
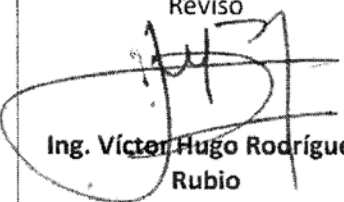



Instituto Catastral y Registral del Estado de Sonora

“MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA”

Elaboró	Revisó	Autorizó
 <p>Ing. Víctor Manuel Verdugo Encinas Jefe del Departamento de Seguridad y comunicaciones</p>	 <p>Ing. Víctor Hugo Rodríguez Rubio Director General de Servicios Informáticos</p>	 <p>Lic. Rafael Gastelum Salazar Vocal Ejecutivo del Instituto Catastral y Registral del Estado de Sonora</p>

Historia del Documento

Control de Cambios

Fecha de elaboración	Fecha de autorización	Versión	Elaboró	Naturaleza del cambio
6 de febrero de 2018		0.1	Victor Manuel Verdugo Encinas	borrador
6 de marzo de 2018		0.2	Victor Manuel Verdugo Encinas	Versión preliminar

Revisado por

Área / Dirección	Persona
Director General de Sistemas Informáticos	Ing. Víctor Hugo Rodríguez Rubio

CONTENIDO

JUSTIFICACION Y BENEFICIOS

- 1.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL
- 2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL
- 3.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO
- 4.-POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO
- 5.-POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

ANEXOS

Propósito

El presente documento tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información del Instituto.

Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares 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:

- Seguridad de Personal
- Seguridad Física y Ambiental
- Administración de Operaciones de Cómputo
- Controles de Acceso Lógico
- Cumplimiento

Estas Políticas en seguridad informática se encuentran alineadas con el Estándar Británico ISO/IEC: 27002.

Objetivo

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal Instituto Catastral y Registral del Estado de Sonora, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

Alcance

El documento define las Políticas y Estándares 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

La Dirección General de Servicios Informáticos del instituto está facultada para definir Políticas y Estándares en materia informática.

Sanciones por Incumplimiento

El incumplimiento al presente Manual 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 de Seguridad Informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos e información del Instituto.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos del Instituto, así como el estricto apego al Manual de Políticas de Seguridad Informática para usuarios.

1.1. Obligaciones

De los Usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

1.2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos 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 el presente manual.

1.3. Entrenamiento en Seguridad Informática

Todo empleado del instituto de nuevo ingreso deberá:

Leer el Manual de Políticas de Seguridad Informática del Instituto, el cual se encuentra disponible de manera impresa en cada unidad de trabajo, donde se dan a conocer las obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

1.4. Medidas disciplinarias

1.4.1. Cuando la DGSi identifique el incumplimiento al presente Manual procederá a la elaboración de constancia de hechos y remitirá el reporte o denuncia correspondiente al Órgano Interno de Control de la Secretaría de Hacienda, para los efectos de su competencia y atribuciones.

2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del Instituto Catastral y Registral del Estado de Sonora, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y los diferentes Site del Instituto.

2.1 Resguardo y protección de la información

2.1.1. El usuario deberá reportar de forma inmediata a la DGSi y al área administrativa, 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.

2.1.2. El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

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

2.2. Controles de acceso físico

2.2.1. Cualquier persona que tenga acceso a las instalaciones del Instituto, deberá registrar en (DGSi), el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del Instituto.

En caso de que el equipo que no es propiedad del Instituto, permanezca dentro de la institución más de un día hábil, es necesario que el responsable o titular del área que trabaja el dueño del equipo, elabore y firme oficio de autorización de salida.

2.3. Seguridad en áreas de trabajo

2.3.1 El datacenter y cuartos de comunicación y cableado del Instituto son áreas restringidas, por lo que sólo el personal autorizado por la DGSi puede acceder a ellos.

2.3.2 Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por personal de la DGSi; no obstante, los visitantes siempre deberán estar acompañados durante su visita al centro de cómputo o los centros de cableado.

