CAPITULO II

2 SEGURIDAD DE UNA RED

2.1 Introducción

2.2 Niveles de Seguridad.

2.2.1 Nivel D1.

2.2.2 Nivel C1

2.2.3 Nivel C2.

2.2.4 Nivel B1

2.2.5 Nivel B2.

2.2.6 Nivel B3.

2.2.7 Nivel A.

2.3 Planeación de seguridades en redes.

2.4 Política de Seguridad

2.4.1 Importancia

2.4.2 Aspectos a considerarse en diseño de una Política de Seguridad

2.4.2.1 Análisis del riesgo.

2.4.2.2 Identificación de Recursos

2.4.2.3 Identificación de las Amenazas.

a) Definición del acceso no autorizado
b) Riesgo de revelación de información.
c) Negación de servicio

2.4.2.4 Identificación del uso adecuado de los recursos

2.4.2.5 Plan de acción cuando se sobrepasa una política de seguridad.

2.5 Diseño de una política de seguridad.

2.5.1 Políticas de seguridad del Sitio

2.5.2 Factores externos que influyen en las políticas de seguridad

2.5.3 Diseño de la Política de Seguridad para la Universidad Técnica del Norte.

CAPITULO II

2. SEGURIDAD DE UNA RED

2.1 INTRODUCCIÓN

Internet es una red anárquica donde desde cualquier punto del mundo, un usuario con una computadora y un módem puede conectarse y acceder a la información que circula por la red.

Esta posibilidad hace que Internet se constituya en una nueva plataforma de comunicación que está siendo adoptada rápidamente por millones de usuarios en todo el planeta con diversos fines: comerciales, educativos, culturales, de investigación, etc.

De igual modo, las facilidades mencionadas, hacen que la red sea un ámbito vulnerable donde los datos son relativamente fáciles de interceptar, alterar o destruir.

Actualmente la seguridad informática ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Esto ha llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el

mayor provecho de estas ventajas, para así evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia, sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y

materialización de los compromisos adquiridos con la organización.

2.2. NIVELES DE SEGURIDAD

Los niveles de seguridad son distribuidos de acuerdo con el sistema operativo que se este utilizando sobre la red de la empresa o institución ya sea pública, privada, gubernamental o no gubernamental, entre estos se tiene los siguientes:

2.2.1. Nivel D1	El sistema entero no es confiable
2.2.2. Nivel C1	Protección de hardware
2.2.3. Nivel C2	Resuelve problemas del nivel C1 y C2
2.2.4. Nivel B1	Protección de Seguridad Etiquetada
2.2.5. Nivel B2	Protección Estructurada
2.2.6. Nivel B3	Dominio de Seguridad
2.2.7. Nivel A	Diseño Verificado

2.2.1. Nivel D1

Es la forma mas baja de seguridad, esta norma establece que el sistema entero no es confiable. No dispone de protección para el hardware; el sistema operativo se compromete fácilmente y no existe autentificación respecto de los usuarios y sus derechos a tener acceso a la información almacenada en la computadora.

2.2.2 Nivel C1

Existe cierto nivel de protección para el hardware, ya que este no puede comprometerse fácilmente, auque sea posible. Los usuarios deben identificarse ante el sistema mediante su login y contraseña, se emplea esta combinación para determinar los

derechos de acceso a programas e información que tiene cada usuario.

Estos derechos de acceso son los permisos de archivo y directorio, los controles de acceso discrecional permiten al dueño del archivo o directorio, así como al administrador del sistema, evitar que ciertas personas o grupos tengan acceso a dichos programas o información. Sin embargo, no se impide que la cuenta del administrador del sistema realice ninguna actividad, en consecuencia un administrador poco escrupuloso puede comprometer fácilmente la seguridad del sistema sin que nadie lo sepa.

Además, muchas de las tareas cotidianas de administración del sistema solo pueden ser realizadas por el login de usuario llamado raíz (root). Con la actual descentralización de los sistemas de cómputo, no es raro que en una organización se encuentre dos o tres personas que conocen la clave del usuario root, esto si es un problema pues no hay forma de distinguir cual de los usuarios que ingresa como root realizó los cambios.

2.2.3 Nivel C2.

Está diseñado para ayudar a resolver los problemas anteriores, además de las funciones del nivel C1, el nivel C2 cuenta con características adicionales que crean un ambiente de acceso controlado. Este ambiente tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, con base no sólo en los permisos, sino también en los niveles de autorización. Además, este nivel de seguridad requiere que se audite al sistema, lo cual implica registrar una auditoria por cada acción que ocurra en el sistema.

La auditoría se utiliza para llevar registros de todas las acciones relacionadas con la seguridad como puede ser las actividades efectuadas por el administrador del sistema. La auditoría requiere de autentificación adicional pues, sin ésta ¿cómo estar seguros de que la persona que ejecuta el comando realmente es quien dice ser? ; la desventaja de la auditoría es que requiere recursos adicionales del procesador y del subsistema de disco.

