00623
21

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

LA CRIPTOGRAFÍA COMO UNA HERRAMIENTA DE SEGURIDAD PARA PROTEGER LA INFORMACIÓN DE SISTEMAS EN RED.

TESIS PROFESIONAL QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN INFORMÁTICA

PRESENTA:

ROCIO RÍOS SERVÍN

ASESOR:
DR. RICARDO RIVERA SOLER

MÉXICO, D. F. 2003.

A

AGRADECIMIENTOS

A mis padres

Margarita y Ernesto

Porque gracias a su esfuerzo, sacrificio y ejemplo hoy llego a la etapa final de mi carrera.

A mis hermanos

Eva, Ernesto, Mago, Conchita y Lalo

Porque siempre me dieron un ejemplo a seguir y contribuyeron de una forma importante para que terminara mis estudios.

A Dios

Porque me ha permitido vivir el tiempo necesario para ver realizada una más de mis metas.

DEDICATORIAS

A mi esposo

Charly

Porque has sido testigo de mi esfuerzo desde el inicio hasta el fin de mi carrera, porque siempre me has brindado apoyo incondicional y porque sé, que siempre estarás conmigo en cada nuevo reto que se presente. Te amo.

A mis padres

Margarita y Ernesto

Porque sin su apoyo no hubiera sido posible la culminación de mis estudios. Gracias por darme la vida.

A mis hermanos

Eva, Ernesto, Mago, Conchita y Lalo

Porque durante toda mi etapa como estudiante me brindaron ayuda y orientación siempre que lo necesité. Los quiero mucho.

C

ÍNDICE

INTRODUCCIÓN

INTRODUCCIÓN

En la actualidad las redes de computadoras se encuentran funcionando en casi todo el mundo y la transmisión de información entre ellas se ha vuelto la práctica más importante entre las organizaciones que las utilizan, al mismo tiempo ha surgido la necesidad de proteger la información que se transmite, debido a esto el hombre ha creado diversos métodos de protección de datos e información.

En el presente trabajo muestro a la criptografía como una de estas herramientas para protección de sistemas en un panorama general se habla de la seguridad de redes mencionando los servicios que deben proporcionar éstas, los sistemas más representativos de las técnicas criptográficas; así como un análisis de información proporcionada por empresas establecidas en México y que se dedican a la venta de soluciones basadas en criptografía para seguridad de redes.

El contenido de esta tesis se divide en seis partes principales, las cuales se presentan como sigue:

Marco problemático
En este capítulo se presentan los antecedentes e interés en el estudio del tema, así como el tratamiento de la problemática identificando y delimitando el problema; se muestran las opiniones recopiladas de personas con conocimientos profesionales y empíricos en el tema.

Marco teórico
Este capítulo contiene la recopilación de todas la fuentes de información que fueron consultadas para la realización de este trabajo, libros, tesis, revistas, páginas web, etc.

Marco conceptual
Se presenta un desarrollo del tema objeto de estudio, antecedentes de la criptografía, criptografía de llave pública y privada, principales algoritmos que definen cada una, ventajas y desventajas de utilizarla, así como un repaso de la seguridad en redes y las amenazas a las que están expuestas.

Marco metodológico
Se presenta el estudio realizado por medio de entrevistas a personas calificadas con conocimientos teóricos y prácticos en el tema, con estos resultados se llega a la aprobación de la hipótesis.

Marco instrumental
En este capítulo se presentan las acciones tomadas y algunas más a tomar como resultado de este estudio.

Conclusiones
Se presentan de forma general los resultados obtenidos de este estudio.

PAGINACION DISCONTINUA

MARCO PROBLEMÁTICO

1. MARCO PROBLEMÁTICO

1.1 Antecedentes

En la actualidad la mayoría de las personas sabemos de la gran facilidad y libertad con que se puede conseguir todo tipo de información, hoy en día se llega a creer que esta libertad de información trae consigo sólo consecuencias benéficas para la sociedad, pero también es factible que así como esta libertad de información y expresión brinda grandes beneficios pueda traer consigo algunas desventajas que vale la pena analizar.

El uso de internet y redes de computadoras ha proliferado en los últimos años y el porcentaje de personas que tienen acceso a este servicio cada vez va en aumento, esto da una idea de que un mayor porcentaje de la población mundial tiene la posibilidad de consultar datos y /o información a través de una computadora, la cual muchas veces se encuentra en conexión con otras, es decir en una red; internet es uno de los mejores ejemplos que podemos tomar de esta conexión entre computadoras.

Cada día mas y más computadoras están conectadas en red, compartiendo información y datos, realizando transacciones bancarias o comerciales, impartiendo cursos en línea, publicando software, haciendo publicidad de productos de todo tipo, o simplemente proporcionando diversión a aquellas personas que navegan por la red en busca de distracción, pero todas estas computadoras están expuestas a ser objeto de un ataque o intromisión, es por ello que el tema de la seguridad en los equipos de cómputo ha cobrado verdadera importancia en los últimos tiempos, todas estas máquinas deberían tener un adecuado sistema de seguridad informático para evitar ser víctimas de ilícitos , sin embargo muchas veces no sucede así y las empresas y organizaciones llegan a tener grandes pérdidas, debido a ataques a sus sistemas de información.

La seguridad para cualquier tipo de sistema es un punto muy importante que no debe olvidarse, más aún si se trata de un sistema conectado en red; ya que éstos tienen un mayor índice de probabilidad de ser objeto de un ilícito; aún quienes utilizan las computadoras por mera distracción o como usuarios finales han llegado a ser víctimas de ataques en sus diversas formas.

Hablar sobre la seguridad informática exige tener un conocimiento vasto sobre el tema, ya que así como ha proliferado el uso de redes, así también han aumentado los índices de delitos cometidos a través de ellas; si consideramos que así como mucha gente descubre internet día a día, así también muchos de ellos cometen conductas ilícitas. El descubrimiento de esta red, su apertura y fácil acceso ha dado lugar a que un sin número de personas hagan uso ilícito de datos e información que fluyen a través de ella.

Para evitar todo este tipo de situaciones el hombre ha inventado diversos métodos o herramientas de seguridad, muchas de ellas son muy eficaces, aunque ninguna es cien por ciento segura; como ejemplos podemos mencionar los firewalls, programas antivirus, los métodos de autenticación y la criptografía; esta última se ha utilizado desde hace muchos siglos, tal vez no en una modalidad computacional, pero ya existían los mensajes cifrados en la escritura antigua.

La criptografía es una herramienta eficaz para la protección de la información de los sistemas en red, y cada vez va cobrando mayor popularidad entre la gente dedicada al cómputo; muchas veces no como una precaución sino como un componente indispensable ante la necesidad de enviar y recibir información íntegra y con un bajo porcentaje de probabilidad de riesgo.

Sin embargo todavía muchas de las personas y empresas mexicanas que han sistematizado sus procesos no se preocupan lo suficiente por estar al tanto de la seguridad de sus equipos, así como de sus sistemas, algunos piensan, erróneamente que "**nada puede pasarles**", y dejan de lado lo que tiene que ver con la seguridad de sus sistemas de información; cuando por alguna razón se comete un ataque o intromisión en su contra, se encuentran en desventaja, ya que no cuentan con la infraestructura ni el conocimiento necesario para superarlo; después de esto tal vez se vuelvan más cuidadosos en el aspecto de la seguridad de redes.

Un ejemplo real que puedo mencionar y que tiene que ver con el tema se trata del Sistema de Universidad en Línea de la Facultad de Contaduría y Administración de la UNAM; este sistema fue creado para que los alumnos del Sistema de Universidad Abierta puedan cursar las materias de su carrera vía Internet. Por experiencia propia puedo decir que este tipo de sistema en red, es consultado por varias personas a la vez, y son muchas las intromisiones que se sufren a diario, personas que están interesadas en acceder a una computadora o al servidor sin tener los permisos correspondientes, algunos más enviando mensajes con contenidos perjudiciales, y esto sólo por mencionar algunos ejemplos; afortunadamente existen herramientas de seguridad que hasta el momento han garantizado que la información siempre sea íntegra; pero en esta experiencia es donde se pone de relieve lo frágil que puede ser la seguridad en un sistema en red, y que cometer un ataque es relativamente fácil para una persona que tenga conocimientos de informática y que se proponga efectuarlo.

Otro aspecto importante se refiere a la información que tienen las personas responsables de administrar los sistemas, son ellos quienes deben estar informados en primera instancia de la gravedad que puede implicar un ilícito cometido en contra de sus sistemas, así como conocer las herramientas que existen para la protección de los mismos y son ellos también quienes deben poseer los conocimientos necesarios para saber diferenciar entre una conducta normal y un ataque o intromisión informática, si ellos están informados y transmiten sus conocimientos a las personas que laboran bajo su mando; sus sistemas serán utilizados de forma correcta, no así, si desconocen los delitos de los que pueden ser objeto y las formas de cómo protegerse.

La finalidad de este trabajo de tesis es establecer a la criptografía como una de las herramientas más óptimas para proteger la información de un sistema conectado en red, sin dejar de lado la mención de los posibles ataques a los que están expuestos dichos sistemas; por lo anterior se ha denominado este trabajo de tesis como. "La criptografía como una herramienta de seguridad para proteger la información de sistemas en red".

1.2 Identificación del problema

El hombre en general siempre se ha preocupado por salvaguardar sus intereses y una de sus necesidades básicas es la seguridad; en la actualidad esta necesidad de seguridad se ha extendido hasta el ámbito de la computación y las telecomunicaciones y donde el uso de herramientas y técnicas adecuadas pueden ser una garantía de que la información de las organizaciones tendrán menor riesgo de ser objeto de un ilícito.

Actualmente existen algunas carencias en cuanto a la seguridad de los sistemas de información en nuestro País; a diferencia de los países de primer mundo, México aún tiene deficiencias y atrasos en lo que se refiere a tecnologías de seguridad, y esto trae como consecuencia que los sistemas de información en red sean más vulnerables a intromisiones.

Otro punto crítico es la falta de una cultura de seguridad informática entre los usuarios y responsables de los sistemas; aunado a esto muchas veces la economía de nuestro País no permite realizar una inversión considerable de recursos para el desarrollo e implantación de sistemas que garanticen la seguridad e integridad de los datos e información.

Algunos usuarios y/o administradores consideran que **"nada les pasará a sus sistemas"** y se conforman con usar passwords o algún antivirus (en el mejor de los casos), creen, erróneamente que esto es suficiente para proteger su información, no se dan cuenta que el perjuicio que ocasionan los ataques informáticos es cuantioso; cuando se trata de un ataque grave; y que el daño causado puede traer consigo consecuencias materiales o monetarias muy serias para las empresas y usuarios.

Una opción para hacer más segura la información es el cifrado, es decir usar criptografía como una herramienta eficaz para la protección de la información en su viaje a través de una red, desgraciadamente no muchas personas están concientes de los beneficios que puede traerles este tipo de herramientas y no la toman en cuenta como una buena opción.

Todo lo que se ha mencionado muestra en forma general uno de los problemas a los que se enfrentan los usuarios de las redes de computadoras, debido a que no hay nada que les garantice que la información que envíen o reciban llegará íntegra hasta su destino.

1.3 Demarcación del fenómeno

Tomando en cuenta que ningún equipo y/o sistema informático se encuentra libre del riesgo de un ataque, se hace difícil demarcar el problema ya que las redes de computadoras están presentes en casi todo el mundo y esto a su vez representa un conflicto para la demarcación del fenómeno del presente estudio, puesto que una persona tiene relativa facilidad para interceptar la información en cualquier punto de su viaje sin ser descubierta, y esta persona puede encontrarse también en cualquier parte del mundo.
Debido a la amplitud del tema, en este estudio el problema se delimita solamente a la Ciudad de México.

1.4 Conocimiento empírico en el medio

Para indagar información a cerca del tema se aplicará un cuestionario a personas que tienen conocimientos teóricos y prácticos en el área de cómputo, aunque su área de desarrollo no sea la seguridad, pero que de alguna forma están involucradas en actividades relacionadas y pueden dar una opinión valiosa que contribuya a la realización de este trabajo de tesis.

1.4.1 Objetivo

El objetivo es conocer la opinión de personas empíricas en el tema pero que viven de cerca la problemática antes mencionada.

1.4.2 Definición de las preguntas

A continuación se presenta un análisis de las preguntas incluidas en el cuestionario propuesto para obtener información relacionada al tema "Análisis de la criptografía como herramienta de seguridad para proteger la información de sistemas en red"

1. ¿Cree usted que la información que viaja a través de las redes de computadoras sea segura? ¿Por qué?	
Justificación: Con esta pregunta es posible unificar criterios a cerca de la seguridad con la que viajan los datos e información a través de una red; así como conocer la opinión de cada persona de acuerdo a su experiencia. Si se da la respuesta esperada, esta pregunta permitirá constatar que es necesario hacer énfasis en el tema de la seguridad de los sistemas.	**Respuesta esperada:** No. Porque en cualquier momento puede ser interceptada y modificada o destruida.

2. ¿Cuáles cree usted que son las principales ventajas y desventajas de transmitir datos o información a través de una red?	
Justificación: Esta pregunta está relacionada con la anterior y permite tener una visión más amplia en cuanto a los aspectos positivos y negativos de la transmisión de datos e información en una red; permitirá conocer si es mayor el porcentaje de ventajas mencionadas o el de desventajas.	**Respuesta esperada:** Ventajas: rapidez, disponibilidad inmediata, entre otras. Desventajas: Inseguridad

3. ¿Considera usted que los datos e información que obtiene de los sistemas con los cuales trabaja diariamente son seguros? ¿Por qué?	
Justificación: Permite conocer hasta qué grado el encuestado confía en los sistemas con los que trabaja diariamente; esto da una idea de qué tanto se ha preocupado el usuario o administrador, por hacer que los sistemas con los que trabajan sean seguros.	**Respuesta esperada:** Aunque sería mejor que la respuesta fuera si en todos los casos; para efectos de este trabajo de tesis y demostración afirmativa de la hipótesis se espera una respuesta negativa.

4. ¿Conoce algún tipo de tecnología que proteja a los sistemas de ataques informáticos? Menciónelo	
Justificación: La respuesta a esta pregunta permitirá tener una perspectiva más amplia de las herramientas que existen hoy en día para proteger los sistemas e información contra ataques informáticos; además de inferir qué tanto saben las personas encuestadas a cerca de este tipo de herramientas.	**Respuesta esperada:** Afirmativa. Se espera obtener mención de por lo menos tres de las herramientas de protección de datos, como son: criptografía, firewalls, métodos de autenticación, antivirus, entre otros.

5. ¿Utiliza algún mecanismo de seguridad contra ataques informáticos en el lugar donde trabaja? Menciónelos.	
Justificación: Permite tener una visión sobre qué tan frecuente es el uso de mecanismos de seguridad en las diferentes organizaciones donde laboran los cuestionados, así como un conocimiento sobre la preocupación que existe por tener 'sistemas e información seguros'.	**Respuesta esperada:** Si. Siempre se utilizan. Además de hacer mención de algunos de estos mecanismos de seguridad.

6. ¿Para usted qué es un sistema de información seguro?	
Justificación: Esta pregunta permitirá tener diferentes puntos de vista en cuanto al concepto de seguridad, ya que cada persona, dependiendo de sus conocimientos, experiencia y necesidades, efectuará una definición. Con la conjunción de estas definiciones se podrá llegar a una general.	**Respuesta esperada:** Es aquel sistema que esta siempre disponible y que permite que la información que se obtiene de el sea confiable; y respuestas similares.

7. Mencione de acuerdo a su criterio las principales características que debería tener un sistema de información seguro?	
Justificación: Esta pregunta permitirá conocer algunas características que debe tener un sistema para considerarse seguro, de esta forma se contribuye a los conceptos que se manejan en el presente trabajo; haciendo énfasis en que debe protegerse la información.	**Respuesta esperada:** Disponibilidad, rapidez, confiabilidad e integridad de la información.