2.3.3. La DGSi debe discontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

2.4. Protección y ubicación de los equipos

2.4.1. 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 de la DGSi, debiéndose solicitar a la misma en caso de requerir este servicio.

2.4.2. El área de soporte técnico de la DGSi será la encargada de generar el aviso al área administrativa de cambios, asignación o reasignación de los activos informáticos del instituto para que esta realice la actualización de resguardos correspondiente.

2.4.3. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario del Instituto.

2.4.4. 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.

2.4.5. Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.4.6. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea a una distancia donde una caída accidental de líquido no afecte ningún componente del equipo..

2.4.7. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete o colocar calcomanías en los mismos.

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

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

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

2.4.11. Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

2.5. Mantenimiento de equipo

2.5.1. Únicamente el personal autorizado de la DGSI podrá llevar a cabo los servicios y reparaciones al equipo informático por lo que no está permitido los servicios de mantenimiento por terceros sin autorización expresa de la DGSI.

2.5.2. Los usuarios en lo individual deberán asegurarse de respaldar la información que considere 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 de proceso de reparación, solicitando la asesoría del personal de la DGSI.

2.6. Pérdida o transferencia de equipo

2.6.1. 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.

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

2.6.3. El usuario deberá dar aviso de inmediato a la DGSi de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7. Uso de dispositivos especiales

2.7.1. El uso de Discos duros externos, memorias USB, los grabadores de discos compactos o cualquier dispositivo de almacenamiento externo es exclusivo para respaldos de información que por su volumen así lo justifiquen.

2.7.2. La asignación de este tipo de equipo será previa justificación por escrito y autorización del titular o jefe inmediato correspondiente.

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

2.7.4. Los dispositivos de acceso a la red inalámbricos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones de la institución para conectarse a ningún servicio de información externo, excepto cuando lo autorice la DGSi.

2.8. Daño del equipo

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

2.9 RespalDOS de Información

2.9.1 La DGSi validará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la DGSi, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, La DGSi velará porque los medios de almacenamiento que contienen la información crítica sean resguardados en diferentes sitios. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

2.9.2. La DGSI, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

2.9.3 La DGSI debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

2.9.4. La DGSI, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

2.10 Infraestructura tecnológica

2.10.1. Deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

2.10.2. Todo equipo de TI debe ser revisado, registrado y aprobado por la DGSI antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

2.10.3. La configuración de Routers, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la DGSI

2.10.4 La DGSI debe velar porque los recursos de la plataforma tecnológica ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

2.11 Seguridad perimetral

2.11.1. La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

2.11.2. La DGSI implementará soluciones lógicas y físicas que garanticen la protección de la información de la Dependencia o Entidad de posibles ataques internos o externos.

- Rechazar conexiones a servicios comprometidos.
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).

- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

2.11.3. Firewall

- La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, ya sean clientes o servidores.
- Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- La DGSi establecerá las reglas en el Firewall necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.
- El firewall debe controlar los ataques de “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
- Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

2.11.4. Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés) es una aplicación usada para detectar accesos no autorizados a un computador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

- La DGSi implementará soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos.
- Detección de ataques en el momento que están ocurriendo o poco después.
- Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
- Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS.

- Análisis de comportamiento anormal, para revelar o descubrir una máquina comprometida o un usuario con su contraseña al descubierto o un sistema con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.

2.11.5. Conectividad Remota - Redes Privadas Virtuales (VPN)

La DGSI establecerá los requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Dependencia o Entidad; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

2.12. Servidores Configuración e instalación

2.12.1. La DGSI proveerá y supervisará la operación de los servidores físicos (Hosts) y su rendimiento.

2.12.2. La DGSI mantendrá actualizado las configuraciones de servidores físicos (Hosts) que componen el Data Center que podrán ser utilizados por las y unidades administrativas siempre y cuando las capacidades de los mismos lo permitan.

Manual de Políticas y Estándares de Seguridad Informática -11-

2.12.3. El servicio de Aprovisionamiento de servidores será bajo el esquema de servidores virtuales.

2.12.4. En Caso de que los requerimientos de desempeño y capacidad de los servidores requeridos superen las configuraciones existentes, las unidades administrativas o entidades podrán convenir con la DGSI la entrega de componentes necesarios para proveerles el servicio, tales como procesadores, memorias, discos duros y servicios de instalación de los mismos.