Con el uso de autorizaciones adicionales, es posible que los usuarios de un sistema C2 tengan la autorización para realizar tareas de administración del sistema sin necesidad de la contraseña del root., esto permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

2.2.4 Nivel B1

Es también llamado Protección de Seguridad Etiquetada, es el primer nivel con soporte para seguridad multinivel, como el secreto y el ultra secreto. En este nivel se establece que el dueño del archivo no puede modificar los permisos de un objeto que este bajo control de acceso obligatorio.

2.2.5 Nivel B2

Conocido como Protección Estructurada, requiere que todos los objetos estén etiquetados, los dispositivos como discos, cintas y terminales, pueden tener asignado uno o varios niveles de seguridad. Este es el primer nivel en que aborda el problema de la comunicación de un objeto con otro que se encuentra en un nivel de seguridad inferior.

2.2.6 Nivel B3

Llamado de Dominios de Seguridad, refuerza los dominios con la instalación de hardware. Por ejemplo, se utiliza hardware de manejo de memoria para proteger el dominio de seguridad contra accesos no autorizados y modificaciones de objetos en diferentes dominios de seguridad. Este nivel requiere también que la terminal del usuario esté conectada al sistema a través de una ruta de acceso confiable.

2.2.7 Nivel A.

Conocido como Diseño Verificado, constituye actualmente el nivel de seguridad válido más alto. Para alcanzar este nivel de seguridad, deben incluirse todos los componentes de los niveles inferiores; el diseño debe verificarse matemáticamente y debe realizarse un análisis de los canales cubiertos y de distribución confiable. La distribución confiable significa que el hardware y el software hayan estado protegidos durante su traslado para evitar violaciones de los sistemas de seguridad.

2.3 PLANEACION DE SEGURIDAD EN REDES

Antes de construir una barrera de protección, como preparación parar conectar la red con el resto de Internet, es importante entender con exactitud qué recursos de la red y servicios se desea proteger.

Una política de red es un documento que describe los asuntos de seguridad de red de una organización. Este documento se convierte en el primer paso para construir barreras de protección efectivas.

Es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía, vale la pena implementar una política de seguridad si los recursos y la información que la organización tiene en su rede merecen protegerse. La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes esto debe protegerse del vandalismo del mismo modo que otros bienes como la propiedad corporativa.

La mayoría de diseñadores de redes por lo general empiezan a implementar soluciones de firewall antes de que se haya identificado un problema particular de seguridad de red, quizá una de las razones de esto es que, idear una política de seguridad de red efectiva significa plantear preguntas difíciles acerca de los tipos de servicios de interredes y recursos, cuyo acceso se permitirá a los usuarios y cuales tendrán que restringirse debido a los riesgos de seguridad .

Si actualmente los usuarios tienen acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso, también se debe tomar en cuenta que la política de seguridad que se emplee, que no disminuirá la capacidad de la organización; una política de red que impide que los usuarios cumplan efectivamente con sus tareas, puede traer consecuencias indeseables; los usuarios de la red quizá encuentren la forma de eludir la política de seguridad lo que la vuelve inefectiva, una política de red efectiva es algo que todos los usuarios y administradores de red pueden aceptar y están dispuestos a aplicar.

2.4 POLÍTICA DE SEGURIDAD

2.4.1 Importancia

Una política de seguridad es una forma de comunicarse con los usuarios y los gerentes. Las Políticas de Seguridad Informáticas establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.

No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de lo que se desea proteger. Cada política de Seguridad Informática es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como, un motor de intercambio y desarrollo en el ámbito de sus negocios.
Las Políticas de Seguridad Informática deben orientar las decisiones que se toman en relación con la seguridad, por tanto requieren una disposición de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informáticas deben considerar entre otros, los siguientes elementos:

- Alcance de la políticas, incluyendo facilidades, sistemas y personal sobre el cual se aplica.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

- Definición de violaciones y de las consecuencias por el no cumplimiento de la Política de Seguridad Informática.

- Responsabilidades de los usuarios con respecto a la información a la que él o ella tiene acceso.

Las Políticas de Seguridad Informáticas deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones, transmitir por qué son importantes éstos u otros recursos o servicios.

De igual forma, las Políticas de Seguridad Informática establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía, deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otro lado, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones, que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer, no debe especificar con

exactitud que pasará cuando algo suceda; no es una sentencia obligatoria de la ley.

2.4.2 Aspectos a considerarse en diseño de una Política de Seguridad

Definir una política de seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra pérdida y daño. Uno de los enfoques posibles para elaborar dicha política es examinar lo siguiente:

- ¿Qué recursos se está tratando de proteger?
- ¿De quiénes se necesita proteger los recursos?
- ¿ Qué tan posibles son las amenazas?
- ¿ Qué tan importante es el recurso?
- ¿Qué medida se puede implementar para proteger los bienes de
  forma económica y oportuna?
- Examinar periódicamente la política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

Si bien las características de la Política de Seguridad Informática que se han mencionado hasta el momento, muestran una perspectiva de las implicaciones en la formulación de estas directrices, a continuación se mencionan algunos aspectos generales recomendados para la formulación de las mismas.