8. De las siguientes opciones numere en orden de importancia aquellas con las que debe contar un sistema de información seguro. 1- Más importante 4- Menos importante ____ Firewalls ____ Métodos criptográficos ____ Métodos de autenticación ____ Programas Antivirus ____ Otro (menciónelo) _____	
Justificación: Con esta pregunta se constatará si la criptografía en realidad se trata de una herramienta útil y eficaz en la protección de la información de sistemas en red.	**Respuesta esperada:** Se espera que las menciones más importantes sean para la criptografía, ya que es un medio eficaz para proteger la información que viaja de un sistema a otro.

9. ¿ Considera que hace falta difundir una cultura de seguridad informática en México? ¿ Por qué?	
Justificación: Proporciona una visión acerca de la idea que tienen los encuestados sobre la situación de México y la seguridad informática en nuestros días.	**Respuesta esperada:** Si. Porque no es suficiente lo que se sabe y además mucha gente no hace uso de herramientas de seguridad.

1.4.3 Definición de las personas entrevistadas

- ☑ Miriam Fernández Galicia
  Licenciada en Informática. Egresada de la UNAM
- ☑ Catalina Román
  Licenciada en Informática egresada de la Universidad Tecnológica (UNITEC)
- ☑ Humberto Rétiz Ramírez
  Pasante de Ingeniería en Comunicaciones y Electrónica
  PC-TV Televisión por Cable. Departamento de Sistemas

1.4.4 Cuestionario Piloto

Antes de llevar a cabo la aplicación del cuestionario definitivo se realizó un cuestionario piloto, con el fin de conocer si la información que se pedía era realmente de utilidad, así como corregir errores de redacción, modificar y aumentar algunos conceptos en las preguntas, así como determinar el tiempo de respuesta; este cuestionario piloto se aplicó a cinco personas, después de esto se hicieron las correcciones pertinentes y se elaboró el cuestionario definitivo, mismo que aparece en el anexo de esta sección.

1.4.5 Aplicación del cuestionario y recopilación de la información

1. ¿Cree usted que la información que viaja a través de las redes de computadoras sea segura?		
Miriam Fernández	**Catalina Román**	**Humberto Rétiz**
No. Hay varias formas de acceder a las computadoras en caso de que estas no tengan medios de seguridad, además los usuarios en México desconocen como proteger su información.	No. En redes normales no. El que sea seguro o no, depende de la forma en que se transmita y que tipo de red se utilice.	No. Porque siempre habrá forma de violar la privacidad o destruir la información.
2. ¿Cuáles cree usted que son las principales ventajas y desventajas de transmitir datos o información a través de una red?		
Ventajas: Compartir y acceder a la información que uno desee rápidamente y teniendo varias opciones. *Desventajas.* Si no se tienen precauciones, es más fácil para un hacker accesar a la información.	*Ventajas:* Se puede obtener información de una forma rápida y segura y se puede tener control de la misma, esto también depende del tipo de red. *Desventajas:* La información no siempre es segura y para tener una red altamente segura se requiere de altos costos.	*Ventajas:* Rapidez, comodidad, disponibilidad de recursos. *Desventajas:* vulnerable a ataques, circulación de virus, saturación de usuarios.
3. ¿Considera usted que los datos e información que obtiene de los sistemas con los cuales trabaja diariamente es segura? ¿Por qué?		
No. Debido a que diariamente se trabaja en red, creo que nunca se puede garantizar que la información sea segura, pero si poner los mayores obstáculos posibles para que no accesen a la información.	No. Porque la información la accesamos a través de la red.	No totalmente, por la intercepción o destrucción de información, por virus y también por fallas eléctricas.

4. ¿Conoce algún tipo de tecnología que proteja a los sistemas de ataques informáticos? Menciónelo		
Miriam Fernández	**Catalina Román**	**Humberto Rétiz**
Si. OpenBSD en Linux y Antivirus.	No.	Antivirus
5. ¿Utiliza algún mecanismo de seguridad contra ataques informáticos en el lugar donde trabaja? Menciónelos		
Si. Restringiendo los accesos de máquinas remotas al servidor, monitoreo de accesos y en máquinas Windows se utilizan antivirus.	Se utilizan algunas herramientas de seguridad para conectarse como ssh. Se utiliza TCP wrappers para permitir el acceso a una determinada máquina a través de los servicios permitidos para ella.	Si. Programas antivirus y detección de información de procedencia insegura.
6. Para usted ¿Qué es un sistema de información seguro?		
Un sistema del cual se tenga pleno conocimiento de cómo funciona, permitiendo controlar la información, ya sea restringiéndola o bien compartiéndola.	Aquel que va a mantener mi información segura, el cual va a permitir acceso a la información solo a personas autorizadas.	Creo que no hay un sistema de información 100% seguro, aunque adoptando ciertas medidas aumenta la seguridad.
7. Mencione de acuerdo a su criterio las principales características que debería tener un sistema de información seguro.		
Confiable, consistente, veraz e integro.	Integridad de datos, control de acceso seguro, envío de información encriptada, un servidor que asigne claves aleatorias para cifrar los mensajes con el ordenador.	Oportunidad, veracidad de la información.
8. De las siguientes opciones numere en orden de importancia aquellas con las que debe contar un sistema de información seguro. 1- Más importante 4- Menos importante **____ Firewalls ____ Métodos criptográficos ____ Métodos de autenticación** **____ Antivirus ____ Otro (menciónelo)**		
1.Métodos criptográficos 2.Métodos de autenticación 3.Firewalls 4.Antivirus	1.Métodos de autenticación 2.Métodos criptográficos 3.Firewalls 4.Antivirus	1.Antivirus 2.Métodos criptográficos 3.Métodos de autenticación 4.Firewalls

9. ¿Considera que hace falta difundir una cultura de seguridad informática en México? ¿Por qué?		
Miriam Fernández	Catalina Román	Humberto Rétiz
Si. La mayoría de las personas solo usan la computadora como una herramienta de trabajo pero desconocen como proteger su información.	Si. Sería bueno que todos aquellos quienes manejan información importante sepan que hacer para mantenerla segura.	Si. Por la importancia mayor cada día que tiene el intercambio de información electrónica.

1.4.6 Conclusiones por pregunta

1. ¿Cree usted que la información que viaja a través de las redes de computadoras sea segura?

No. La información siempre es susceptible de ser modificada o destruida en su viaje a través de una red, y nada garantiza que llegue íntegra a su destino, mucho menos si no se cuenta con adecuadas herramientas y medidas de seguridad en los sistemas de información.

2. ¿Cuáles cree usted que son las principales ventajas y desventajas de transmitir datos o información a través de una red?

Existen tanto ventajas como desventajas en este aspecto; entre las primeras se señalan: rapidez, control, comodidad y ahorro de tiempo; mientras que las desventajas mencionadas fueron: inseguridad, virus e intercepción de la información como las más relevantes. Aunque el uso de sistemas en red proporciona muchas ventajas; no están libres de riesgos y de esto se encuentran plenamente concientes las personas entrevistadas.

3. ¿Considera usted que los datos e información que obtiene de los sistemas con los cuales trabaja diariamente es segura? ¿Por qué?

No. Porque la información se accesa a través de las redes y éstas son inseguras.

4. ¿Conoce algún tipo de tecnología que proteja a los sistemas de ataques informáticos? Menciónelo

Si. Los entrevistados conocen antivirus como una herramienta de protección y también se señalaron herramientas de protección para las conexiones como ssh para permitir acceso a las máquinas remotas.

5. ¿Utiliza algún mecanismo de seguridad contra ataques informáticos en el lugar donde trabaja? Menciónelos

Si. Se utilizan filtrados de información, antivirus, así como restricción de acceso a máquinas remotas y monitoreo de accesos.

6. Para usted ¿Qué es un sistema de información seguro?

Es un sistema que solo permite el acceso a personas y equipos autorizados y que la información que comparte es controlada y restringida.

7. Mencione de acuerdo a su criterio las principales características que debería tener un sistema de información seguro.

Las principales características de un sistema en red seguro son: confiabilidad, consistencia, integridad, veracidad, envío de información cifrada y control de acceso.

8. De las siguientes opciones numere en orden de importancia aquellas con las que debe contar un sistema de información seguro. 1- Más importante 4- Menos importante
____ Firewalls ____ Métodos criptográficos ____ Métodos de autenticación
____ Antivirus ____ Otro (menciónelo)

La mayoría de las menciones más importantes fueron para los métodos criptográficos y para los métodos de autenticación, por lo que se concluye que estas dos opciones deben ser tomadas en cuenta en el correcto funcionamiento de un sistema de información seguro.

9. ¿Considera que hace falta difundir una cultura de seguridad informática en México? ¿Por qué?

Si. La mayoría de la gente usa solo la computadora como herramienta de trabajo pero no sabe como proteger su información. Todos aquellos que manejan información y sistemas en red deberían saber los procedimientos a seguir para mantenerla segura.

1.4.7 Conclusiones generales sobre el cuestionario aplicado a empíricos.

1. La información que viaja a través de las redes de computadoras nunca es cien por ciento segura ni confiable, ya que puede ser interceptada y modificada o destruida durante su viaje por una red.
2. Aunque existen muchas ventajas en el uso de sistemas de información en red, no esta libre de riesgos y aunque esta información que se obtiene diariamente en estos sistemas es revisada por varios filtros siempre existe la posibilidad de que esté corrompida.
3. Se conocen muchas herramientas de seguridad para protección de los sistemas, pero no se usan en todos los casos.
4. Las principales características de un sistema seguro son: la confiabilidad, la integridad y la consistencia, aunque siempre queda el riesgo de sufrir un ataque ya que no hay un sistema que garantice la seguridad en su totalidad.
5. La criptografía es una herramienta necesaria en la protección del envío y recepción de información entre sistemas en red.
6. Es necesario difundir una cultura de seguridad informática en México ya que los usuarios y administradores de sistemas carecen de estos conocimientos y esto los hace más vulnerables a ataques.

1.5 Opiniones profesionales

Se aplicarán cuestionarios a personas que tienen conocimientos teóricos y prácticos, así como un desarrollo profesional en el área.

1.5.1 Objetivo

Conocer las opiniones de personas calificadas con conocimientos teóricos y prácticos, lo cual proporcionará una visión más amplia sobre el tema, así como un conocimiento más exacto de la información relacionada con este trabajo de tesis.

1.5.2 Definición de las personas entrevistadas

- ☑ Luz María Ramírez Romero
  Licenciada en Informática
  Coordinadora de servicios de seguridad y redes.
- ☑ Rubén Aquino Lara
  Ingeniero en Computación
  Coordinador de Departamento de Seguridad Informática.
- ☑ Lourdes Yolanda Flores Salgado
  Licenciada en Informática
  Administradora de Sistemas
- ☑ Alejandro Núñez Sandoval
  Ingeniero en Computación
  Técnico Académico- UNAM, Departamento de Seguridad DGSCA

1.5.3 Aplicación del cuestionario y recopilación de la información

1.¿ Cree usted que la información que viaja a través de las redes de computadoras sea segura?			
Luz María Ramírez	**Rubén Aquino**	**Lourdes Flores**	**Alejandro Núñez**
No. La mayoría de las veces viaja en claro y cualquier programa *sniffer* puede verla sin problema.	Depende de cómo viaje la información. Si viaja *en claro* no es segura. Si viaja por un canal cifrado y se usa un buen algoritmo podría considerarse segura.	No. Es relativamente fácil analizar las tramas que viajan por la red y de esa forma ver su contenido.	Depende de la infraestructura con la que se cuente (ejemplo telnet, ftp) son inseguros; mientras que ssh es seguro.

2. ¿Cuáles cree usted que son las principales ventajas y desventajas de transmitir datos o información a través de una red?			
Luz María Ramírez	**Rubén Aquino**	**Lourdes Flores**	**Alejandro Núñez**
Ventajas: Compartirla, mejorar la comunicación en la institución, facilitar el trabajo. *Desventajas:* Inseguridad, falta de confidencialidad y peligro de la integridad de la información.	*Ventajas:* Facilidad, velocidad. *Desventajas:* Canales inseguros	*Ventajas:* Rapidez, no se requiere de medios secundarios alternos, permite disponibilidad más eficiente. *Desventajas:* La información esta expuesta a ser leída e incluso modificada por externos.	*Ventajas:* Disposición de datos desde cualquier lugar de la red.
3. ¿Considera usted que los datos e información que obtiene de los sistemas con los cuales trabaja diariamente es segura? ¿Por qué?			
No. No hay sistemas 100% seguros.	La información de nuestros servidores y algunos conocidos si es segura; sin embargo en la información de la red externa no tengo garantía de que sea segura.	Si. Tenemos mucho cuidado en verificar que la información sea consistente y utilizamos medios seguros de transmisión de datos.	Si. Porque el departamento cuenta con una infraestructura de seguridad, firewalls, auditing systems.
4. ¿Conoce algún tipo de tecnología que proteja a los sistemas de ataques informáticos? Menciónelo			
Si. Firewalls, herramientas como ssh, pgp, servidores proxy, antivirus, etc.	Si. Mecanismos de autenticación, cifrado, detección de intrusos, firewalls.	Si. Actualización y parches del sistema y también el filtrado externo a nivel ruteador, e incluso los firewalls.	Firewalls, IDS, Antivirus, Hosts intrusión detection
5. ¿Utiliza algún mecanismo de seguridad contra ataques informáticos en el lugar donde trabaja? Menciónelos			
Si. Tcp wrappers, antivirus y no utilizamos Microsoft Outlook.	Si. Mecanismos de autenticación, mecanismos y herramientas que implementan un canal cifrado (ssh, ssl)	Si. Parches del sistema, herramientas de seguridad como tcp wrappers. Filtrado a nivel ruteador. Herramientas de transmisión segura como ssh y ssl. Además se cuenta con un oficial de seguridad permanente que realiza un monitoreo constante de los equipos.	Si Firewalls, IDS, Antivirus, Hosts intrusion detection.

6. Para usted ¿Qué es un sistema de información seguro?			
Luz María Ramírez	**Rubén Aquino**	**Lourdes Flores**	**Alejandro Núñez**
Aquel que asegura la confidencialidad de la información, su integridad y que evita los ataques de negación de servicio.	Un sistema que se comporta como los usuarios esperan que lo haga y que contempla aspectos fundamentales de privacidad, integridad y disponibilidad.	Un sistema en el cual puedo confiar que la información va a ser correcta e integra, además de disponible.	Un sistema que proporciona integridad de los datos, autenticación y confidencialidad.
7. Mencione de acuerdo a su criterio las principales características que debería tener un sistema de información seguro.			
Que asegure la integridad y la confidencialidad de la información. Que evite ataques de negación de servicio.	Privacidad, integridad, disponibilidad y no repudio.	Confiabilidad, integridad y disponibilidad.	Proporcionar las características anteriores a través de herramientas como ssh, ssl, firewalls, etc.
8. De las siguientes opciones numere en orden de importancia aquellas con las que debe contar un sistema de información en red seguro. 1- Más importante 4- Menos importante **____ Firewalls ____ Métodos criptográficos ____ Métodos de autenticación** **____ Antivirus ____ Otro (menciónelo)**			
1. Métodos criptográficos 2. Métodos de autenticación 3. Firewalls 4. Programas antivirus.	1. Métodos de autenticación 2. Programas antivirus 3. Métodos criptográficos 4. Firewalls	1. Una tecnología bien configurada. 2. Métodos de autenticación 3. Métodos criptográficos 4. Firewalls 5. Programas antivirus.	1. Métodos de autenticación 2. Métodos criptográficos 3. Firewalls 4. Programas antivirus. Dependiendo del sistema, tal vez cambie el orden de uno a otro.
9. ¿Considera que hace falta difundir una cultura de seguridad informática en México? ¿Por qué?			
Si. Porque incluso podemos tener problemas de seguridad nacional con la falta de expertos en seguridad informática, además la seguridad la hacemos todos.	Si. Porque en general la gente no tiene conciencia a cerca de las implicaciones que puede tener el uso de cualquier sistema de cómputo y los riesgos que corre su información.	Si. No solamente una cultura de seguridad sino una de administración, es triste ver que en México la mayoría de los problemas de seguridad comienzan por una pésima administración de los equipos. Un administrador conciente siempre se preocupará por la seguridad.	Si. Existen muchos incidentes de seguridad actualmente y esto se debe a la falta de una cultura de seguridad.