2.12.5. El Aprovisionamiento de servidores a externos deberá ser respaldada vía Oficio y solicitud debidamente llenada, con los requisitos de Hardware y Software, así como los requisitos de publicación de servicios vía Internet (IP pública, Dominio), y solicitud de acceso seguro vía VPN.

2.12.6. La DGSI proporcionará acceso a través de una Virtual Private Network VPN.

2.12.7. La DGSI proporcionará las claves de acceso (misma se solicita sea modificada al primer acceso) y certificados de seguridad para las conexiones VPN.

2.12.8. La DGSI, se limita al acceso al equipo, en el cual se encuentran instaladas las aplicaciones y Bases de Datos, propias de las unidades administrativas.

2.12.9. El administrador del servidor será responsable de la administración del mismo en su totalidad (sistema operativo, antivirus, aplicaciones instaladas y respaldos).

2.12.10. El administrador del servidor deberá acreditar la propiedad del licenciamiento de los sistemas a instalar en el servidor.

2.12.11. La dependencia y/o unidad administrativa responsable de la administración deberá implementar los métodos o acciones necesarias para garantizar la seguridad a nivel de información y Sistema Operativo incluyendo cualquier vulnerabilidad reportada, parches y actualizaciones necesarias para el óptimo funcionamiento del mismo.

2.12.12. La DGSI en caso de que detecte alguna falla de seguridad, será puesto fuera de producción (cuarentena) con el fin de evitar brecha de seguridad hacia los demás servidores del Data Center hasta la remediación de la falla por parte del Administrador responsable de la dependencia o Unidad Administrativa.

2.12.13. Los servidores que proporcionen servicios a través de la red e Internet deberán: Funcionar 24 horas del día los 365 días del año, recibir mantenimiento anual que incluya la revisión de su configuración, ser monitoreados.

2.12.14. La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

- Diariamente, información crítica.
- Mensual. Información con poco o nulo movimiento
- Trimestral. Respaldo totales

2.13. Seguridad en Centro de Datos (Data Center)

El Centro de Datos es área restringida, por lo que sólo el personal autorizado por la DGSI puede acceder a él.

2.13.1. Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la DGSI. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito de los responsables de la DGSI.

2.13.2 El Data Center deberá:

- Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.
- Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por la Dirección de Tecnología Informática.
- Recibir limpieza, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- Controles de humedad y temperatura. Mantener la temperatura a 21 grados centígrados.

- Los sistemas de Refrigeración deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Asignar un técnico para que realice un control diario temperatura y aires acondicionados
- Sistemas de Detección y extinción de incendio.
- Sistema de Vigilancia o alarma.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

3. POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura 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 del Instituto que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir a la DGSI , o a su jefe inmediato, para solicitar asesoría.

3.1. Uso de medios de almacenamiento

3.1.1. Toda solicitud para utilizar un medio de almacenamiento de información compartido, deberá contar con la autorización del titular del área dueña de la información.

Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con sello y firma del titular a la DGSI o al representante de ésta en su zona. Cualquier información compartida, no autorizada será responsabilidad del titular del equipo.

3.1.2. Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la DGSI, para determinar el medio en que se realizará dicho respaldo.

3.1.3. En caso de que por el volumen de información se requiera algún respaldo en CD u otro dispositivo de almacenamiento, este servicio deberá solicitarse por escrito al Titular de la DGSI, y deberá contar con la firma del titular del área de adscripción del solicitante.

3.1.4. Los trabajadores 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 la Ley de Acceso a la Información Pública del Estado de Sonora, lineamientos y demás criterios y procedimientos establecidos en esta materia.

3.1.5. Las actividades que realicen los usuarios del en la infraestructura de Tecnología de la Información son registradas en bitácoras electrónicas de seguridad y son susceptibles de auditoría.