- Efectuar un ejercicio de análisis de riesgos informático, a través del cual se valora los activos, y se permitirá afinar las Políticas de Seguridad Informática de la organización.
- Involucrar a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la Políticas de Seguridad Informáticas.

- Comunicar a todo el personal involucrado en el desarrollo de las Políticas de Seguridad Informática, los beneficios y riesgos relacionados con los recursos, bienes y sus elementos de seguridad.

- Se debe tener siempre presente que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los interesados en salvaguardar los activos críticos de la funcionalidad de su área u organización.

- Desarrollar un proceso de monitoreo periódico de las directrices en el que hacer de la organización, que permita una actualización oportuna de las mismas

- No se debe dar por hecho algo que es obvio, hacer explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las Políticas de Seguridad Informática trazadas.

2.4.2.1 Análisis del riesgo.

Cuando se crea una política de seguridad es importante comprender que la razón para crear una política es, en primer

lugar, asegurar los esfuerzos dedicados a la seguridad sean costeables, esto significa que se debe conocer cuáles recursos vale la pena proteger, y cuáles son más importantes que otros, también deben identificarse la fuente de amenazas de la que se está protegiendo a los recursos de la red. El análisis de riesgo implica determinar los siguiente:

- ¿Qué necesita proteger?
- ¿De qué necesita protegerlo?
- ¿Cómo protegerlo?

Los riesgos deben clasificarse por el nivel de importancia y gravedad de pérdida, no se debe terminar en una situación en la que se gaste más en proteger algo que es de menor valor. En el análisis de riesgo hay que determinar los siguientes factores:

- Estimación del riesgo de perder el recurso (Ri)
- Estimación de la importancia del recurso(Wi)

Otros factores que hay que considerar al estimar el riesgo de un recurso de red son su disponibilidad, integridad y confidencialidad. La disponibilidad de un recurso es la medida de qué tan importante es tenerlo disponible todo el tiempo; la integridad de un recurso es la medida de qué tan importante es que éste o los datos del mismo sean consistentes, esto es de particular importancia para los recursos de bases de datos; la confidencialidad se aplica a recursos tales como archivos de datos a los cuales se desee restringir el acceso.

2.4.2.2 Identificación de Recursos

Al realizar el análisis de riesgo, se debe identificar todos los recursos que corran el riesgo de sufrir una violación de seguridad, los recursos como el hardware son bastante obvios para incluirlos en este cálculo, pero en muchas ocasiones se ignoran recursos tales como las personas que en realidad utilizan los sistemas, es importante identificar a todos los recursos de la red que puedan ser afectados por un problema de seguridad.

La RFC 1244 enlista los siguientes recursos de red que se debe considerar al calcular las amenazas a la seguridad general:

- Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores, terminales, routers.

- Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

- Datos: durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, base de datos, en tránsito a través de medios de comunicación.

- Personas: usuarios, personas necesarias para operar los sistemas.

- Documentación: sobre programas, hardware, sistemas, procedimientos administrativos locales.

- Suministros: papel, formularios, cintas, medios magnéticos.

2.4.2.3 Identificación de las Amenazas.

Una vez que se han identificado los recursos que requieren protección se deben identificar las amenazas a las que están expuestos, se pueden examinarse las amenazas para determinar que posibilidad de pérdida existe, también deben identificarse de qué amenazas se está usted tratando de proteger a sus recursos.

A continuación se detallan algunos tipos de amenazas que se deben tomar en cuenta el momento de elaborar una Política de Seguridad Informática.

a) Definición del acceso no autorizado

El acceso a los recursos de la red debe estar permitido sólo a los usuarios autorizados, esto se llama acceso autorizado, una amenaza común que afecta a muchos sitios es el acceso no autorizado a las instalaciones de cómputo, este acceso puede tomar muchas formas, como el uso de la cuenta de otro usuario para tener acceso a la red y sus recursos. En general, se considera que el uso de cualquier recurso de la red sin permiso previo es un acceso no autorizado.

La gravedad del acceso no autorizado depende del sitio y de la naturaleza de la pérdida potencial, en algunos sitios, el solo hecho de conceder acceso a un usuario no autorizado puede

causar daños irreparables por la cobertura negativa de los medios.

b) Riesgo de revelación de información.

La revelación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza, se debe determinar el valor y delicadeza de la información guardada en los computadores, en el caso de vendedores de hardware y software, el código fuente, los detalles de diseño, los diagramas y la información específica de un producto representan una ventaja competitiva.