1.5.4 Conclusiones por pregunta

1. La información que viaja a través de las redes no es segura, ya que es relativamente fácil ver su contenido, más aún si ésta viaja por un canal inseguro.

2. Las ventajas son la facilidad y velocidad con que viaja la información así como su disposición casi inmediata.

3. La información interna si es segura pero la que se obtiene de medios externos no esta libre de riesgos, ya que no hay sistemas 100% seguros.

4. Si se conocen muchas y muy diversas tecnologías que ayudan a proteger a los sistemas de ataques e intromisiones.

5. Si. Se utilizan varias herramientas de seguridad, las que se utilizan generalmente son los cifrados, mecanismos de autenticación y filtrados de información.

6. Un sistema que proporciona información íntegra, auténtica, confidencial y disponible en el momento que se requiere.

7. 1. Integridad, 2. Confidencialidad, 3. Privacidad 4. Disponibilidad.

8. Métodos criptográficos y métodos de autenticación son las herramientas más importantes para hacer del sistema de información un sistema seguro y confiable.

9. Definitivamente hace falta difundir una cultura de seguridad informática ya que la gente no tiene conciencia del peligro que corre su información cuando viaja a través de una red.

1.5.5 Conclusiones generales

1. La información que viaja a través de una red de computadoras no es segura, menos aún si viaja por un canal inseguro, los datos que se obtienen de las redes no siempre son seguros ya que en muchas ocasiones no se tiene la certeza de su procedencia.

2. Existen muchas desventajas en la transmisión de información a través de redes y la principal es que esta información está expuesta a ser leída, modificada o destruida mientras viaja por la red.

3. En la actualidad existen muchas tecnologías para la protección de los sistemas de información y si se utilizan adecuadamente son altamente eficaces en la protección de los mismos.

4. Un sistema de información seguro es aquel que tiene las siguientes características en orden de importancia.
    1. Integridad
    2. Disponibilidad
    3. Confidencialidad
    4. Autenticidad

5. Algunas de las herramientas más importantes para hacer que un sistema sea seguro son los métodos criptográficos y los métodos de autenticación.

6. En México es necesario difundir una cultura de seguridad informática, ya que actualmente existen muchos incidentes en contra de la seguridad de los sistemas, y la gente encargada de éstos muchas veces no está capacitada para enfrentar este tipo de situaciones.

1.6 Hipótesis Preliminar

Relación causa – efecto

Causas (variables independientes)	Efectos (variables dependientes)
Conocer las herramientas de seguridad para redes que existen y aplicar las adecuadas.	Menor probabilidad de ser objeto de un ilícito informático.
Utilizar una herramienta de seguridad adecuada.	El sistema de información estará protegido contra intromisiones, intercepción, o alteración de la información.
Proteger los sistemas de información en red utilizando herramientas criptográficas.	La información enviada y recibida será íntegra, confiable y veraz.
Utilizar criptografía como herramienta de seguridad para cifrar información	La información tendrá un alto índice de probabilidad de verse libre de intromisiones, alteración o destrucción parcial o total.

Relaciones hipotéticas posibles

a) Forma positiva

- ✓ Si conoce las herramientas de seguridad para redes que existen, sus sistemas tendrán menor probabilidad de ser objeto de un ilícito informático.
- ✓ Si utiliza una herramienta de seguridad adecuada, su sistema de información estará protegido contra intromisiones, intercepción, robo o alteración de la información.
- ✓ Si protege su sistema de información en red utilizando herramientas criptográficas, la información que envíe y reciba será íntegra, confiable y veraz.
- ✓ Si utiliza criptografía como herramienta de seguridad para cifrar información, ésta tendrá un alto índice de probabilidad de verse libre de intromisiones, alteración o destrucción parcial o total.

b) Forma negativa

- ✓ Si no conoce las herramientas de seguridad para redes que existen, sus sistemas tendrán mayor probabilidad de ser objeto de un ilícito informático.
- ✓ Si no utiliza una herramienta de seguridad adecuada, su sistema de información no estará protegido contra intromisiones, intercepción, robo o alteración de la información.
- ✓ Si no protege su sistema de información en red utilizando herramientas criptográficas, la información que envíe y reciba no será íntegra, confiable y veraz.
- ✓ Si no utiliza criptografía como herramienta de seguridad para cifrar información, ésta no tendrá un alto índice de probabilidad de verse libre de intromisiones, alteración o destrucción parcial o total.

c) Hipótesis propuestas

- ✓ Si conoce las herramientas de seguridad para redes que existen y utiliza las adecuadas, su sistema tendrá menor probabilidad de ser objeto de un ilícito informático.
- ✓ Si protege su sistema de información en red utilizando cifrado de información, ésta será íntegra, confiable y veraz en su envío y recepción.
- ✓ Si utiliza la criptografía como una herramienta para proteger su información, ésta se verá libre de intromisión, alteración o destrucción parcial o total.

Hipótesis preliminar

Al utilizar la criptografía como herramienta de seguridad para proteger la información, ésta tendrá un alto índice de probabilidad de verse libre de intromisión, alteración o destrucción parcial o total.

1.7 Marco Justificatorio

Objetivos

Objetivos personales

- Obtener el título profesional como Licenciada en Informática de la Facultad de Contaduría y Administración, de acuerdo al Título II, artículos 44 a 56 del Reglamento General de Exámenes Profesionales vigente.
- Contribuir con este estudio a que las personas responsables de administrar sistemas en red tengan una base para darse cuenta de lo importante que es el tema de la seguridad y que la criptografía es una de las posibles soluciones para disminuir el riesgo de intercepción, modificación y hasta destrucción de información.

Objetivos particulares

- Aportar un nuevo criterio útil para cualquier tipo de organización que ayude a tomar decisiones importantes sobre la protección de sus sistemas.
- Elaborar a futuro documentos importantes que sean de utilidad para todas aquellas personas que requieren saber a cerca del uso de la criptografía como una herramienta de seguridad para proteger los sistemas de información en red.
- Que este estudio sirva de base para realizar estudios posteriores.

1.8 Anexos

1.8.1 Anexo 1-1

Formato del cuestionario aplicado a empíricos y profesionales.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

Cuestionario preliminar para definir el Marco problemático de la tesis denominada: "La criptografía como una herramienta de seguridad para proteger la información de sistemas en red" que realiza Rocio Ríos Servín, alumna de la Facultad de Contaduría y Administración con número de cuenta 9429487-7 para obtener el grado de Licenciada en Informática.

Nombre: Ocupación:
Estudios: Puesto:
Teléfono:

1. ¿Cree usted que la información que viaja a través de las redes de computadoras sea segura?

Si_____ ¿Por qué?
_____.

No_____¿Por qué?_____
_____.

Otra respuesta
_____.

2. ¿Cuáles cree usted que son las principales ventajas y desventajas de transmitir datos o información a través de una red?

Ventajas_____
_____.

Desventajas_____
_____.

1

3. ¿Considera usted que los datos e información que obtiene de los sistemas con los cuales trabaja diariamente es segura? ¿Por qué?

Si_____¿Por qué

_____

_____.

No_____¿Por qué?_____

_____.

Otra respuesta _____

_____.

4. ¿Conoce algún tipo de tecnología que proteja a los sistemas de ataques informáticos? Menciónelo

Si_____ Menciónelo_____

_____.

No_____

5. ¿Utiliza algún mecanismo de seguridad contra ataques informáticos en el lugar donde trabaja?

Si_____Menciónelos_____

_____.

No_____

Otra respuesta _____

_____.

6. Para usted ¿Qué es un sistema de información seguro?

_____

_____

_____.

7. Mencione de acuerdo a su criterio las principales características que debería tener un **sistema de información seguro**

_____

_____

_____.

2

8 ¿De las siguientes opciones numere en orden de importancia aquellas con las que debe contar un **sistema de información en red seguro?.**

1- Más importante 4 – Menos importante

___ Firewalls
___ Métodos criptográficos (Encriptación de la información)
___ Métodos de autenticación.
___ Programas Antivirus

9.¿Considera que hace falta difundir una cultura de seguridad informática en México?¿Por qué?

Si_____ ¿Por qué? _____
_____

No_____ ¿Por qué?_____
_____

Otra respuesta _____
_____.

Con la finalidad de complementar este estudio se le solicita describir brevemente las actividades que realiza en su trabajo cotidiano.

- ✓ _____
- ✓ _____
- ✓ _____
- ✓ _____
- ✓ _____

Gracias por su cooperación.

Asesor de tesis
Dr. Ricardo Rivera Soler
Tel. 54 82 00 70

3

MARCO TEÓRICO

2. Marco teórico

2.1 Acopio de libros

El marco teórico contiene todos los conocimientos adquiridos de diversas fuentes tales como libros, tesis, revistas, periódicos, páginas de internet, seminarios o conferencias, mesas redondas, películas, etc.

Dentro de los libros consultados se presentan dos variantes: los libros de estudio, que son aquellos que se han leído completos o casi completos y los libros de lectura ligera, de los cuales se han estudiado solo cierto número de capítulos.

2.1.1. Libros de estudio.

Nombre	Seguridad informática
Autor	Pino Caballero Gil
Editorial	Alfaomega
Edición	1ª. Edición
ISBN	970-15-0328-7
Colocación Biblioteca	QA76.9A25.C33 Biblioteca FCA
Capítulo 1 Criptografía teórica	Se mencionan los conceptos básicos de criptografía, criptoanálisis y criptología; se hace mención de las reglas de Kerckhoffs para los sistemas criptográficos, menciona los tipos de ataques que puede efectuar un enemigo; así como las condiciones del secreto perfecto.
Capítulo 2 Criptografía de clave secreta.	En este capítulo se mencionan los métodos de cifrado basados en criptografía de clave secreta como son: transposición, sustitución y producto; se hace un estudio detallado del algoritmo DES (Data Encryption Standard), y por último se trata el punto del cifrado en flujo.
Capítulo 3 Criptografía de clave pública.	Se detallan las características de la criptografía de llave pública, incluye un análisis de los sistemas RSA, Rabin, ElGamal y Merkle-Hellman; se hace mención de los sistemas basados en curvas elípticas y un sistema probabilístico.
Capítulo 4 Aplicaciones criptográficas	Este capítulo se divide en dos partes, por un lado trata la autenticación, donde habla del modelo matemático y como se lleva acabo la autenticación mediante criptosistemas simétricos y asimétricos. Habla de la firma digital mencionando las características de ésta, trata la problemática del uso de passwords, incluye un apartado de seguridad de redes mencionando el cifrado de información en las diferentes capas del modelo OSI y trata los protocolos criptográficos explicando cada uno con detalle.

Nombre	Técnicas criptográficas de protección de datos
Autor	Amparo Fúster Sabater
Editorial	Ra-Ma
Edición	2ª. Edición
ISBN	970-15-0602-2
Colocación Biblioteca	QA76.9A25 T48 2001 Biblioteca de DGSCA
Capítulo 1 La criptología	En este capítulo se hace una rápida introducción y se mencionan los métodos de cifrado clásicos, es como lo es el método César el cual es básico saberlo para conocer los antecedentes, se mencionan las características más sobresalientes de la criptografía y el criptoanálisis, así como los conceptos básicos que se utilizaran durante los capítulos siguientes.
Capítulo 2 Criptografía de clave secreta. Método de cifrado en flujo	En este capítulo se comienza a profundizar en los métodos existentes en cuanto al cifrado de información se refiere; el capítulo se centra en los métodos de cifrado en flujo.
Capítulo 3 Criptografía de clave secreta. Método de cifrado en bloque	Lo más importante de este capítulo es la explicación a cerca del DES, mencionando su estructura, su evolución y la forma en como funciona y se manipula, sus propiedades y las ventajas que puede brindar al usarlo como una medida de seguridad para proteger la información. En este capítulo también se hace mención de los cifrados en bloque y se explican varios algoritmos más como el RC5 y el IDEA. También se encuentra en este capítulo una rápida reseña del Criptoanálisis diferencial.
Capítulo 4 Gestión de claves simétricas	En este capítulo se comienza por hacer una breve reseña de la arquitectura de una red , poco a poco el capítulo introduce al lector en el conocimiento de las claves para algoritmos de llaves simétricas, por medio del estudio de los llamados protocolos de autenticación y claves de sesión.
Capítulo 5 Aplicaciones y arquitectura con cifrado simétrico	Este capítulo esta enfocado en forma preferencial a la autenticación de una entidad, los temas de los cuales trata son la firma digital, las tarjetas electrónicas y los sistemas de identificación personal.
Capítulo 6 Criptosistemas de clave pública	En este capítulo da inicio otra parte del libro en el que se pasa a la tecnología de cifrado de clave o llave pública, se hace una breve introducción explicando algunos conceptos y después se da paso a la explicación de los algoritmos más importantes basados en llave pública; tal es el caso de RSA, ElGamal, curvas elípticas y mochila tramposa; de los cuales también se hace mención de los ataques a los que se encuentran expuestos.
Capítulo 7 Protocolos criptográficos y firmas digitales	El capítulo da un enfoque hacia la autenticación de entidades, utilizando el criptosistemas RSA, también se hace mención de algunas funciones de HASH para cifrar.

Capítulo 8 Aplicaciones de la criptografía de llave pública	Enfoque total hacia la autenticación se menciona como debe autenticarse e identificarse un usuario, además se mencionan varios ejemplos en los que se ha utilizado la criptografía como una aplicación real.
Capítulo 9 Aplicaciones criptográficas en redes de comunicaciones	Se hace una pequeña introducción, después el capítulo se avoca hacia el tema de las redes, como se aplican los principios de seguridad, así como mención de los sistemas de autenticación en red, tales como: kerberos. Existe un apartado que hace alusión a la seguridad en internet, los protocolos seguros y algunas herramientas para hacer segura la red.

Nombre	Protección de la Información. Diseño de criptosistemas informáticos.
Autor	Amador Rodríguez Prieto
Editorial	Parainfo
Edición	1ª. Edición
ISBN	84-283-1434-9
Colocación Biblioteca	QA76.9A23 R63 Biblioteca de DGSCA
Capítulo 1 Introducción e historia	En este primer capítulo el autor hace una cronología desde el surgimiento de la criptografía hasta la época contemporánea, dentro de un apartado que denomina criptografía clásica, menciona todos los métodos antiguos de encriptación como son: César, sustitución simple, cifrados homófonicos, entre otros y se explican mediante ejemplos de cada uno.
Capítulo 2 El cifrado hoy	En este capítulo se explican los algoritmos de cifrado y su complejidad, menciona varios tipos de cifrado de tipo computacional, de esta forma incluye operaciones lógicas, transformaciones mediante manipulación de bits, cifrados doble y triple.
Capítulo 3 Taxonomía de los cifrados	Este capítulo presenta una clasificación o taxonomía de los cifrados, dividiendo estos en cifrados en bloque y cifrados de flujo. Se hace un estudio detallado del DES (Data Encryption Standard).
Capítulo 4 Seguridad	En este capítulo se tratan ampliamente los cifrados simétricos y los cifrados asimétricos incluyendo la complejidad computacional de ambos, así como la verificación de autenticidad; incluye también un apartado de firma digital y de criptoanálisis.
Capítulo 5 Revisión a la situación legal	En este capítulo se trata el tema de la seguridad de los datos e información desde el punto de vista legal, de esta manera habla de varias leyes que se han aplicado en países como Suecia, Portugal, Alemania y Estados Unidos entre otros.

