

El DTI tiene como uno de sus objetivos institucionales la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

Derechos de propiedad intelectual

Está prohibido por la ley de derechos de autor, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por el Instituto.

Los sistemas desarrollados por personal interno o externo que controle el DTI son propiedad intelectual del Instituto.

Revisiones del cumplimiento

El DTI realizará acciones de verificación del cumplimiento de las presentes Políticas.

La Dirección de Planeación, junto con el DTI, podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en estas Políticas.

Los dueños de los procesos establecidos en el Instituto deben apoyar las revisiones del cumplimiento de los sistemas con las políticas de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

Violaciones de Seguridad en Informática

Está prohibido el uso de herramientas de hardware o software para violar los controles de Seguridad en Informática, así como realizar pruebas a los controles de los diferentes elementos de Tecnología de Información. Ninguna persona puede probar o intentar comprometer los controles internos.

Ningún usuario debe probar o intentar fallas de la Seguridad en Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por el DTI.

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Instituto.

APROBÓ:

Dr. Jorge Arturo Cardona Pérez
Director General

ELABORÓ:

Lic. Edgar Maldonado Ramírez
Jefe del Departamento de
Tecnologías de la Información

REVISÓ:

Dr. Ramón Alberto Ruiz Tapia
Director de Planeación

VALIDÓ:

Lic. María de las Mercedes Ugarte Silva
Subdirectora de Desarrollo Organizacional