Muchas veces la gente supone que las intrusiones a las redes y computadoras son realizadas por individuos que trabajan por su cuenta, no siempre es así, los peligros del espionaje industrial y gubernamental sistemático, son realidades desafortunadas de la vida.

c) Negación de servicio

Las redes vinculan recursos valiosos como computadoras y bases de datos y proporcionan servicios de los cuales dependen la organización, la mayoría de los usuarios dependen de estos servicios parar realizar su trabajo con eficiencia, si no están disponibles estos servicios, hay una pérdida correspondiente de productividad.

Es difícil predecir la forma en que se produzca la negación del servicio, los siguientes son algunos ejemplos de cómo la negación de servicios puede afectar a una red.

- La red puede volverse inservible por un paquete extraviado

- La red puede volverse inservible por inundación de tráfico
- La red puede ser fraccionada al desactivar un componente importante, como el router que enlaza los segmentos de la red.

- Un virus puede alentar o invadir un sistema de cómputo al consumir los recursos del sistema.

- Los dispositivos reales que protegen a la red podrían subvertirse.

2.4.2.4 Identificación del uso adecuado de los recursos

Una vez determinados los usuarios autorizados a tener acceso a los recursos de la red, se debe establecer los lineamientos del uso aceptable de dichos recursos. Los lineamientos dependerán de la clase de usuarios ya sean estos:

- Desarrolladores de software
- Estudiantes
- Profesores
- Usuarios externos, etc.

Se deben tener lineamientos aparte para cada clase, la política debe establecer qué tipo de uso es aceptable y cuál es inaceptable, así como qué tipo de uso está restringido. La política que se elabore será la Política de uso aceptable de esa red, si el acceso a un recurso de la red está restringido, debe considerarse el nivel de acceso que tendrá cada clase de usuario.

La Política de Acceso debe establecer con claridad que cada usuario es responsable de sus acciones, no tiene caso construir costosos mecanismos de seguridad con firewalls si un usuario puede revelar la información copiando archivos en disco o cinta poniendo de esta manera a disposición de individuos no autorizados.

Aunque parezca obvio la Política de Acceso debe establecer claramente que no está permitido irrumpir en las cuentas o pasar por alto la seguridad, esto puede ayudar a evitar cuestiones legales planteadas por empleados que pasan por alto la seguridad de la red y después aseguran que no se les informó o capacitó adecuadamente acerca de la política de la red. A continuación se muestra los lineamientos que deben escribirse al desarrolla una Política de Acceso:

- ¿Se permite introducirse en las cuentas?
- ¿Se permite descifrar las contraseñas?
- ¿Se permite interrumpir servicios ?
- ¿Los usuarios deben suponer que si un archivo tienen permiso general de lectura, eso los autoriza a leerlos?
- ¿Debe permitirse que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permisos de escritura?
- ¿Los usuarios deben compartir cuentas?

A menos que se tenga requerimientos especiales, la respuesta a estas preguntas, en la mayoría de las organizaciones debe ser No.

2.4.2.5 Plan de acción cuando se sobrepasa una política de seguridad

Cada vez que se viola la política de seguridad, el sistema está sujeto a amenazas. Si no se producen cambios en la seguridad de la red cuando ésta sea violada, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros. La política de seguridad y su implementación deben ser lo menos obstructiva posible, si la política de seguridad es demasiado restricta, o está explicada inadecuadamente, es muy probable que sea violada.

Al margen del tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla, en ocasiones las violaciones a la política son evidentes; otras veces estas infracciones no son detectadas. Los procedimientos de seguridad que se establezca debe reducir al mínimo la posibilidad de que no se detecte una infracción de seguridad.

Cuando se detecte una violación a la política de seguridad, se deben determinar las circunstancias en que ésta ocurrió, ya sea debido a la negligencia de un individuo, un accidente, un error, por ignorancia de la política vigente o si deliberadamente la política fue pasada por alto, en este ultimo caso, la violación quizá haya sido efectuada no sólo por una persona, sino por un grupo que a sabiendas realizó un acto de violación directa de la política de seguridad. En cada una de estas circunstancias, la política de seguridad debe contar con lineamientos acerca de las medidas que se deben tomar.

Cuando ocurre una violación, la respuesta puede depender del tipo de usuario responsable del acto, las violaciones a la política pueden ser cometidas por gran variedad de usuarios; algunos pueden ser locales y otros externos, los usuarios locales son llamados usuarios internos y los externos, usuarios foráneos. Por lo general la distinción entre ambos tipos está basada en los limites de red administrativos, legales o políticos, el tipo de límite determina cuál debe ser la respuesta a la violación de la seguridad, las respuestas pueden ir desde una reprimida, una advertencia verbal, una carta formal o la presencia de cargos judiciales.

Se necesita definir la acción según el tipo de violación, estas acciones requieren ser definidas con claridad, con base en el tipo de usuario que haya violado la política de seguridad de cómputo, los usuarios internos y externos de la red deben estar conscientes de la política de seguridad, si hay usuarios externos que utilicen legalmente la red, es responsabilidad del administrador verificar que esas personas conozcan las políticas que se han establecido.