2.1.2 Libros de lectura ligera

Nombre	Seguridad Informática
Autor	Juan José Nombela
Editorial	Parainfo
Edición	1ª. Edición
ISBN	84-283-2341-0
Ubicación	QA76.9A25 N65 Biblioteca de la FCA
Capítulo 7 Protección de la información	Este capítulo se refiere en su totalidad a la criptografía; comienza con algunas definiciones básicas y se mencionan los métodos de cifrado clásicos como el método César, sustitución simple, sustitución polialfabeto, entre otros; después se hace mención de los sistemas de cifrado modernos, donde los puntos principales son la explicación de los algoritmos DES y RSA, por último hay un apartado donde se mencionan a grandes rasgos las características de las firmas digitales, el criptoanálisis y herramientas de cifrado.
Capítulo 8 Seguridad en redes y comunicaciones	El capítulo trata de los conceptos necesarios que debe conoce un administrador de red para brindar servicio con un adecuado nivel de seguridad, menciona tópicos como permisos y derechos, identificación y autenticación de usuarios, copias de seguridad, entre otros. También hace mención de algunos conceptos de seguridad en Windows NT y en NETWARE.
Capítulo 10 Delitos informáticos	Este capítulo habla de los diferentes delitos informáticos que existen, así como de los riesgos a la que están expuestos todos los sistemas y menciona algunas leyes que se han publicado con respecto a los delitos informáticos.

Nombre	Seguridad y comercio en el Web
Autor	Simson Garfinkel y Gene Spafford
Editorial	Mc Graw Hill
Edición	1ª Edición
ISBN	970-10-2142-8
Colocación Biblioteca	TK 5105.59 63718 Biblioteca de la FCA
Capítulo 1 El problema de la seguridad en el web	Este capítulo menciona en forma general el porque debemos preocuparnos de que los sistemas sean seguros y cuales son los principales riesgos que se corren, así como algunas recomendaciones para asegurar los equipos y la información; como parte de las soluciones para aumentar la seguridad se mencionan los firewalls, su definición y la forma en que actúan.

Capítulo 2 Errores de los navegadores	Una breve reseña histórica de cómo han ido evolucionando los dos navegadores más populares actualmente, y como tuvieron que pasar por problemas serios de seguridad, que si bien en nuestros días algunos se han corregido, cabe aún la posibilidad de que se cometan errores nuevos.
Capítulo 5 Privacía	En este capítulo se menciona como punto importante el uso de bitácoras en los navegadores , se habla también de la política de privacidad que debe tenerse al utilizar un sistema, ya que existen delitos como es el espionaje donde pueden violarse o conseguirse secretos comerciales o información confidencial de la organización o persona a la que se interesa perjudicar.
Capítulo 6 Técnicas de identificación digital	Este capítulo trata de la infraestructura de la criptografía de llave pública, pero antes hace un análisis de las diferentes técnicas de identificación , como credenciales, huellas y firmas digitales.
Capítulo 10 Introducción a la criptografía	En este capítulo se proporcionan los conceptos básicos asociados al estudio de la criptografía, así como una explicación de los algoritmos de llave pública y llave simétrica; también se retoma con mayor amplitud el tema de infraestructura de llaves públicas.
Capítulo 11 La criptografía y el web	Se trata a la criptografía como una herramienta de seguridad para el web, así como también aparece un estudio de los sistemas actuales de encriptación. Por otra parte el capítulo también menciona las restricciones en EU y algunos otros países en cuanto al uso de la criptografía.
Capítulo 12 SSL	Este capítulo habla de SSL que es un protocolo de red seguro, se explican sus características, la forma de implementarse y la forma de utilizarse.
Capítulo 13 Seguridad de la máquina y del sitio	En este capítulo se habla de la seguridad en todos sus aspectos tanto físico como lógico, se hace una reseña indicando a través de la historia cuáles han sido las máquinas inseguras, se menciona el tema de la inseguridad de las máquinas en nuestros días indicando los principales problemas al respecto; una parte importante de este capítulo es la mención de las diferentes herramientas de seguridad con las que podemos proteger a los sistemas de información; se menciona entre otras; programas para escudriñar la red y programas de detección de intrusiones.
Capítulo 17 Software de bloqueo y tecnología de censura	En este capítulo se amplía lo mencionado en el capítulo 13 a cerca de la forma cómo proteger los sistemas, y se menciona software de bloqueo.

2.1.3 Tesis

Nombre	Estudio y análisis de mecanismos de autenticación en red
Autor	Genny León Leal
Fecha	2002
Carrera	Lic. en Informática
Universidad	UNAM – Facultad de Contaduría y Administración
El tema que se trata en este trabajo de tesis es muy interesante, ya que menciona los principales algoritmos para cifrar, tal es el caso del DES que en este trabajo se menciona de manera amplia y explícita, comenta también las principales técnicas de autenticación en red y hace una reflexión a cerca de la necesidad de fomentar una cultura de seguridad entre los administradores y usuarios de sistemas.	

Nombre	Análisis de riesgos en centros de cómputo
Autor	Víctor López Guerrero
Fecha	2001
Carrera	Lic. en Informática
Universidad	UNAM- Facultad de Contaduría y Administración
El tema central de esta tesis son las amenazas que sufren los centros de cómputo, Víctor López Guerrero realiza una taxonomía muy completa de estas amenazas, hace mención de los servicios de seguridad que se deben proporcionar para mantener la información a salvo, y estos son: confidencialidad, autenticación, no repudio, disponibilidad e integridad.	

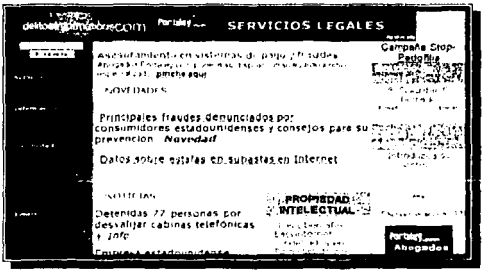
2.1.4 Revistas

Nombre de la revista	PC World
Fecha de publicación	Octubre 2002.
En esta revista se consultó un artículo publicado acerca de redes inalámbricas, en el que se trata la problemática de garantizar la seguridad de una red de este tipo, así como varios temas más relacionadas a la seguridad de redes.	

2.1.5 URL's

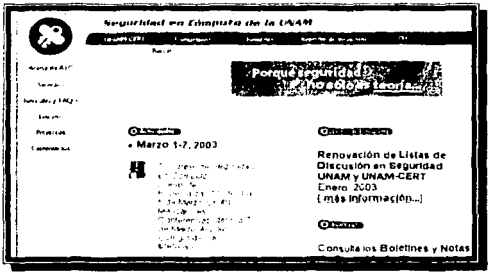
http://www.delitosinformaticos.com

Esta dirección de internet contiene las últimas noticias en cuanto a los delitos de todo tipo que se cometen en muchas partes del mundo, así como la regulación en varios países y las nuevas leyes o disposiciones que se publican.



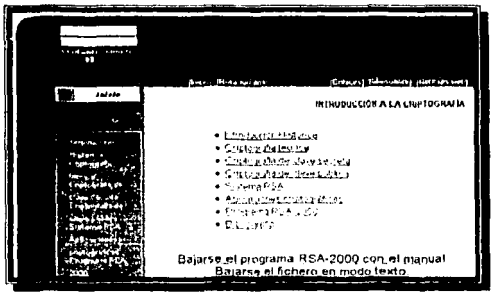
http://www.asc.unam.mx

Esta página está dedicada a la seguridad en cómputo es publicada por la UNAM y contiene apartados de noticias se seguridad, boletines informativos, actividades a realizar (ejemplo dia internacional de la seguridad en cómputo)y algunos tutoriales sobre guias y herramientas de seguridad.



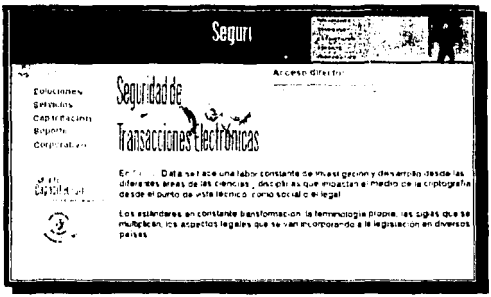
http://rinconquevedo.iespana.es/rinconquevedo/Criptografia/criptografia.htm

En esta página se puede encontrar todo lo relativo a la criptografía de clave pública y de clave privada, incluso bajar del sitio algunos algoritmos para encriptar.



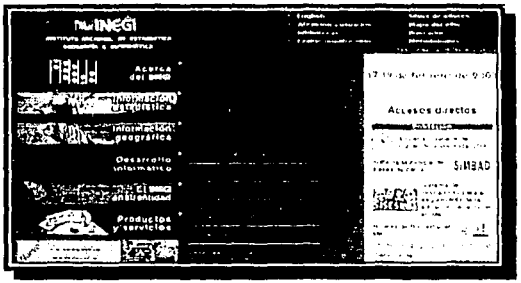
http://www.seguridata.com

Esta página es una de las más importantes y a que corresponde a una de las pocas empresas mexicanas que trabajan ofreciendo soluciones y herramientas de tipo criptográfico.



http://www.inegi.gob.mx

En esta página se pudo consultar información relacionada a las leyes que protegen a los sistemas informáticos en nuestro Pais.



2.1.6 Otras fuentes

- *Apuntes Academia Mexicana de Informatica A C*

Nombre:	Seguridad en internet y comercio electrónico
Autor:	Ulises Castillo
Apuntes AMIAC	
Amenzas	En este apartado el autor menciona ciertos tipos de amenazas que pueden afectar a los sistemas entre ellas se encuentran, las amenazas naturales, politicas, fisicas humanas, entre otras. Para cada amenaza posible es importante tener en cuenta algunos puntos de probabilidad de que ocurra, los elementos afectados, los costos asociados y la forma de resolución.
Antidotos	Maneja los más comunes que son: la encriptación de la información, programas antivirus, firewalls y los métodos de autenticación, de usuarios, de mensajes, de equipos y de aplicaciones.
Hackers	En este apartado hace regencia a la forma en como trabajan y cuales son las caracteristicas de los llamados hackers.

- *Información proporcionada por SeguriData*

Nombre	Soluciones SeguriData
Autor:	Empresa SeguriData S.A de C.V.
bSigned	Se trata de una aplicación de firma digital que permite a los firmantes intercambiar y firmar documentos multilaterales.
SeguriNotary	Se trata de una aplicación que brinda servicios de notaría electrónica para dar constancia de que una transacción electrónica ocurrió en una fecha y hora específicos.
SeguriSign	Permite garantizar la integridad y autenticidad de transacciones y documentos electrónicos que requieren ser transmitidos o concentrados en un servidor para su posterior consulta.
SeguriServer	Este software está diseñado para crear una autoridad certificadora, que emite y administra certificados digitales
SeguriDoc	Es un programa creado para Windows con el propósito de brindar características de integridad, autenticidad, no repudio de origen y confidencialidad PKCS (Public Key Cryptography Standard)

MARCO CONCEPTUAL

3. Marco conceptual

3.1 Antecedentes

Seguridad y criptografía

Desde el inicio de la era de las computadoras el hombre se preocupó por hacerlas seguras; es decir, procurar que sus datos e información estuvieran a salvo de alteraciones y que solamente pudieran ser accesadas por personas autorizadas. En un principio bastaba con colocar vigilancia a la entrada del lugar donde se encontraban los equipos, de esta forma se aseguraba que el acceso se permitía solo a personas autorizadas por la empresa u organización en la que se encontraban, pero la inseguridad física no era el único problema que resolver. Con el paso del tiempo y el surgimiento de la tecnología de redes se hizo difícil el cuidado de los equipos y la información, ya que no solamente se trataba de vigilar las máquinas que estuvieran en determinada habitación, sino también evitar que personas ajenas se conectaran a través de la red e hicieran mal uso de la información existente.

Con el surgimiento de internet el problema se acentúa ya que ahora no se trata de una sola red, sino de un número mucho mayor de redes conectadas entre si, de esta forma el hombre comienza a pensar en otras alternativas de seguridad para proteger los equipos, los sistemas de cómputo en red y la información que éstos contienen. Así con el paso del tiempo nacen los antivirus, firewalls, métodos de autenticación y tecnologías de encriptación entre otras; a los que en adelante se hará referencia como *herramientas de seguridad*.

Cada herramienta de seguridad que se ofrece para la protección de un sistema de información tiene características muy particulares, y cada una protege a un sistema en forma determinada, brindado diferentes servicios, la criptografía es una de las herramientas que más popularidad ha cobrado en las últimas décadas, y puede llegar a ser la mejor opción para el envío y recepción de información **segura**; la criptografía tiene sus orígenes en la era antes de Cristo, cuado entre los romanos los comunicados importantes se efectuaban en secreto, poco a poco esta técnica fue evolucionando, hasta llegar a las tecnologías y algoritmos recientes de encriptación, en el siguiente punto se presenta una cronología basada en la evolución de la criptografía.

3.2 Evolución de la criptografía

Siglo III a. C.

Se enviaban mensajes durante la guerra de Esparta y Atenas en Grecia. Escítalo Lacedemonio es el ejemplo más antiguo de que se tiene registro; se trataba de una lista con un conjunto de letras aparentemente sin sentido, pero esta lista al ser enrollada en un rodillo de madera mostraba los signos colocados de tal forma que el mensaje pudiera comprenderse. Así la lista viajaba como un mensaje sin sentido, pero al llegar a su destino y ser colocada en el rodillo el mensaje era comprensible.

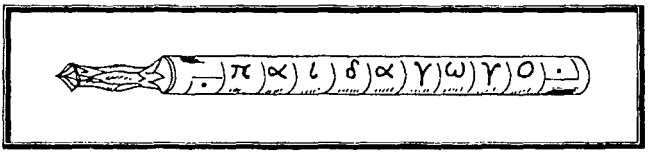


Figura 3-1 escítalo lacedemonio

Siglo I a.C.

César escribe a sus generales con un método que consistía en cambiar cada letra del alfabeto por una letra fija, en este caso tres letras después de la elegida, así A cambia por D, B cambia por E, y así sucesivamente; a este método se le denomina precisamente: Método César.

Año 1270

Roger Bacon filósofo y naturalista inglés expone en sus obras su conocimiento a cerca de un sistema de cifrado que denominó "cifrado bilateral". El cual consistía en sustituir parejas de símbolos de un mensaje por uno o más símbolos convencionales.

Año 1375

La obra Liber Zifrorum de Cicco Simonetta es considerada por algunos como la primera y más antigua sobre criptografía que se conoce. Analiza diversos sistemas basados en sustituciones simples de letras.

Año 1450

León Battista Alberti, se le considera el padre de la criptología ya que fue un gran impulsor en esta materia. Inventó un aparato que constaba de círculos concéntricos con un eje común, cada uno se dividía en 24 casillas y las letras eran colocadas en un orden específico, el cifrado se efectuaba con la correspondencia entre las letras de cada círculo.

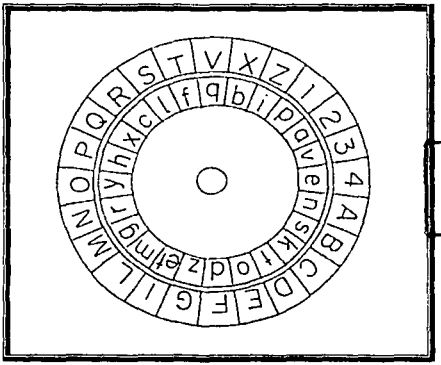


Figura 3–2 disco de Alberti

Año 1480

G. di Lavinde inventa una técnica de cifrado que consiste en sustituir palabras por un determinado código.

Siglo XVI

El historiador y religioso Trithe Mius publica la obra "Poligraphiae" donde aporta varios métodos basados en un sistema de varios alfabetos y otro basado en un sustitución de letras por palabras (método inverso al propuesto por Lavinde).