3.2. Instalación de Software

3.2.1. Los usuarios que requieran la instalación de software que no sea propiedad del Instituto, deberán justificar su uso y solicitar su autorización a la DGSI, a través de un oficio firmado por el titular del área de su adscripción, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software.

Si el dueño del software no presenta la factura de compra del software, el personal asignado por la DGSI procederá de manera inmediata a desinstalar dicho software.

3.2.2. 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 la DGSI.

3.3. Identificación del incidente

3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a la DGSI o a su titular de adscripción, lo antes posible, indicando y documentando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2. Cuando exista la sospecha o el conocimiento de que información ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar al titular de su adscripción.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del Instituto, debe ser reportado a la DGSI.

3.4. 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, alámbricas o inalámbricas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del instituto, sin la autorización por escrito de la DGSi.

3.5. Seguridad de la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la DGSi 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 mostrar una posible vulnerabilidad.

3.6. Uso del correo electrónico

3.6.1. 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 encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una cuenta de correo electrónico externa al Instituto, a menos que cuente con la autorización del titular del área de adscripción.

3.6.2. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad del Instituto. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3. Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la DGSi.

3.6.4. El Instituto, se reserva el derecho de 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 violando políticas de Seguridad Informática del Instituto o realizado acciones no autorizadas.

3.6.5. El usuario debe de utilizar el correo electrónico oficial del instituto, única y exclusivamente para 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 distinto.

3.6.6. La asignación de una cuenta de correo electrónico externo, deberá solicitarse por escrito a la DGSi, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área que corresponda.

3.6.7. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.7. Controles contra código malicioso

3.7.1. Para prevenir infecciones por virus informáticos, los usuarios del Instituto, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la DGSI.

3.7.2. Los usuarios del Instituto, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, CD's y discos duros externos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la DGSI o pedir apoyo para realizarlo.

3.7.3. El usuario debe verificar mediante el software de antivirus autorizado e instalado por la DGSI que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

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

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

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

3.7.7. Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica a la DGSI las actualizaciones del software de antivirus.

3.7.8. Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la DGSI en programas tales como:

- Antivirus;
- Correo electrónico;
- Paquetería Office;

- Navegadores;
- Otros programas.

3.7.9. Debido a que algunos virus son extremadamente complejos, ningún usuario del Instituto debe intentar erradicarlos de las computadoras, lo indicado es suspender inmediatamente el uso del equipo y llamar al personal de la DGSI para que sean ellos quienes lo solucionen.

3.8. Permisos de uso de Internet

3.8.1. El acceso a internet provisto a los usuarios del Instituto es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución por usos distintos a los solicitados se procederá de acuerdo a lo que determine el Órgano Interno de Control de la Secretaría de Hacienda.

3.8.2. La asignación del servicio de internet, deberá solicitarse por escrito a la DGSI, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área correspondiente.

3.8.3. Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por el Instituto por lo que se prohíbe la conexión de los equipos a través de las conexiones de los dispositivos personales (Celulares o cualquier dispositivo inalámbrico).

3.8.4. Los usuarios con acceso a Internet tienen que reportar todos los incidentes de seguridad informática a la DGSI, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.7. Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas especificadas en los sistemas de seguridad del instituto.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados y de aquellos que estén contemplados para su cobro en los aranceles.
- Saben que existe la prohibición de descarga de software sin la autorización de la DGSI.
- La utilización de internet es para el desempeño de su función y puesto en el Instituto y no para propósitos personales.

3.8.8. Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

- **Directores:** Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea, excepto la siguiente tabla:

1. Violence/Hate/Racism
2. Intimate Apparel/Swimsuit
3. Nudism
4. Pornography
5. Weapons
6. Adult/Mature Content
7. Cult/Occult
8. Drugs/Illegal Drugs
11. Gambling
12. Alcohol/Tobacco
22. Games
28. Hacking/Proxy Avoidance Systems
50. Pay to Surf Sites
56. Other
57. Internet Watch Foundation CAIC

- **SISTEMAS:** Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea, excepto la siguiente tabla:

1. Violence/Hate/Racism
2. Intimate Apparel/Swimsuit
3. Nudism
4. Pornography
5. Weapons
6. Adult/Mature Content
7. Cult/Occult
8. Drugs/Illegal Drugs
9. Illegal Skills/Questionable Skills
10. Sex Education
11. Gambling
12. Alcohol/Tobacco

-

- **EMPLEADOS CON STREAMING MEDIA:** Internet con streaming media y sin redes sociales: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación.
- **EMPLEADOS SIN STREAMING MEDIA:** Internet sin streaming media, redes sociales y mensajería instantánea: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación.
- **CARTOGRAFIA:** Los empleados podrán acceder a todos los servicios de google maps y correo electrónico y alojamiento web: Los usuarios no podrán navegar en redes sociales y servicios de mensajería instantánea.

- SIGER: Los usuarios podrán acceder a servicios de correo y página de la Secretaría de Economía. Los usuarios sólo podrán hacer uso de internet a páginas oficiales permitidas y correo electrónico, aplicándose las políticas de seguridad.
- Default: El usuario solo tendrá acceso a portales de búsqueda y páginas de gobierno.

4. POLÍTICAS Y ESTÁNDARES DE 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 (userID) y contraseña (password) necesarios para acceder a la información, sistemas y a la infraestructura del Instituto, por lo cual deberá mantenerlo de forma confidencial.

La vocalía ejecutiva del Instituto o la Dirección General titular de generadora de la información, son los únicos que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica del Instituto, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones.

4.1. Controles de acceso lógico

4.1.1. El acceso a la infraestructura tecnológica del Instituto para personal externo debe ser autorizado al menos por un titular de área del Instituto, quien deberá notificarlo por oficio a la DGSI, quien lo habilitará para tal efecto.

4.1.2. 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.

4.1.3. Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.4. Todos los usuarios deberán autenticarse por los mecanismos de control físicos o lógicos de acceso provistos por la DGSI antes de poder usar la infraestructura tecnológica y sistemas del Instituto.

4.1.5. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Instituto.

4.1.6. Cada usuario que accede a la infraestructura tecnológica del Instituto debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

4.1.7. Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad

exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

4.1.8. Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros empleados del Instituto.

4.2. Administración de privilegios

4.2.1. Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica y sistemas del Instituto, deberán ser solicitadas por escrito a la DGSÍ con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.3. Equipo desatendido

4.3.1 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por la DGSÍ, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo. Para lo anterior deberán realizar el bloqueo de su equipo (Windows + L) o el retido de su dispositivo de autenticación.

4.3.2 Todos los movimientos realizados en los equipos responsabilidad del usuario serán atribuidos a este de acuerdo a lo consignado en las bitácoras de seguridad de los sistemas, bases de datos servidores o servicios de directorio del instituto.

4.3.3 La DGSÍ podrá, sin notificación previa, realizar el bloqueo del equipo y el usuario de acceso en caso de detectar equipos desatendidos por largos períodos de tiempo.

4.4. Administración y uso de contraseñas

4.4.1. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas está prohibido.

4.4.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito a la DGSÍ, indicando si es de acceso a la red o a módulos de sistemas desarrollados por la DGSÍ, para que se le proporcione una nueva contraseña.

4.4.3. La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la DGSÍ como empleado del Instituto.

4.4.4. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

4.4.5. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener serie de números consecutivos
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos, o sea, números y letras;
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario (siglas, fechas de nacimiento, apodos, etc); y
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.4.7. La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta o a través de políticas forzosas de cambio de la misma por parte de la DGSI.

4.4.8. Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente o solicitar el apoyo para su cambio a la DGSI.

4.4.9. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad dentro o fuera del equipo, ya sea a través de medios digitales o escritos.

4.4.10. Los cambios o desbloqueo de contraseñas solicitados por el usuario a la DGSI serán solicitados mediante el formato correspondiente y firmado por el jefe inmediato del usuario que lo requiere.