Esto es de particular importancia si se tiene que emprender acciones legales en contra de los transgresores, si se ha producido una pérdida significativa quizá se tendrá que tomar acciones más drásticas, si todo esto implica una publicidad negativa, cuando se prefiera arreglar la falla de seguridad y no emprender acción judicial.
Se podría tener una violación de la política de seguridad en la que el agresor sea un usuario interno, esto podría ocurrir en las siguientes situaciones:

- Un usuario local viola la política de seguridad de un sitio local

- Un usuario local viola la política de seguridad de un sitio remoto.

En el primer caso, debido a que se viola la política de seguridad interna, se tendrá más control sobre el tipo de respuesta ante esta violación de seguridad. En el segundo caso, un usuario local ha violado la política de seguridad de otra organización, esto podría ocurrir a través de una conexión como Internet, esta situación se complica por el hecho de que está implicada otra organización, y cualquier respuesta que se tome tendrá que discutirse con la organización cuya política de seguridad fue violada por el usuario local de la red.

2.5 DISEÑO DE UNA POLÍTICA DE SEGURIDAD

El primer paso para conformar una política de seguridad funcional para un sito es decir cuál es su opinión personal., debe tener una comprensión clara y explícita de lo que es la política interna antes de poder discutir con otra persona asuntos relacionados a fin de escribir una política para el sitio.

Con esto en mente, se deben observar las decisiones que ha tomado sobre seguridad y decidir cuáles se cree son las metas de seguridad del sitio, tal vez esa no sea la política final de éste, pero es un paso muy importante y será la base sobre la cual trabajará la seguridad de la organización.

2.5.1 Políticas de seguridad del Sitio

Una organización puede tener muchos sitios y cada uno contar con sus propias redes. Si los sitios están conectados por una red

interna, la política de red deberá agrupar las metas de todos los sitios que estén interconectados.
Cada sitio tiene al menos una política de seguridad, el problema es que la mayoría de los sitios tienen más de una; tal vez tantas como hay gente relacionada con las computadoras del sitio. A veces, la proliferación de políticas es del todo inconsciente; es posible que diferentes salas de cómputo dentro del mismo sitio hagan cosas radicalmente diferentes sin darse cuenta siquiera.

Pueden ser que hayan sido escritas algunas políticas de seguridad del sitio pero la mayoría tienden ha se implícitas y desconocidas . La única manera de averiguar si existen es preguntar. Asegúrese de preguntar a los gerentes, administradores de sistemas y usuarios.

En general, un sitio es cualquier parte de una organización que posee computadoras y recursos relacionados con la red. Dichos recursos incluyen, pero no se limitan a lo siguiente:

- Estaciones de trabajo.
- Computadoras anfitrión y servidores.
- Dispositivos de interconexión: compuertas, enrutadores, puentes, repetidores.
- Servidores de terminal.
- Software para red y aplicaciones.
- Cables de red.
- Información en archivos y bases de datos.

La política de seguridad del sitio debe tomar en cuenta la protección de estos recursos, debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas. Éste es un punto importante ya que es posible idear una política de seguridad que salvaguarde sus intereses pero que no sea dañina para los otros.

Puede ser que ya hayan sido escritas algunas de las políticas de seguridad de un sitio, pero la mayoría tienden a ser implícitas y desconocidas. La única manera de averiguar si existen es preguntar. Asegúrese de preguntar a los gerentes, administradores de sistemas y usuarios. Después observe las computadoras actuales y vea lo que ocurre en realidad. No es factible que alguien le mienta. Sin embargo puede decirle lo que creen que ocurre, o lo que desearían que ocurriera, o lo que saben que se supone debe ocurrir, en lugar de indicarle el estado real de las cosas.

2.5.2 Factores externos que influyen en las políticas de seguridad

Su sitio no es del todo independiente. Hay elementos fuera de un centro de cómputo que influyen en la política de seguridad. Incluyen requisitos legales, obligaciones contractuales y políticas organizacionales existentes.

Su organización puede tener, también, obligaciones contractuales para proteger la información. Si tiene en su sistema información de consumidores o clientes, quizá sus contratos lo hagan protegerla, si tienen código fuente o software preliberado

comercialmente, es casi seguro que tiene una licencia que le pida protegerlo.

Es posible que su organización también tenga políticas ya existentes que influyan en las políticas de seguridad. Con frecuencia son políticas sobre protección de la información, pero puede haber políticas que requieran que la gente tenga acceso a la información, en especial en universidades e instituciones públicas.

2.5.3 Diseño de la Política de Seguridad para la Universidad Técnica del Norte.

IDENTIFICACIÓN DE LOS RECURSOS.

HARDWARE

- Los computadores, terminales, impresoras no se deben mover del lugar asignado sin previo permiso del Administrador del Sistema.