Año 1535

Giovanni Batista mejora el sistema de Alberti, usando los mismos círculos, pero ahora con signos no convencionales.

Siglo XVIII

Epoca muy activa del uso de la criptografía aunque sin avances evidentes. Lo que si es importante es la investigación criptoanalítica ya que son descubiertas claves y hay descifrado de correspondencia. Edward Willes y John Wallis son los primeros criptoanalistas.

Siglo XIX

Se consolida un método de cifrado que consiste en dividir en bloques el mensaje y alterar el orden de los símbolos, a esto se le llama transposición.

Año 1914

Durante la Primera Guerra Mundial franceses e ingleses consiguen descifrar mensajes en clave. La criptografía comienza a entrar en auge.

Año 1930

Aparecen máquinas que efectúan cifrados muy complejos, comparados con los existentes hasta esta época.

Año 1950

Mejoran las técnicas de cifrado y aparecen potentes herramientas para el criptoanálisis.

1951- Actual

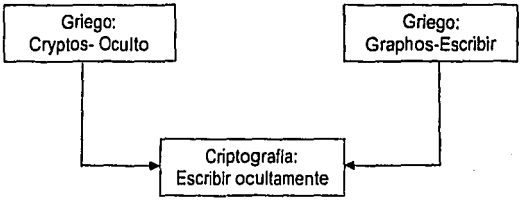
Surgen diversos algoritmos para cifrar con una complejidad matemáticamente demostrable, así como potentes herramientas de cifrado y criptoanálisis. La criptografía está en constante evolución.

3.3 Definiciones

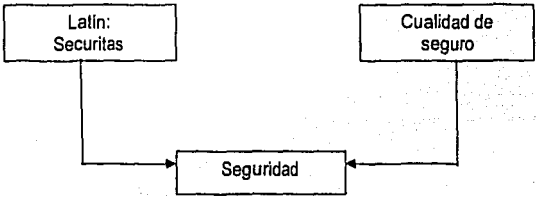
Las siguientes definiciones se proporcionan para la mejor comprensión de los temas que se tratan a lo largo de este trabajo de tesis.

3.3.1 Etimológicas

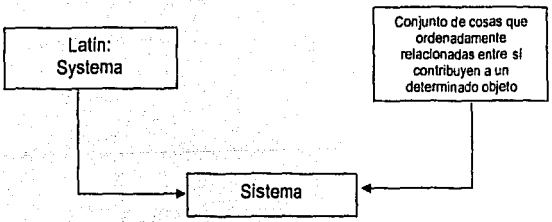
Criptografía



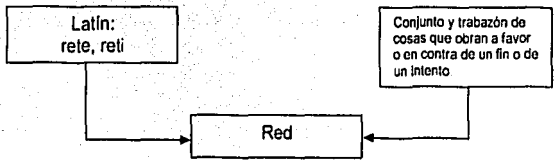
Seguridad



Sistema



Red



3.3.2 De diccionarios

1. Diccionario de la Lengua Española. Real Academia Española

Criptografía	Arte de escribir con clave secreta o de modo enigmático.
Seguridad	Dicho de un mecanismo que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente.
Seguro	Exento de todo peligro o riesgo. Cierto, que no admite duda.
Sistema	1. Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí. 2. Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto.
Red	1.Conjunto sistemático de caños, hilos, conductores, vías de comunicación, etc. 2.Conjunto y trabazón de cosas que obran a favor o en contra de un fin o de un intento.

2. Diccionario Enciclopédico Espasa 2001. (Tomo I y II)

Criptografía	Arte de escribir enigmáticamente.
Seguridad	1. Calidad de seguro. 2 Fianza u obligación de indemnización a favor de uno
Seguro	Libre y exento de todo peligro, daño o riesgo.
Sistema	1. Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí 2. Conjunto de cosas que ordenadamente relacionadas entre sí contribuyen a un determinado objeto. 3 Medio o manera usados para hacer una cosa.
Red	Conjunto de cosas que obran a favor o en contra de un fin o de un intento.

3. Diccionario Oxford de Informática

Criptografía	Escritura cifrada.
Seguridad	Security. Protección. Preservación. Protección de los datos almacenados contra alteraciones no autorizadas. Un usuario que archiva información puede necesitar que el contenido de su fichero pueda alterarse únicamente por otros usuarios que han sido autorizados de una forma explícita a hacerlo así. Los conceptos de integridad, intimidad y seguridad están interrelacionados.
Seguro	No susceptible de desaparecer, de perderse, de ser robado, de caerse, o de fallar en cualquier forma.
Sistema	System. Algo que se considera (a) como una entidad y (b) como un conjunto de componentes relacionados. En informática se utiliza mucho este término con múltiples matices, significativos, sin embargo más comúnmente puede referirse a un conjunto relacionado de unidades de soporte físico o de programas o de ambas cosas.
Red	Organización de servicios o cosas enlazadas o relacionadas entre si.

4. Diccionario de Informática. Publicaciones Cultural

Criptografía	Cryptography. Protección de un mensaje haciéndolo ininteligible para todos los que no sean sus receptores autorizados.
Seguridad informática	Bajo este término se agrupan un conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el acceso a bases de datos de personas no autorizadas, el mal funcionamiento del hardware y la pérdida física de datos.
Sistema	1. Conjunto formado por un ordenador y todos sus periféricos 2. Dícese de cualquier colección o combinación de programas, procedimientos, datos y equipamiento utilizado en el proceso de la información. 3. En el entorno de los ordenadores Machintosh, dícese del conjunto de rutinas que intervienen entre la caja de herramientas y las aplicaciones, por un lado y dicha caja y el hardware por otro.
Red	Network. En comunicaciones, término definido en sentido bastante amplio, aplicado a un sistema que consta de terminales, nodos, y medios de interconexión que pueden comprender líneas, satélites, microondas, radio de onda media y larga, etc. En general, una red es una colección de recursos utilizados para establecer y conmutar vías de comunicación entre sus terminales.

3.3.3 De Autores

1. Simson Garfinkel

Seguridad de un Sistema Computacional	Una computadora es segura si se puede confiar en ella y su software se comportará como usted espera.
Seguriadad en el Web	Conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios del Web y las organizaciones que los rodean. La seguridad en una protección contra el comportamiento inesperado.

2. Juan José Nombela

Seguridad computacional	Se puede definir la seguridad computacional como todo aquello que permita defenderse de una amenaza.

3.3.4 Definción propia

Para poder llegar a esta definición tuve que estudiar y comprender las diferentes definiciones antes mencionadas, para rescatar los puntos mas importantes e integrar un concepto propio; en dicho concepto se toma en cuenta que ningún sistema puede ser totalmente seguro, pero se rescatan los puntos más importantes de todas las definiciones anteriores.

Un sistema de información seguro es aquel que cuenta con los servicios necesarios que hacen posible que proporcione un alto grado de inmunidad ante alguna amenaza informática.

3.3.5 Sinónimos.

En este apartado de presentan las palabras de igual significado a los términos que se utilizan en este trabajo.

Criptografía	Abreviatura, clave, cifra, anagrama,jeroglífico.
Seguridad	Certidumbre, certeza, convicción, confianza, firmeza.
Sistema	Método, conjunto, plan, procedimiento, modo, ordenación.
Red	Enlace, malla, reticulo, enrejado.

3.3.6 Antónimos

Se presentan las palabras que expresan lo contrario a los términos utilizados en el presente trabajo.

Criptográfico	Claro, abierto.
Seguridad	Inseguridad, duda, debilidad, capricho.
Sistema	Desorganización, anarquía.
Red	Desligar

3.3.7 Denominación en otros idiomas.

Este apartado ayuda a identificar fácilmente los términos en otros idiomas.

Palabra / Idioma	Inglés	Francés	Alemán
Criptografía	cryptography	cryptographie	beziffer
Seguridad	security	sécurité	sicherheit
Sistema	system	système	verfahren
Red	net, network	filet	netz

3.4 Seguridad de redes

En los últimos años la tecnología de redes de computadoras ha cobrado verdadera importancia, ya que tareas y actividades que antes requerían cierta cantidad de tiempo y esfuerzo ahora se han simplificado con el uso de las redes; hoy en día se pueden hacer compras a través de una red, operaciones bancarias y transferencia de información entre otras, pero a la par de este gran avance tecnológico también han surgido graves problemas de seguridad; los principales peligros a los que se encuentra expuesta la información que viaja por una red son la intromisión, alteración, robo o destrucción de sus bancos de información y es por ello que en la actualidad existe preocupación entre los administradores de red por mantenerla segura y en la medida de lo posible libre de intromisiones ilícitas.

Ante el rápido crecimiento de las redes de distintos fabricantes y para facilitar la comunicación entre ellas, la Organización Internacional de Estandarización (ISO, Internacional Organization for Standarization) publicó a principios de los años ochenta una normativa en la que se definía un modelo estándar de interconexión de redes entre sistemas con diferentes equipos y diferentes sistemas operativos, en 1988 se publicó una segunda parte de esta norma, ISO7498-2 donde se definen los servicios de seguridad de la arquitectura, estos servicios tratan básicamente temas relacionados con la confidencialidad, integridad y control de acceso; así mismo en este agregado a la normativa se menciona que el cifrado de información es uno de los mecanismos más adecuados para cumplir con todos estos servicios de seguridad.
En la siguiente figura se presenta el modelo de referencia OSI.

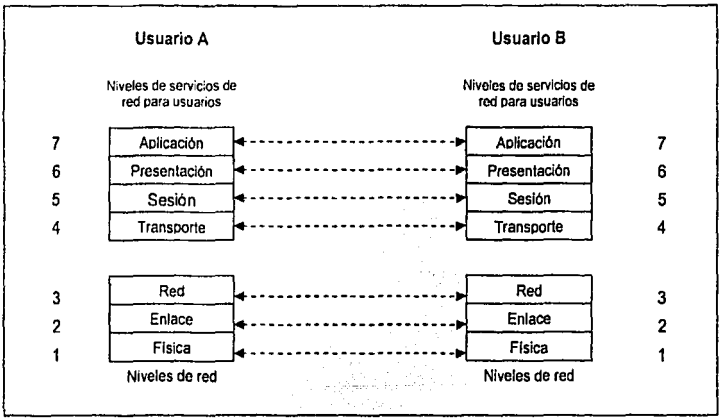


Figura 3-3 Capas de red del modelo OSI

La seguridad de una red consiste en garantizar la confidencialidad, integridad, autenticidad y disponibilidad de los datos transmitidos en ella y puede subdividirse en seguridad física y seguridad lógica. La seguridad física consiste en contar con los elementos de hardware necesarios para asegurar que la red funcionará en la manera que se espera; la seguridad lógica consiste en definir las políticas de uso y configurar adecuadamente los servicios informáticos que proporciona la red en cuestión.

Las capas del modelo OSI

A continuación se describen brevemente las capas de red ilustradas en la figura 3-3.

Capa física
Define la conexión física de la red. Proporciona los medios para activar y terminar el enlace físico entre dos sistemas, es decir, se deberá asegurar que cuando se envía un bit con valor 0, en el otro extremo se reciba ese valor y no otro. Define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Capa de enlace de datos
Entrega los datos entre un nodo y otro en un enlace de red. Convierte las líneas ruidosas en canales de comunicación libres de errores de transmisión, para utilizarlos en la capa de red. Se encarga de la topología de red, el acceso a la red, la notificación de errores y control de flujo.

Capa de transporte
Maneja la entrega entre un punto y otro de la red de los mensajes de una sesión.

Capa de red
Maneja destinos, rutas, congestión en rutas, alternativas de enrutamiento, etc. Agrupa paquetes y determina que camino toma cada paquete desde su origen hasta su destino.

Capa de sesión
Establece conexiones lógicas entre puntos de la red. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. Controla la integridad y el flujo de los datos en ambos sentidos.

Capa de presentación
Maneja los datos de la aplicación y los acomoda en un formato que pueda ser transmitido en una red.

Capa de aplicación
Es el nivel último de la capa, el que aloja los programas que interactúan con el usuario. No proporciona servicios a ninguna otra capa solamente a las aplicaciones.

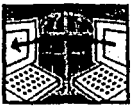
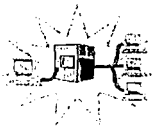
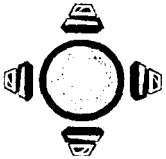
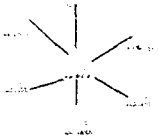
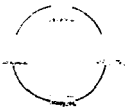
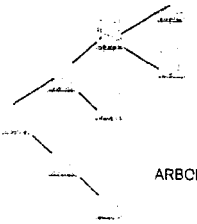
Todo administrador de red debe conocer los servicios de seguridad que es necesario proporcionar a los usuarios de ésta (la red) para que la transmisión de información no sea objeto de intromisiones ilícitas; así como definir las políticas de seguridad sobre las que se basará el funcionamiento de esta red.

Existe una gran diversidad de herramientas para brindar los servicios de seguridad necesarios y proteger la información que se transmite y cada una desempeña una función en particular; passwords, firewalls, programas antivirus, herramientas de encriptación, protocolos de red seguros, etc., cada uno de ellos actúa de forma diferente y trata de solucionar un problema de seguridad específico. Hoy en día no solo existen herramientas de protección comerciales, sino que el mercado del software libre va cobrando cada vez mayor auge y en la actualidad se encuentran herramientas de seguridad libres.

Es muy importante que las personas encargadas de garantizar la seguridad de una red, comprendan el funcionamiento de las herramientas que utilizan y los conceptos sobre los cuales funcionan, así como todo el potencial que pueden tener, para un mejor aprovechamiento de las mismas.

3.5 Monografía de redes de computadoras

Para comprender mejor los conceptos básicos y el alcance de una red de computadoras se presenta la siguiente monografía de redes.

<table>
<tr><th colspan="2">Redes de computadoras</th></tr>
<tr><td>Historia
  </td><td>Objetivos
 
Compartir recursos
 
Comunicar</td></tr>
<tr><td>Tipos de redes
 
LAN
 
MAN
 
WAN</td><td>Algunas topologías
 
BUS
 
ESTRELLA
 
ANILLO
 
ARBOL</td></tr>
</table>

Redes de computadoras

Historia

A principios de los años 70 surgieron las primeras redes de transmisión de datos destinadas exclusivamente a este propósito, como respuesta al aumento de la demanda del acceso a redes a través de terminales para poder satisfacer las necesidades de funcionalidad, flexibilidad y economía. Se comenzaron a considerar las ventajas de permitir la comunicación entre computadoras y entre grupos de terminales, ya que dependiendo de el grado de similitud entre computadoras es posible permitir que compartan recursos en mayor o menor grado.

Objetivos

Las redes en general, consisten en compartir recursos, y uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que así lo solicite, sin importar la localización física del recurso y del usuario. Otro objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Un tercer objetivo es el ahorro económico. Otro objetivo del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí.

Tipos de red

LAN. Local Area Network. Se trata de una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc. No habrá por lo general dos computadoras que disten entre sí más de un kilómetro.

MAN. Metropolitan Area Network. Las redes de área metropolitana cubren extensiones mayores como puede ser una ciudad o un distrito. Mediante la interconexión de redes LAN se distribuye la información a los diferentes puntos del distrito. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

WAN Wide Area Network. Una WAN se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas maquinas se llaman Hosts. Los hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un host a otro.

Algunas topologías

Bus. Consiste en un cable con un terminador en cada extremo del que se "cuelgan" todos los elementos de una red. Todos los nodos de la red están unidos a este cable. Este cable recibe el nombre de *backbone* cable.