4.4.11 Los medios físicos de autenticación a través de dispositivos usb, tokens o tarjetas electrónicas proporcionados por el instituto, son personales e intransferibles. El costo de reposición del mismo por extravío o mal uso será a cargo del usuario.

4.5. Control de accesos remotos

4.5.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo físico, lógico, alámbrico o inalámbrico, cualquier excepción deberá ser documentada y contar con el visto bueno de la DGSI.

4.5.2. La administración remota de equipos internos del instituto conectados a internet por cualquier medio, no está permitida, salvo que se cuente con la autorización de la DGSI y con un mecanismo de control de acceso seguro.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política

De acuerdo al artículo 21 del Reglamento Interior del Instituto Catastral y Registral del Estado de Sonora, corresponde a la Dirección General de Servicios Informáticos: “Organizar a los usuarios

del Instituto para que éstos se encarguen de vigilar la integridad y calidad de los datos catastrales y registrales”

5.1. Derechos de Propiedad Intelectual

5.1.1. Está prohibido por las leyes de derechos de autor realizar copia no autorizadas de software, ya sea adquirido o desarrollado por el Instituto. Las copias se permiten para conservar una respaldo del software original.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte de la DGSI, o sea coordinado por ésta, son propiedad intelectual del Instituto y deberá invariablemente mantenerse los códigos fuentes de los mismos para actividades de mantenimiento o reuso.

5.2. Revisiones del cumplimiento

5.2.1. La DGSI podrá realizar de manera autónoma y sin previo aviso acciones de verificación del cumplimiento del Manual de Políticas de Seguridad Informática.

5.2.2. La DGSI podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar y supervisar 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 la Política de Seguridad del Personal.

5.3. Violaciones de seguridad informática

5.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la DGSI.

5.3.2. Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información. Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación de la DGSI, con excepción de los Órganos Fiscalizadores.

5.3.3. Ningún usuario debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas (Sniffers, network o IP scanners, etc), a menos que estas pruebas sean controladas y aprobadas por la DGSI.

5.3.4. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para autoreplicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información del Instituto.

ANEXOS

A. Lista de Acrónimos y figuras Utilizados

DGSI

Dirección General de Servicios Informáticos

Instituto

Instituto Catastral y Registral del Estado de Sonora

B. Glosario de términos

Es una recopilación de palabras claves que se encuentran en el documento, las cuáles pueden ser términos técnicos, o bien palabras con un significado especial para el proceso definido. Su objetivo es lograr que se maneje un mismo concepto y evitar cualquier tipo de confusión para el correcto entendimiento del documento. Su estructura deberá ser por orden alfabético y la definición de los términos deberá ser clara y breve

A

Acceso. Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.

Acceso Físico. Es la actividad de ingresar a un área.

Acceso Lógico. Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo, o bien usar su información.

Acceso Remoto. Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.

Aplicación. Acción que se realiza a través de un programa de manera directa con el usuario. Navegadores, Chat, correo electrónico, etc. Son algunos ejemplos de aplicaciones en el medio de Internet.

Antivirus. Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o disquete.

Ataque. Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese activo y lograr afectarlo.

Archivo. Una colección identificada de registros relacionados.

Autorización. Es el proceso de asignar a los usuarios permisos para realizar actividades de acuerdo a su perfil o puesto.

B

Base de Datos. Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.

C

CD. Medio de almacenamiento de información.

Código Malicioso. Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un caballo de Troya es ejemplo de un código malicioso.

Comprimir (zip). Reducir el tamaño de los archivos sin que éstos pierdan nada de su información. Zip es el nombre de la extensión que contiene un archivo comprimido.

Computadora. Es un conjunto de dispositivos electrónicos que forman una máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas.

Confidencialidad. Se refiere a que la información no sea divulgada a personal no autorizado para su conocimiento.

Control de Acceso. Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo tecnológico.

Copyright. Derecho que tiene un autor, incluido el autor de un programa informático, sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida. El símbolo de este derecho es ©.

Correo Electrónico o E- mail. La funcionalidad es similar a usar el correo normal, pero ahora el individuo puede utilizar una computadora y un software para enviar mensajes o paquetes a otro individuo o grupo de personas a una dirección específica a través de la red o Internet.