- Jamás se preemitirá la manipulación de los computadores, impresoras y demás equipos por personas no autorizadas ya sean personas de la institución o ajenas a esta.

- No se permitirá el préstamo de ningún tipo de hardware ya sean tarjetas de red, monitores, teclados, mouse, Unidades Centrales de Procesamiento, impresoras, etc.

- La instalación de hardware nuevo es de exclusiva responsabilidad del Administrador del Sistema.

- El hardware nuevo debe poseer sus respectivas garantías en vigencia.
- El hardware que no este instalado ya sean tarjetas de red, mainboard, impresoras, etc., deben encontrarse guardados en armarios o anaqueles que posean llaves especiales.

- El hardware en su totalidad debe encontrarse debidamente inventariado.

- Se debe realizar periódicamente mantenimiento preventivo.

SOFTWARE

- Se debe poseer licencias de uso

- No se debe realizar prestamos de software sin previa autorización del Administrador del Sistema.

- Se debe mantener un control de inventario del software existente.

- Se debe realizar renovaciones periódicas de las licencias del Software.

- El Software debe mantenerse guardado en un lugar seguro y bajo llaves especiales.

- La instalación de nuevo Software es de responsabilidad del Administrador del Sistema.

- La manipulación del Software debe ser de sumo cuidado y guardando con las respectivas seguridades.

- No se debe permitir realizar copias del Software sin previa autorización del Administrador del Sistema.

DATOS

- Se debe acceder sólo a los datos y transacciones asignados.

- Antes de sacar información pregunte si tiene los permisos respectivos.

- Se debe salvaguardar la diseminación de información por teléfono, fax, o materiales impresos.

- El acceso inapropiado o el descubrimiento de información no autorizado puede ser catalogado como una violación de la política.

- La información impresa catalogada como confidencial debe ser tratado con el mismo cuidado que se trata los archivos confidenciales.

- El acceso a los sistemas administrativos se debe conceder solo al Administrador del Sistema.

- Los usuarios que intentan acceder a la información confidencial de manera no autorizada se someterán a medidas disciplinarias dispuestas por la institución.

- Se debe guardar en lugar seguro bajo llave los discos flexibles y cartuchos que contienen los datos del sistema teniendo en cuenta que la llave no debe ser normal.
- Para asegurar la información original se debe quemar los archivos impresos luego de ser utilizados.

- Se debe realizar la mayor cantidad de pantallas orientadas a prevenir la lectura de la información confidencial.

- El Administrador debe supervisar periódicamente el acceso de los usuarios del sistema.

- El almacenamiento de información en formas no electrónicas deben ser protegidas contra accidentes no predecibles ya sean estas destrucciones por personas no deseadas, deterioro del lugar de almacenaje, etc.

- El Administrador del Sistema es responsable de establecer las reglas para protegerlos.

- Si se encuentra con un caso raro de demanda de información el Administrador debe consultar con un Consejo General sobre la autorización para obtener información.

- El usuario autorizado para el acceso a la información debe tener en cuenta la manera de proteger la información.

- La persona autorizada al acceso de cualquier información se protegerá del uso u observación por personas no autorizadas.

- El usuario que accede a cualquier información se debe registrar antes de utilizar la información.

- El administrador es el encargado de adquirir, usar, cambiar, borrar los datos realizado un procedimiento adecuado con el cual la información tenga un buen respaldo.

- La instalación de la computadora mantendrá listas de personas autorizadas par acceder a las aplicaciones de las computadoras.

- Se debe realizar test para evaluar el correcto uso de las computadoras.

- Desarrolle programas para resolver problemas de emergencia suscitados en los datos del sistema.

- Los datos de niveles más altos de sensibilidad deben ser encriptados.

- Todas las copias de la información restringida debe etiquetarse de la manera mas clara posible.

- Para asegurar la integridad de los datos se puede requerir a técnicas avanzadas de backup de archivos.

- Los centros de datos deben encontrase en lugares mas seguros.

- Los centros de datos deben disponer de bóvedas seguras para poder guardar las cintas de backup.

- Los datos obtenidos en el transcurso del trabajo diario jamás serán usados de manera directa o indirectamente para cualquier propósito, sino únicamente para las tareas asignadas oficialmente.

- Después de la terminación del empleo con la Institución los datos administrativos deben ser confidenciales.

- Las autoridades deben proporcionar evidencia suficiente para acceder a los datos de los estudiantes o tener el permiso específico del estudiante.

- El personal que esta en goce de vacaciones o se ha retirado del trabajo temporalmente o por jubilación tiene derecho a acceder a sus datos personales.

- Si falleciere un miembro de la Institución, los representantes legales del mismo tendrán derecho a accesar a los datos o archivos hasta cinco años después de su muerte.

- Las impresoras y copiadoras usadas para obtener información confidencial deben estar en lugares seguros y supervisados por personal de seguridad.