Estrella. En una topología estrella todos y cada uno de los nodos de la red se conectan a un concentrador o hub. Los datos en estas redes fluyen del emisor hasta el concentrador, éste controla y realiza todas las funciones de red además de actuar como amplificador de los datos.

Árbol. La topología de árbol combina características de la topología de estrella con la de bus. Consiste en un conjunto de subredes estrella conectadas a un bus. Esta topología facilita el crecimiento de la red.

Anillo. En esta configuración, todas las estaciones repiten la misma señal que fue mandada por la terminal transmisora, y lo hacen en un solo sentido en la red. El mensaje se transmite de terminal a terminal y se repite, bit por bit, por el repetidor que se encuentra conectado al controlador de red en cada terminal. Una desventaja con esta topología es que si algún repetidor falla, podría hacer que toda la red se caiga, aunque el controlador puede sacar el repetidor defectuoso de la red, y evitar así algún desastre.

3.6 Servicios de Seguridad

Podemos llamar servicio de seguridad al procedimiento o funcionalidad que sirva para proteger la información y los sistemas de información de cualquier ataque informático; estos servicios son los siguientes:

Confidencialidad

Se refiere a que la información viajará segura, de tal forma que cualquier persona no autorizada que intente interceptarla no pueda tener acceso al contenido de ésta. Y solo las personas autorizadas podrán verla.

Autenticación.

El receptor de la información puede comprobar la identidad de la persona que envió el mensaje o información, así como comprobar que la información es la correcta; es decir la que verdaderamente fue enviada.

Integridad

Se refiere a tener la seguridad de que la información enviada no ha sido modificada, ni falsificada en su viaje a través de la red y que el destinatario la recibirá tal y como se envió.

No repudio

El emisor ni el receptor del mensaje o información puedan negar su envío o recepción ya que se crean registros donde se puede verificar que efectivamente se realizó el envío de la información.

Disponibilidad

Se refiere a que el servicio o recurso solicitado por las entidades autorizadas se encuentre disponible en el momento que se requiera.

Se requiere que un sistema de información en red, ofrezca todos los servicios mencionados anteriormente como mínimo, para garantizar la seguridad del mismo. Si alguno de ellos falla, se corre el riesgo de que se cometa alguna intromisión o delito en contra del sistema. Para una mejor retención de estos servicios de seguridad en el presente trabajo se han denominado con las siglas **CANDI**:

C onfidencialidad
A utenticación
N o repudio
D isponibilidad
I ntegridad

3.7 La criptografía como herramienta de seguridad

Después de estudiar la seguridad en redes y los servicios de seguridad, se puede encontrar a la criptografía como una herramienta eficaz para proteger el envió y recepción de información. Si bien hoy en día existen muchas técnicas para protección de información, la criptografía ocupa un lugar muy importante dentro de esta lista, ya que proporciona los servicios de seguridad necesarios para mantener la información en un alto porcentaje libre de intromisiones, alteración o destrucción parcial o total.

3.7.1 Conceptos y teoría

El estudio de la criptografía abarca varios conceptos que vale la pena analizar, pues se utilizaran en los siguientes puntos a desarrollar en el presente trabajo.
Algunos autores la llaman ciencia, otros técnica y algunos más la denominan como un arte, pero para efectos del presente estudio se denominara a la criptografía como una herramienta de seguridad para proteger la información que viaja entre redes.
La criptografía como un medio de proteger la información es una herramienta muy antigua y desde tiempos antiguos permaneció vinculada a círculos militares y diplomáticos ya que eran este tipo de grupos quienes más tenían la necesidad de proteger información valiosa; con el tiempo esta situación se fue modificando hasta que en la actualidad ha sufrido un cambio radical. Con el desarrollo de las comunicaciones electrónicas el uso de la criptografía ha proliferado y en el entendido de que la transmisión y almacenamiento de información es cada vez mayor y de que existe la necesidad de salvaguardar esa información; han surgido nuevas técnicas y herramientas basadas en criptografía.

La palabra criptografía se deriva de las raíces griegas ***kriptos*** que significa oculto y ***graphos*** que se traduce como escribir, de ahí se deduce el siguiente significado: escribir ocultamente.
A la par de la criptografía se desarrolla también el criptoanálisis, la primera trata de ocultar mensajes e información, mientras que la función de la segunda es descifrarlos; y en su conjunto forman lo que se denomina criptología, de lo anterior se derivan varios conceptos más, como; criptograma que se trata de un documento o archivo cifrado, cifrar que significa 'escribir en cifra' y esto se entiende como 'ecribir en secreto'; al proceso de análisis de un criptograma para encontrar su verdadero significado, se le denomina criptoanálisis, la figura 3-4muestra el proceso de cifrado y descifrado de información.

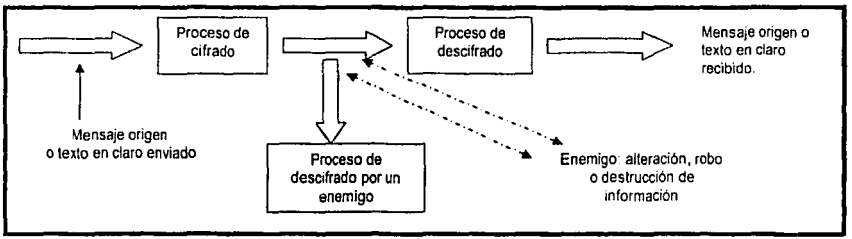


Figura 3-4 Proceso de cifrado y descifrado de información.

Como cualquier otra herramienta existen reglas que los sistemas criptográficos deben cumplir para brindar un alto porcentaje de efectividad, estas reglas fueron propuestas por Kerckhoffs en el siglo XIX y son las siguientes:

1. No debe existir ninguna forma de recuperar manualmente el criptograma, el texto inicial o la clave para cifrar.
2. Todo sistema criptográfico debe componerse de dos tipos de información:
   Pública (la familia de algoritmos que lo definen)
   Privada (la clave que se usa en cada cifrado particular)
3. La forma de escoger la clave debe ser fácil de recordar y modificar.
4. La comunicación del criptograma con los medios de transmisión comúnmente usados debe ser factible.
5. la complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.

3.7.2 Elementos que intervienen en un sistema criptográfico

Los elementos que intervienen en el proceso de comunicación o del viaje de un mensaje o información a través de una red son el emisor, el receptor, un mensaje y un canal; si el mensaje viaja en claro (sin cifrar) existe el peligro de que sea intervenido por un enemigo con el fin de alterar o destruir parcial o totalmente la información, lo anterior se muestra en la figura 3-5.

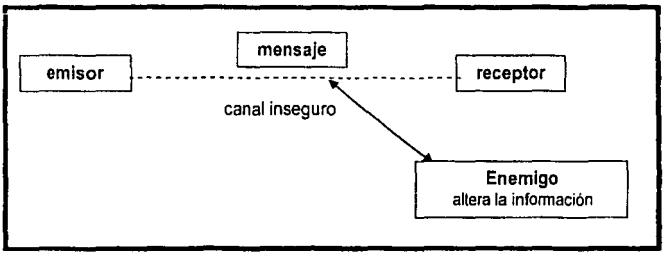


Figura 3-5 Elementos que intervienen en un sistema criptográfico.

3.8 Criptografía de clave secreta o clave privada

En los sistemas basados en clave privada, el emisor cifra el mensaje con una determinada clave que el receptor también posee y que utilizará para descifrar el mensaje; en un sistema de cifrado con clave secreta, la seguridad solo depende de un secreto que comparten emisor y receptor; el algoritmo basado en clave privada mas representativo es el DES, mismo que se analiza más adelante.

3.8.1 Métodos antiguos de encriptación

Desde tiempos antiguos, el hombre se ha preocupado por mantener segura la información importante; si se habla de criptografía; el método más antiguo de que se tiene registro es precisamente el llamado escitalo lacedemonio, que consistía en símbolos escritos al parecer sin sentido en un banda de papel, pero que al ser enrollada en un rodillo de madera también grabado con símbolos acomodados en cierta posición, se podía leer un mensaje claro; después surgirían otras modalidades como el llamado método César, en el cual se sustituye cada letra del alfabeto por otra que ocupa tres posiciones adelante, así la A cambia por D, la B por E y así sucesivamente. La sustitución homofónica es otro método basado en criptografía de llave privada, en este cada letra del alfabeto corresponde a un conjunto de símbolos denominados homofónicos, la sustitución polialfabeto también se cuenta en este rubro se elige una palabra clave y basados en esta se construye una tabla con los alfabetos, comenzando cada uno de ellos con la letra que corresponde a la clave, de esta forma se repite la clave tantas veces como sea necesario para abarcar todo el mensaje claro y de acuerdo a la correspondencia con cada alfabeto se obtiene el mensaje cifrado.

3.8.2 Transposición y sustitución

Cualquier método de cifrado, ya sea antiguo o se refiera a los modernos algoritmos se basan en uno de estos dos principios fundamentales o bien en ambos, estos son los siguientes:

Sustitución. Consiste en realizar una correspondencia del alfabeto del texto en claro con otro conjunto de símbolos que puede ser del mismo alfabeto o de uno distinto, de esta forma cada letra del texto en claro se sustituye por su correspondiente en el segundo alfabeto.

Transposición. Consiste principalmente en desordenar los elementos del texto en claro y colocarlos en una forma distinta a la original, pero el criptograma siempre contendrá los mismos elementos.

Aunque los algoritmos basados en sustitución son parte de los procedimientos clásicos de cifrado, en la actualidad no son muy usados debido a su vulnerabilidad.

En el siguiente punto se analiza el funcionamiento del algoritmo más representativp de la criptografía de llave privada, el DES.

3.8.3 Data Encryption Standard

En el año 1973, el NBS (Nacional Bureau of Standards, USA) organizó un concurso para encontrar un algoritmo de encriptación para la protección de información durante su transmisión y almacenamiento. En 1974 IBM presentó un sistema llamado LUCIFER, mismo que después de algunos ajustes y cambios se convirtió en el Data Encryption Standard (Norma de Encripción de Datos), también conocido como DES.

La aprobación y modificación de la propuesta se hizo bajo la supervisión de la NSA (National Security Agency, USA). En consecuencia casi todos los gobiernos del mundo aceptaron este algoritmo de cifrado o parte de el como estándar en las comunicaciones entre redes de computadoras.

Este algoritmo está basado en sustituciones y transposiciones, intercambiando algunos bits por otros y luego reordenándolos, el texto en claro pasa por una serie de 16 iteraciones.

El DES trabaja así:

1. El algoritmo toma el texto en claro en bloques de 64 bits y les aplica un intercambio o permutación inicial, esto da como resultado los mismos 64 bits pero permutados.

2. El bloque de los 64 bits permutados es dividido en dos partes de 32 bits cada una, denominadas I y D (bloque izquierdo y bloque derecho).

3. Los 32 bits que ocupan el lado derecho entran a una caja donde se les efectúa una función f con una llave de 56 bits menos el bit menos significativo de cada byte que se emplea como bit de paridad, y esto da como resultado una subllave de 48 bits cada una(k_n)

4. El resultado a la salida de la caja f son 32 bits a los cuales se les aplica una función XOR junto con los 32 bits que quedaron en el lado izquierdo, el resultado son 32 bits que ahora pasan al lado derecho. Los 32 bits que se encontraban inicialmente en el lado derecho pasan tal cual (sin cambio) al lado izquierdo.

5. Los 32 bits que ahora ocupan el lado derecho entran a una caja F con una subllave de 48 bits (k2) dando como resultado 32 bits, a los cuales se les aplica una función XOR con los 32 bits de lado izquierdo y se obtienen 32 bits que pasan al lado derecho.

6. Nuevamente los 32 bits de lado derecho pasan al lado izquierdo y así sucesivamente 16 intercambios o permutaciones, en la última permutación en el lado izquierdo se omite el intercambio, pero se realiza una permutación final que es inversa de la inicial, dando como resultado nuevamente 64 bits, que son el texto cifrado.

La complejidad de este algoritmo se basa en la función f, misma que se describirá en el siguiente punto, esta realiza un número determinado de sustituciones y permutaciones utilizando cajas S (sustituciones) y cajas P (permutaciones).

El tamaño de la llave (56 bits) hace que este algoritmo sea vulnerable a ataques de fuerza bruta y se cree que es posible construir una máquina capaz de desencriptar un mensaje encriptado con DES a un costo menor a un millón de dólares, incluso algunos autores afirman que tales máquinas ya existen aunque los gobiernos no lo acepten públicamente.

El proceso de descifrado para este algoritmo es el mismo aplicado en forma inversa, se utilizan las llaves de cada iteración, así k16 para la primera, k 15 para la segunda y así sucesivamente hasta llegar a la última, el resultado que se obtendrá será el texto claro.

El proceso del DES se muestra con mayor claridad en la figura 3-6

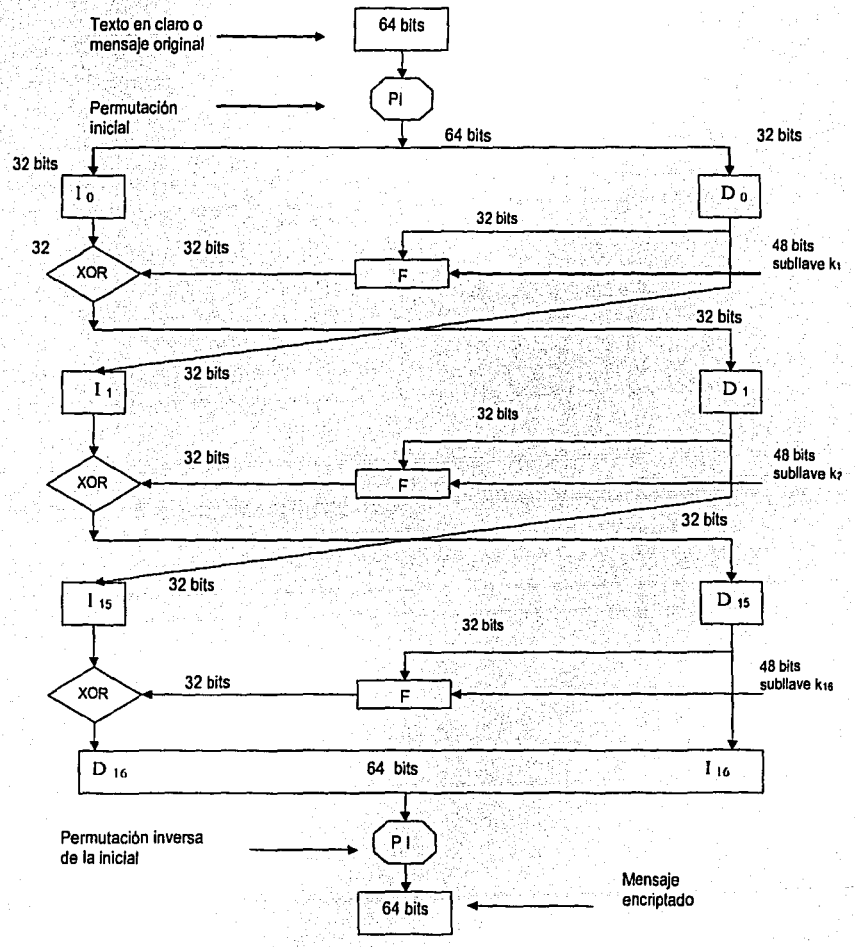


Figura 3-6 Proceso del DES

Función F

La complejidad del DES se basa en una función F, misma que ahora se explica:

La función F toma como entrada 32 bits

1. Se aplica una función de expansión E cuya principal característica es recibir menos bits que los que regresa como resultado. El resultado son 48 bits.
2. Al resultado (los 48 bits) se les aplica un XOR con una llave K_i de 48 bits y se obtiene un nuevo bloque de 48 bits el cual se subdivide en 8 bloques de 6 bits.
3. Los bits de los 8 bloques entran por bloque por una función S_i, la cual produce como salida 4 bits por bloque es decir 32 bits nuevamente.
4. Finalmente estos 32 bits son objeto de una última permutación p.