Cuentas de Usuario. Es un identificador único, el cual es asignado a un usuario del sistema para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.

D

Descargar. Acción de transferir información computarizada de una computadora a otra.

Descomprimir (unzip). Acción que se lleva a cabo después de haber comprimido un archivo para regresarlo a su estado original.

Discos Ópticos. Los discos ópticos son medios de almacenamiento de información que presentan una capa interna protegida, donde se guardan los bits mediante el uso de un rayo láser, éste al ser reflejado, permite detectar variaciones microscópicas de propiedades “óptico- reflectivas” ocurridas como consecuencia de la grabación realizada en la escritura. Un sistema óptico con lentes encamina el haz luminoso, y lo enfoca como un punto en la capa del disco que almacena los datos.

Disponibilidad. Se refiere a que la información esté disponible en el momento que se requiera.

Dominio. Sistema de denominación de host en Internet. Conjunto de caracteres que identifica y diferencian los diferentes sitios Web.

E

Encriptación. Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados. El término encriptación como tal, no existe en el lenguaje español, el término correcto es cifrado de datos.

Estándar. Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

F

Falta administrativa. Es la consecuencia que resulta del incumplimiento de la normatividad.

Freeware (Software Libre). Programas que se pueden bajar desde Internet sin cargo.

FTP. Protocolo de transferencia de Archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red

G

Gusano. Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

H

Hardware. Se refiere a las características técnicas y físicas de las computadoras.

Help Desk / SAU. Soporte técnico brindado a los usuarios telefónicamente, su función es proveer conocimientos especializados de los sistemas de producción para identificar y asistir en el ámbito / desarrollo de sistemas y en la resolución de problemas.

Herramientas de seguridad. Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica del Instituto.

I

Impacto. Magnitud del daño ocasionado a un activo en caso de que se materialice una amenaza

Incidente de seguridad. Cualquier evento que represente un riesgo para la adecuada conservación de la confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función

Integridad. Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional o accidental.

Internet o World Wide Web (www). Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes en donde cualquier usuarios consulta información de otra computadora conectada a esta red e incluso sin tener permisos necesarios acceder a dichos activos.

Intrusión. Es la acción de introducirse o acceder sin autorización a un activo tecnológico.

L

Lenguaje de Programación. Sistema de escritura para la descripción precisa de algoritmos o desarrollo programas informáticos.

M

Maltrato, descuido o negligencia. Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la Institución.

Mecanismos de seguridad o de control. Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Medios Magnéticos (medios de almacenamiento). Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CDs, Cintas, Cartuchos, etc.).

Mecanismos de seguridad o de control. Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Metodología. Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente definidas.

N

Nodo. Punto principal en el cual se les da acceso a una red a las terminales o computadoras.

Normatividad. Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización

P

Página Web. Ver sitio Web.

Parche (patch). Un parche (algunas veces llamado Fix) son piezas de programación que representan una solución rápida al software o sistema, para incrementar la seguridad o incrementar la funcionalidad del mismo.

Password o Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a un computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6-10 caracteres alfanuméricos.

R

Respaldo. Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Riesgo. Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.

S

Servidor. Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

Sitio Web. El sitio Web es una lugar virtual en el ambiente de Internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a el.

Software. Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.

Software Antivirus. Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.

Switch. Dispositivo de red que filtra y direcciona paquetes a las direcciones destinatarias. El switch opera en la capa de enlace de datos del modelo OSI.

T

Tarjeta electrónica o inteligente. Es una tarjeta de plástico del tamaño de una tarjeta de crédito, que incorpora un microchip o emisor RFID, en el cual se puede cargar datos como números telefónicos anteriormente llamados, pagos realizados a través de medios electrónicos y otro tipo de aplicaciones, las cuales pueden ser actualizadas para usos adicionales.

U

User-ID (identificación de usuario). Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, números o signos.

Usuario. Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal, o dispositivo (hardware).

V

Virus. Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o diskettes de computadoras.

Vulnerabilidad. Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencionado o accidental.