- Cuando la información es totalmente delicada y confidencial no debe ser guardada en los discos duros, sino en disquetes y ser impresos en las impresoras de seguridad.

USUARIOS

- Se debe clasificar a los usuarios dependiendo de las necesidades.
- No se debe permitir la creación de usuarios innecesarios para la utilización de servicios del sistema.

- Cada usuario es responsable del hardware que ha sido asignado para su utilización.

- No se permite que el usuario manipule de ninguna manera el hardware de cualquier tipo.

- Los permisos que tengan los diferentes usuarios serán asignados por el Administrador del Sistema.

DOCUMENTOS

- Los manuales tanto de hardware como de software debe ser guardados en lugares seguros y bajo llave.

- El Administrador del sistema es el encargado de mantener en buen estado los documentos.

- Los documentos serán catalogados como confidenciales y no serán prestados sin previa autorización del Administrador del Sistema.

- Todos los documentos deben tener cualquier tipo de respaldo en caso de perdida o de deterioro.

- No se permitirá el préstamo de dichos documentos por periodos largos sin previa justificación.

- Se tomará como una violación de la Política de Seguridad si el documento que entrega el usuario se encuentra deteriorado ateniéndose este a las sanciones impuestas por el Administrador del Sistema.

SUMINISTROS

- Se debe mantener un control adecuado sobre las existencias.

- La reposición debe ser de una manera adecuada y oportuna.

- Los Suministros deben ser guardados en lugares que garanticen un buen estado y no exista pérdida.

- Será catalogado como una violación de la Política de Seguridad el uso inadecuado de los suministros en cualquier ocasión ateniéndose a las sanciones pertinentes.

- La transportación debe ser la mejor posible para evitar daños.

- Se debe disponer de proveedores calificados para que no fallen en la entrega de los suministros.

IDENTIFICACIÓN DEL USO NO AUTORIZADO

RED

- La seguridad para el acceso a la red estará basada en un identificador de usuario y una contraseña.

- Nadie debe intentar degradar el funcionamiento de un sistema de información de manera deliberada.

- Se recomienda que los usuarios transmitan su correo electrónico desde el servidor hacia las estaciones de trabajo.
- Se considera como violación a la Política de Seguridad si se interceptación información que no sea autorizada.

- El acceso a los servicios de la red involucra a menudo un retraso de mandos de seguridad que pueden incluir varios password diferentes.

- Para asegurar un orden legítimo de conectividad, el sistema de autentificación debe distinguir entre un usuario y su servicio para que nadie pueda acceder sin el permiso adecuado a tratar de obtener información del sistema.

- No se debe permitir usar la máquina para instalar juegos.

- No se debe impedir el uso de las redes poniendo reservas o claves sin la autorización respectiva del Administrador del Sistema.

- Si el usuario sabe que la capacidad de la máquina no es suficiente par instalar un determinado paquete y corre el riesgo de estar forzando la máquina debe informar al Administrador.

- Los usuarios no deben usar los sistemas de la Institución fuera de la misma.

- Si determinadas operaciones relacionadas con el funcionamiento del sistema se realizan para la comprobación de eficiencia y están autorizados por los miembros no deben considerarse como inadecuadas o mal usadas.

- El uso no debe interferir con el acceso de otros usuarios a los recursos y este uso no debe ser excesivo.

- El uso del sistema con fines de lucro personal debe contar con una autorización previa.

- Ordinariamente no es apropiado para los empleados convertir los recursos institucionales en esfuerzos privados.

- Las violaciones de esta política incluye conductas irrazonables que interfieren con el uso justo de los recursos de la informática por los demás usuarios.

- Nadie puede usar los medios de las computadoras de la institución para los propósitos impropios, como jugar bromas, etc.

- Los sistemas electrónicos no deben usar accesos "public" ya que permite la distribución anónima de información arbitraria.

SERVIDOR

- El servidor jamás deberá ser usado como una estación de trabajo, a excepción cuando el administrador lo necesite para propósitos de administrar el servidor en situación excepcionales.

- Los servidores deben estar ubicados en áreas físicamente seguras.

- Los cables de los servidores y conexiones deben estar protegidos si es posible.
- La contraseña del usuario root debe ser solo de conocimiento del Administrador del Sistema.

- El Servidor debe estar conectado a una fuente continua de energía

- El encargado de una máquina conectada a una red institucional es el único responsable de la conducta de esa máquina, y el tráfico de información desde esa computadora a la red.

- Queda terminantemente prohibido el acceso a la red por parte de computadoras externas que no sean propiedad de la Institución.

- El administrador puede desconectar a cualquier máquina (computadora) que este utilizada de manera inapropiada los recursos de la red ya sea con fines de ganancia.

- No se puede ingresar más equipos de computación a la red ya que se considera una violación de está política.

- La instalación de otros computadores será realizada por el Administrador del Sistema.

- Todas las acciones de desorden dentro de la red están sujetos a reglas disciplinarias institucionales.