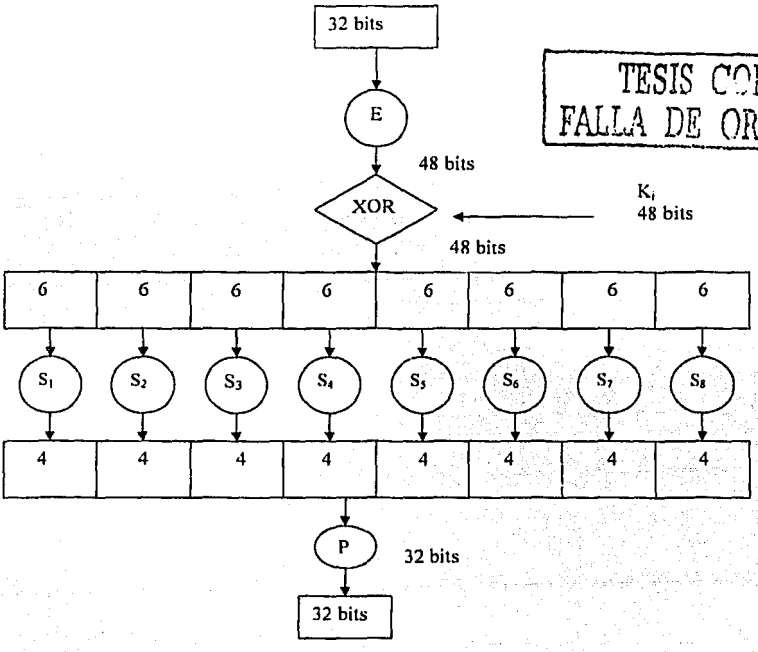


Figura 3-7 Función F

Generación de la llave K

Para poder generar la llave K se utiliza un algoritmo de generación de llaves, que opera como se muestra a continuación:

1. Se parte de la llave K con 64 bits los cuales sufren una primera permutación llamada Permuted Choice – 1 (PC-1), en esta permutación se eliminan los 8 bits de paridad (múltiplos de 8) dando como resultado 56 bits.

2. Estos 56 bits se dividen en 2 partes iguales de 28 bits cada uno se denotan como C y D con un subíndice, cuyo rango es de 0 a 16.
   C_0 y D_0 son obtenidos directamente de la permutación PC-1

3. Se obtienen los bloques siguientes siempre partiendo del bloque anterior. De esta forma C_1 y D_1 se obtiene de C_0 Y D_0 al efectuar a cada mitad por separado un proceso de rotaciones a la izquierda cada ciclo, de acuerdo a la tabla fija que se muestra en la parte inferior.

4. Cada una de las parejas Ci Di con valores para i desde 1 hasta 16, es sometida a una nueva permutación llamada permutación segunda y pasa nuevamente todo el ciclo.

No ciclo	No bits a rotar a la izquierda
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

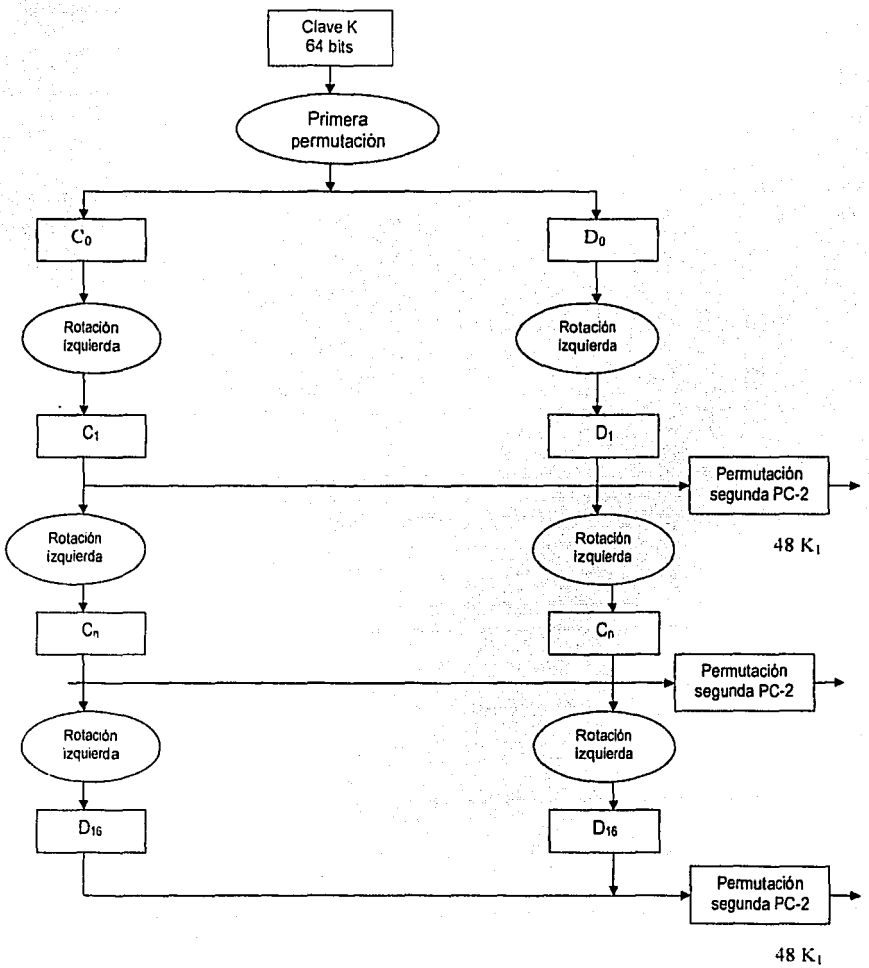


Figura 3-8 Algoritmo de generación de llaves

3.9 Criptografía de clave o llave pública

En los sistemas criptográficos de clave pública se utilizan dos llaves, una pública y otra privada; el emisor del mensaje o información cifra el mensaje con la clave pública del receptor, dicha clave deberá ser conocida, y el receptor descifra el mensaje con su propia llave privada que deberá ser solo conocida por el y permanecer en secreto.

Un esquema del proceso de cifrado con llave pública se puede representar como en la figura 3-9 donde un emisor A envía un mensaje cifrado con una clave pública K a un receptor B que los descifra con su clave privada.

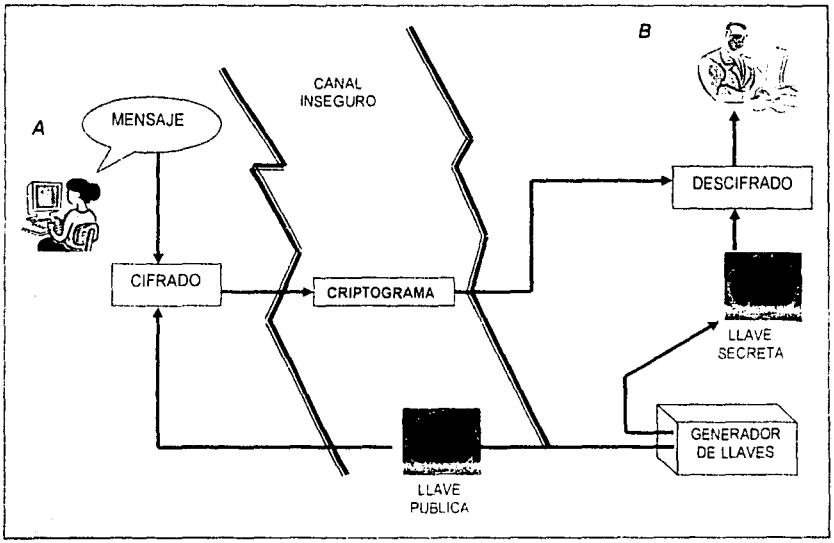


Figura 3-9 Ejemplificación de cifrado con llave pública.

Al igual que en la criptografía de llave privada, en la criptografía de llave pública también existe un sistema representativo se trata del algoritmo RSA, que a continuación se describe

3.9.1 Sistema RSA

Este sistema fue desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman, de las iniciales de los apellidos de los autores se formó el nombre de este sistema, a continuación se describe su funcionamiento:

1. El primer paso es encontrar dos números primos grandes denominados como ***p*** y ***q*** los cuales serán secretos y luego calcular un número ***n*** mediante su producto, este número será público, tal procedimiento se representa como sigue:

$$n = p \cdot q$$

2. Se escoge un número d que no tenga divisores en común aparte de 1 y que el mcd entre d y (p-1) . (q-1) debe ser 1, con esto se calcula un número e.

$$e \cdot d = 1 \ (mod \ ((p-1) \cdot (q-1)) \ )$$

3. El operador del módulo es el resto de la división entera.

$$(e \cdot d) \ mod \ ((p-1) \cdot ((p-1) \cdot (q-1)) = 1$$

4. Lo anterior se puede leer como e multiplicado por d y dividio entre (p-1) por (q-1) debe dar como resto 1

$$e = inv \ (d \ , ((p-1) \cdot (q-1)) \ )$$

5. Inv es la función inversa que permite obtener ***e***.

El emisor y receptor publican los valores e y n que serán su clave pública y que todos los remitentes deben conocer, en tanto que d y n permanecerán en secreto formando la clave privada de cada usuario.
p y q también serán secretas y se utilizarán únicamente para la obtención de las claves, después ya no serán necesarios en el funcionamiento del sistema.
Para cifrar la información el usuario deberá utilizar la función $C = M^e \ mod \ n$ donde ***M*** es el mensaje o texto en claro y ***C*** es el cifrado que se obtendrá.

La seguridad de este algoritmo radica en el tamaño del número ***n*** (producto de ***p.q***), no es recomendable trabajar con números inferiores a 154 dígitos o 512 bits.

Las dos grandes dificultades para la implementación de RSA son:
Las potencias modulares y
La búsqueda de números primos
El punto más débil de RSA es su velocidad comparado con otros algoritmos.

A manera de un cuadro comparativo se presenta el siguiente cuadro mostrando las características, ventajas y desventajas de usar algoritmos de llave privada o de llave pública.

Algoritmos criptográficos		Características	Ventajas	Desventajas
	Algoritmos de llave privada	Misma clave para encriptar y desencriptar. Encriptación de datos en masa. Por lo general contienen un gran número de llaves posibles.	Más rápidos Más fáciles de implementar Son los algoritmos más populares en la criptografía moderna.	Para intercambiar información, ambas partes primero deben intercambiar en forma segura una llave de encriptación.
	Algoritmos de Llave pública	Una llave para encriptar y otra para desencriptar	La llave pública puede ser conocida sin que corra peligro el mensaje o la llave de desencriptado.	Este tipo de algoritmos son mas lentos.

3.10 Algunos sistemas de encriptación actuales

Una vez que se ha estudiado en que consiste la criptografía de llave privada y llave pública se pueden mencionar algunos de los sistemas actuales de encriptación que se basan en alguna de estas dos modalidades ó bien en las dos, además se hace una breve descripción de su funcionamiento.

A continuación se mencionan algunos de los sistemas actuales de encriptación y una descripción breve de su funcionamiento.

- Sistemas actuales de encriptación
  - Programas y protocolos para encriptar mensajes de correo electrónico.
    - PGP
    - S/MIME
  - Protocolos de red seguros
    - SSL
    - SSH
    - PCT
    - S-HTTP
    - Kerberos
    - DNSSEC
    - CyberCash

PGP
Pretty Good Privacy

PGP es un sistema completo para la protección de correo electrónico y archivos y se encuentra disponible en dos formas: como aplicación independiente y como un programa integrado de correo electrónico, disponible por parte de PGP Inc. Aunque el primero se puede ejecutar en diversas plataformas, es más difícil de utilizar.

Uno de los problemas con el uso de PGP es la administración y certificación de llaves públicas, ya que las llaves de PGP nunca expiran, en su lugar cuando una de las llaves se ve comprometida o está en riesgo, es responsabilidad del poseedor de ésta enviar un mensaje a todos quienes poseen la llave en cuestión avisando de la revocación de la misma.

Una de las formas de distribuir las llaves PGP es mediante los servidores de llaves públicas PGP en internet; de esta forma cualquier usuario de internet puede mandar una llave pública al servidor y este mantendrá una copia y entregará la llave a cualquiera que lo solicite.

La habilidad de PGP para certificar la identidad de un usuario de manera confiable se ve limitada por la falta de infraestructura de llaves públicas.

S/MIME
Multipurpose Internet Mail Extensión

Las extensiones multipropósito de correo de internet son un estándar para enviar mensajes de correo electrónico con archivos binarios anexos. S/MIME (seguro) extiende este estándar para proporcionar correo electrónico firmado, a diferencia de PGP, S/MIME no fue diseñado en principio para funcionar de manera independiente sino como una biblioteca que se agregaba a los paquetes de correo electrónico existentes.

SSL
Secure Sockets Layer

Se trata de un protocolo criptográfico para asegurar canales de comunicación bidireccionales, se utiliza por lo general junto con el protocolo TCP/IP y es un sistema de encriptación que ha cobrado popularidad en los últimos años, navegadores como Netscape e Internet Explorer lo utilizan pero puede emplearse como un servicio basado en TCP/IP.
Este protocolo ofrece confidencialidad, integridad y no repudio de origen.

SSH
Secure Shell

Se trata de un interpréte de comandos seguro, el cual proporciona operaciones protegidas de terminal virtual (Telnet) y transferencia de archivos (ftp), SSH se encuentra disponible para Unix, Windows y Macintosh.

PCT
Private Communications Technology

Se trata de un protocolo de seguridad a nivel de transporte, es similar a SSL y fue desarrollado como respuesta a los problemas que se presentaron en la segunda y tercera versión de SSL.

S-HTTP
Secure Hper Text Transfer Protocol

Se trata de un sistema para encriptar información enviada mediante el protocolo http de web (S viene de seguro) tiene algunas características importantes como la capacidad de guardar documentos prefirmados en un servidor web, hoy este protocolo esta prácticamente en desuso ya que los principales navegadores de web no lo incluyen.

Kerberos

Es un sistema de seguridad que no utiliza tecnología de llaves públicas; se basa en códigos simétricos compartidos entre el servidor de Kerberos y cada usuario, el cual tiene su propia clave de acceso; el servidor Kerberos lo utiliza para encriptar los mensajes enviados a ese usuario, de forma que no pueda leerlos nadie más.
Kerberos debe agregarse a cada programa que se desee proteger. Se trata de un sistema difícil de configurar y administrar, ya que para operar un sistema con Kerberos cada sitio debe tener un servidor de Kerberos físicamente seguro.

DNSSEC
Domain Name System Security

Es un sistema diseñado para proporcionar seguridad al Sistema de Nombres de Dominio (DNS, Domain Name System) de internet. DNSSEC realiza una infraestructura paralela de llaves públicas con el sistema DNS. A cada dominio del DNS le corresponde una llave pública; permite la actualización segura de la información almacenada en los servidores de DNS, lo cual lo hace un sistema idóneo para la administración remota.

SET
Secure Electronic Transactions

Se trata de un protocolo criptográfico que ha sido diseñado para el envío de números de tarjeta de crédito a través de internet. Se compone de tres partes: billetera electrónica (en la computadora del usuario), un servidor que se ejecuta en el sitio web del comerciante y el servicio de pagos SET que se deberá ejecutar en el banco del comerciante.
La forma de utilizar SET es la siguiente:

- El usuario introduce el número de su tarjeta de crédito en el software de billetera electrónica (el software crea una llave pública y una privada para encriptar la información antes de enviarla por internet)
- Cuando el usuario desea comprar algo, su número de tarjeta es encriptado y enviado al comerciante.
- El software del comerciante firma digitalmente el mensaje de pago y lo envía al banco.
- En el banco el servidor de pagos desencripta toda la información y realiza el cargo a la tarjeta. Al final se envía un comprobante de la transacción, tanto al usuario como al comerciante.