ESTACIONES DE TRABAJO (workstation)

- Los usuarios son los responsables de la estación de trabajo que están utilizando ya sea guardando la información del disco duro, instalando y usando el software de protección de virus.

- El uso no autorizado del software comprado o desarrollado por la institución es considerado como una violación a esta política.

- No se debe cerrar con llave una computadora o cualquier otro dispositivo que vaya a ser utilizado o este catalogado de acceso público.

- Queda prohibido la instalación de software y hardware sin previo permiso del Administrador.

- Los usuarios no deben utilizar las estación de trabajo sin previo permiso del Administrador del Sistema.

- Los usuarios deben informar al Administrador en caso que la computadora necesite reparaciones.

- Queda terminantemente prohibido intentar componer las computadoras que estén utilizando, de esta manera se protegerá la confidencialidad de los datos guardados en el sistema.

- No se quitará equipos de ninguna área de trabajo de la institución sin previa información al administrador y sin su autorización.

CONTRASEÑAS

- Los usuarios son los únicos responsables de su ID.
- Los usuarios son responsables de las tareas realizadas con su ID por lo cual debe ser guardado de una manera segura.

- Si el ID está perdido, el usuario de informar de la manera más rápida y oportuna para realizar la cancelación del mismo.

- Evite guardar las contraseñas en las Computadoras.

- No guarde la contraseña en una cinta en la pared, bajo el teclado o en otras áreas fáciles de ser descubiertas.

- Se debe permitir a cada usuario el cambio de su contraseña después de un período de tiempo.

- El software del sistema debe mantener un historial de contraseñas utilizadas.

CONFIDENCIALIDAD

- Los usuarios son responsables de realizar procesos con información confidencial.

- Si usted sabe como proteger su información, protéjala ya que el sistema, no sabe guardar información de personas inescrupulosas que desean hacerle daño.

RECURSOS MAL UTILIZADOS

- Los usuarios deben usar el hardware y el software de las computadoras para el objetivo que fueran adquiridas.

- El acceso a información sin la autorización respectiva y que ocasione destrucción, alteración o desconfiguración en los archivos es una violación a las políticas establecidas por la Institución.

- El Administrador del Sistema puede solicitar la investigación completa (Auditoria Informática) de archivos y datos para obtener la confirmación respectiva en caso de sospechar de una violación de datos.

- Las computadoras de una institución pueden ser mal usadas como por ejemplo para planificar el cometimiento de un crimen.

IMPRESIONES

- Impresión deliberada de manera intencional de documentos innecesarios o de archivos múltiples será considerada como una violación de la Política de Seguridad.

- No se deben imprimir archivos sin las revisiones respectivas.

- Se debe imprimir solo archivos relacionados con el trabajo y no con su vida personal.

RIESGO DE REVELACIÓN DE INFORMACIÓN

DATOS Y DOCUMENTOS

- Los empleados institucionales no pueden usar la información privada para beneficios propios ni menos obstruir el uso de la información para el uso apropiado por la institución.

- Esta considerado como una violación de esta política el uso desautorizado de la información para obtener ganancia propia o para propósitos malévolos.

- Los usuarios no pueden usar datos en cualquier aplicación y menos en aplicaciones que reproducen datos oficiales para el Administrador.

- Los controles superiores de los sistemas de información deben proporcionar la habilidad de rastrear las violaciones de seguridad para los usuarios para poder encontrar responsables.

- El código fuente de los programas deben ser de uso exclusivo para la institución.

- No se debe permitir la reproducción parcial y peor aun total de estos documentos.

BACKUPS

- Se debe tener un buen plan de copias de seguridad.

- Las copias de seguridad deben ser guardadas en un lugar seguro y bajo llave.

- Debe existir por lo menos dos copias de la misma información guardadas en diferentes lugares.

- Debe existir Backups de los archivos importantes de manera periódica.

- Los archivos de Backup deben guardar un histórico para ser utilizado cuando se desee.

SEGURIDAD FÍSICA

- Los usuarios son responsables de entrar a áreas no permitidas.

- Las áreas de seguridad deben ser protegidas mediante llaves, tarjetas, etc.

- Las computadoras deben poseer una buena instalación.

- Se debe tener planes de contingencia con respecto a las instalaciones y al hardware.

- No se debe permitir el acceso de los usuarios a horas que no tengan su debida autorización.

SERVICIOS

- Unicamente se brindarán servicios que sean importantes y necesarios para que la Insitución tenga reconocimiento dentro de Internet.

- Cada servicio será configurado de tal manera que el acceso quede restringido solamente para los usuarios que poseean los permisos adecuados.

- Los usuarios que accedan a cualquier servicio que se brinde, deberán hacerlo dentro de los límites establecidos.
- Se deberá revisar de manera periódica los archivos de log, para controlar los usuarios que han ingresado al sistema.

- El Administrador deberá realizar un mantenimiento a las carpetas de correo electrónico de los usuarios.