A continuación se presenta un cuadro comparativo de los sistemas mencionados anteriormente:

Nombre del sistema	¿Qué es?	¿Qué proporciona?
PGP	Programa o aplicación para encriptar correo electrónico.	Confidencialidad, autenticación, integridad y no repudio.
S/MIME	Formato para encriptar correo electrónico	Confidencialidad, autenticación, integridad y no repudio.
SSL	Protocolo para encriptar , trabajando sobre TCP/IP	Confidencialidad, autenticación, integridad y no repudio.
SSH	Terminal remota encriptada	Confidencialidad y autenticación.
PCT	Protocolo para encriptar, trabajando sobre TCP/IP	Confidencialidad, autenticación, integridad y no repudio.
S-HTTP	Protocolo para encriptar solicitudes y respuestas HTTP	Confidencialidad, autenticación, integridad y no repudio. Sin embargo se encuentra en desuso.
Kerberos	Servicio de seguridad en red para asegurar aplicaciones de más alto nivel.	Confidencialidad y autenticación.
DNSSEC	Sistema de seguridad del Sistema de Nombres de Dominio.	Autenticación e integridad
SET	Protocolo para envío de números de tarjeta de crédito seguros a través de internet.	Solo confidencialidad de los números; integridad del mensaje, autenticación del usuario y proveedor, así como no repudio de las transacciones.

3.11 Lo que puede y no puede hacer la criptografía

Como cualquier otra herramienta de seguridad, la criptografía y programas basados en ella, también presentan vulnerabilidades, a continuación se mencionan algunas de las ventajas y desventajas que proporciona el uso de la criptografía.

Ventajas	Desventajas
La criptografía proporciona confidencialidad, ya que se utiliza para ocultar el verdadero significado de la información que viaja por una red, de tal forma que cualquiera que intente interceptarla no pueda tener acceso al contenido real de los datos.	La criptografía no protege contra ataques de negación de servicio y/o destrucción total de la información.
Proporciona autenticación, ya que mediante el empleo de llaves las personas que reciben un mensaje pueden comprobar la identidad de quien lo envió.	No puede proteger contra el robo de llaves de encriptación. La razón para usar encriptación es hacer que quienes tienen las llaves puedan desencriptar mensajes, por ello cualquier intruso que logre adquirir una de estas llaves, podrá desencriptar cualquier mensaje encriptado con ella.
La información se ve libre de modificaciones en su viaje a través de la red, de esta forma la información permanece íntegra.	La criptografía no puede proteger contra un traidor, aún cuando la persona que descifra el mensaje lo haga legítimamente la criptografía no puede asegurar que esta persona no haga uso ilícito de la información obtenida.

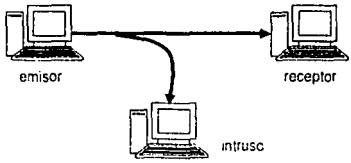
3.12 Monografía de ataques que afectan a una red

A continuación se ha elaborado una monografía de algunos de los posibles ataques que afectan a una red.

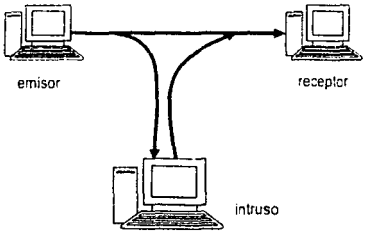
Posibles ataques en contra de un sistema en red

Interrupción de servicio

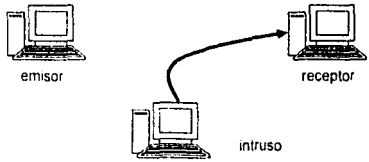
Intercepción o robo de información



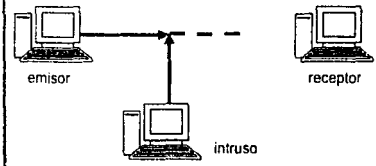
Modificación de información



Fabricación de información falsa



Destrucción de información



Posibles ataques en contra de un sistema en red	
Interrupción del servicio Este ataque atenta contra la disponibilidad del sistema, ya que puede ser deshabilitado o no estar disponible; incluso al momento de la interrupción pueden eliminarse o alterarse datos o información importante.	*Intercepción o robo de información* Se trata de un ataque contra la confidencialidad del sistema, ya que frente a un ataque de esta índole no se asegura que la información original llegue a su destino.
Modificación de información Este ataque en todas sus formas atenta contra la integridad, ya que al realizarlo hay una alteración de la información, de esta forma ya no es integra y por lo tanto no será confiable.	*Fabricación de información falsa* Este ataque atenta contra la autenticación ya que existe una falsedad que puede ser de información o de la entidad que envía y / o recibe esa información. *Destrucción de información* Este tipo de ataque es el más nocivo ya que atenta contra cualquier servicio de seguridad que ofrezca una red, la destrucción de información impide que ésta llegue a su destino.

3.13 ¿Qué se hace en la ciudad de México respecto a la criptografía?

Como parte de este trabajo de tesis se ha recopilado información de empresas dedicadas a la venta y distribución de soluciones para seguridad de redes, en especial soluciones que incluyen el uso de criptografía; la información que han proporcionado estas empresas se incluye a continuación con el fin de ampliar el panorama de conocimiento a cerca de los que se está haciendo en México en pro de la seguridad de las redes y las comunicaciones.

Se obtuvo una entrevista con tres empresas dedicadas a la venta de soluciones de seguridad, estas son:

SeguriData S. A. de C.V.
Arteria Comunicaciones S. A. de C. V.
RedCorp S. A de C.V.

3.13.1 Definición de las preguntas

Construcción del cuestionario aplicado a los representantes de las empresas mencionadas en el punto anterior.

1. ¿Bajo qué condiciones es necesario utilizar software criptográfico para proteger la información que viaja por una red?	
Justificación: Esta pregunta ayuda a definir las necesidades básicas que puede tener un usuario para decidirse a utilizar un software de tipo criptográfico para proteger su información.	**Respuesta esperada:** Cada caso es diferente, pero en general se debe utilizar cuando la información viaja en claro por un canal inseguro. Se espera obtener aportaciones nuevas mencionando otros factores para decidir utilizar una herramienta basada en criptografía.

2. ¿Existen diversos tipos de software criptográfico? ¿Cuáles son?	
Justificación: Esta pregunta permitirá conocer algunos tipos de software que existen y algunas de sus características.	**Respuesta esperada:** Se espera que se haga mención de diversos tipos de software sus nombres y principales características .

3. ¿Hay un software para proteger e-mail y otro para bases de datos? ¿Existe otro tipo de software?	
Justificación: Saber que se está haciendo por la protección de e-mail y de base de datos y si se considera alguna mas importante que la otra.	**Respuesta esperada:** Si. Existe software diferente para proteger cada tipo de información, o por los menos difiere en algunas caracteristicas.

4. ¿Existen requisitos mínimos de sistema para poder instalar y usar un software criptográfico?	
Justificación: Se puede decir que un software criptográfico no es cualquier cosa, y deben existir ciertos requisitos de sistema para poder instalarlo y utilizarlo.	**Respuesta esperada:** Se espera que se especifiquen estos requisitos necesarios para la correcta instalación y operación de este tipo de programas.

5. ¿Cuáles son las principales cualidades del software X?	
Justificación: Una vez que se haya confirmado si existen diferentes tipos de software, las preguntas 5 a la 8 se contestarán por cado uno de los programas que se hayan mencionado. Para saber las ventajas de utilizar este tipo de programa.	**Respuesta esperada:** Se espera que se haga mención de las cualidades más sobresalientes de cada programa.

6. ¿Cuáles son los principales defectos del software x?	
Justificación: Obtener información para saber las desventajas que existen al momento de utilizar este tipo de programa.	**Respuesta esperada:** Se espera que se mencionen pocas , pero reales las desventajas que se tienen al usar este tipo de software.

7. ¿Cómo funciona el software X? ¿Bajo qué tipo de algoritmos? Explicación de funcionamiento.	
Justificación: Conocer qué tipo de algoritmos utiliza cada software ya que durante el desarrollo del marco conceptual se ha estudiado a la criptografía en dos ramas: llave pública y llave privada; así como los algoritmos que los definen.	**Respuesta esperada:** Explicación de los algoritmos

8. ¿Qué porcentaje de confiabilidad proporciona el software X?	
Justificación: Se realiza esta pregunta para saber qué tanto se puede confiar en este tipo de programas y si es que existe alguno que sea más confiable que otro y en qué se basa para proporcionar ese porcentaje de confiabilidad.	**Respuesta esperada:** Se esperaba los programas mencionados tengan un alto índice de confiabilidad.

9. ¿Qué tipo de empresas u organizaciones son las que adquieren este tipo de software con más frecuencia? ¿Han tenido alguna queja de ellas?	
Justificación: Conocer qué empresas y organizaciones se preocupan más por la seguridad de su información, adquiriendo este tipo de productos criptográficos y si en algún momento éstos han fallado ocasionándoles pérdidas.	**Respuesta esperada:** Se espera que esta pregunta sea contestada con honestidad ya que es importante saber si estos programas han tenido fallas en algún momento y en qué han consistido éstas.

10. ¿Existe algún tipo de información que no pueda ser encriptada? ¿Cómo cual?	
Justificación: Con esta pregunta se puede saber si existe alguna dificultad para encriptar información y si realmente hay alguna información o dato que no pueda ser encriptado.	**Respuesta esperada:** Se espera que la respuesta sea: No. Toda la información se puede encriptar; ya que de esta manera se puede comprobar que la criptografía es una herramienta eficaz para la protección de información.

11-¿Sabe si existe software criptográfico libre?	
Justificación: Esta pregunta se realiza con el fin de conocer si este tipo de tecnología, se encuentra al alcance de las empresas que no tienen recursos muy amplios y que desean proteger su información.	**Respuesta esperada:** Se espera que la respuesta sea sí, y que se señale en donde puede obtenerse este tipo de programas.

12.¿Proporciona algún servicio de capacitación o difusión de una cultura de seguridad a los usuarios de sus productos o público general?	
Justificación: La razón más importante es conocer si este tipo de empresas aparte de comercializar con sus productos y servicios promueven una cultura de seguridad informática en el País.	**Respuesta esperada:** Se espera que la pregunta se conteste con un: sí, de esta forma se sabrá que la empresa está contribuyendo a introducir una cultura de seguridad, entre las personas y empresas usuarios de sus productos y servicios.

13. ¿Posee algún otro producto (s) de protección para mantener segura la información en un sistema en red?	
Justificación: Junto con la pregunta siguiente permitirá hacer una comparación sobre los productos existentes para proteger la información que viaja por las redes y saber cuál se utiliza más.	**Respuesta esperada:** Se espera que se mencionen los distintos productos con los que cuentan para proteger la información.

14.Si la respuesta anterior fue sí. ¿Cuál vende más, el tipo de criptográfico o el otro?	
Justificación: Junto con la pregunta anterior, permitirá hacer una comparación sobre los productos existentes para proteger la información que viaja por las redes y saber cual se utiliza más	Respuesta esperada: Se espera que los productos criptográficos obtengan el mayor número de menciones sobre los demás, de esta forma se podrá comprobar que es una de las mejores opciones en la protección de la información.

3.13.2 Aplicación del cuestionario y recopilación.

1.¿Bajo qué condiciones es necesario utilizar un software criptográfico para proteger la informaciónque viaja por una red?		
RedesCorporativas	**SeguriData**	**Arteria Comunicaciones**
El cliente se acerca de acuerdo a sus necesidades y requerimientos, son ellos quienes nos hacen saber sus necesidades.	Las condiciones en las que el cliente considere necesario hacer que su información permanezca siempre segura.	Una persona puede decidir proteger proteger su información en cualquier momento
2. ¿Existen diversos tipos de software criptográfico? ¿Cuáles son?		
El software que se maneja hasta hoy es CRIP IT y posterior a este se ha desarrollado una suit con más productos destinados a la seguridad de la información.	Si nosotros tenemos diversos productos criptográficos que conforman lo que llamamos "escritorio seguro", se trata de bSigned, SeguriDoc, SeguriServer, entre otros, cada uno desempeña una función especifica.	Hay diversas soluciones que pueden ayudar al cliente, debemos conocer primero sus necesidades y requerimientos para poder ofrecer la mejor.
3. ¿Hay un software para proteger e-mail y otro para bases de datos? ¿Existe otro tipo de sofware?		
Solamente contamos con CRIP IT para encripción de archivos.	Hay diferentes tipos de software que utilizan criptografía y que sirve cada uno para proteger información importante.	Nosotros diseñamos la aplicación de acuerdo a los requerimientos del cliente, si éste decide proteger solo sus bases de datos, así se diseña la solución, si requiere seguridad para e-mail así se hace.
4. ¿Existen requisitos mínimos de sistema para poder instalar y usar un software criptográfico?		
Las empresas deben contar con equipos eficientes que permitan el buen funcionamiento del software a instalar, pero no existen requisitos especificos.	Dependiendo del software que se trate pero los requisitos pueden variar, aunque no hay uno especifico, funcionará mejor mientras la máquina tenga mayor capacidad.	De acuerdo a los productos que operamos cada uno tiene sus requerimientos de sistema y capacidad de las máquinas.
5. ¿Cuáles son las principales cualidades del software?		
CRIP IT es un software que puede utilizarse en todas las máquinas que pertenezcan a la red interna, su funcionamiento es muy fácil, ya que mediante la aplicación de una llave pública pueden encriptarse los paquetes de información y ser enviados.	Cada uno de nuestros productos tiene características que lo hacen único, pero también deben tomarse en cuenta las necesidades y requerimientos de la institución.	Dependiendo del software a realizar, éste podrá o no hacer determinadas funciones, en general las cualidades que pueda poseer dependen de las necesidades que cada organización nos haga llegar.

6. ¿Cuáles son los principales defectos del software ?		
Redes Corporativas	**SeguriData**	**Arteria Comunicaciones**
Hasta la fecha no se han reportado quejas sobre mal funcionamiento o defectos. Aunque es importante mencionar que las últimas licencias de CRIP IT fueron vendidas hace ya seis meses.	Cada uno de nuestros programas tiene una función específica, así es que cada uno realiza eficientemente su labor.	Defectos como tal no se presentan, pero en caso de que después de usar la solución para seguridad, se detecta que hay algunas deficiencias, no habrá problema porque nosotros mismos la solucionamos.
7. ¿Cómo funciona el software ? ¿Bajo qué tipo de algoritmos? Explicación de funcionamiento		
Funciona bajo el concepto de llave pública. El algoritmo no puede ser explicado.	Los productos de SeguriData funcionan bajo el estándar PKCS (Public Key Cryptography Standard) que utiliza criptografía de llave pública (RSA) y algoritmo de criptografía simétrica (Triple DES)	Depende de las necesidades del usuario ya que las soluciones se diseñan por cada solicitud.
8. ¿Qué porcentaje de confiabilidad proporciona el software ?		
El cien por ciento.	Hasta la fecha no hemos tenido un mal reporte por falta de confiabilidad.	Los productos que desarrollamos serán siempre confiables para usted y para su empresa.
9. ¿Qué tipo de empresas son las que adquieren este tipo de software con más frecuencia? ¿Han tenido alguna queja de ellas?		
Por lo general las empresas de gran tamaño (no se mencionan nombres) y hasta la fecha no se han recibido quejas.	Instituciones financieras y de gobierno han acudido a nosotros y siempre hemos proporcionado la solución óptima.	Somos proveedores de empresas de gran tamaño como Televisa, Coca Cola y Bimbo. Las soluciones que les hemos diseñado han funcionado bien hasta el día de hoy.
10.¿Existe algún tipo de información que no puede ser encriptada? ¿Cómo cuál?		
No. No existe ninguna.	Hasta la fecha no se ha presentado el caso.	Desconozco si existe alguna, por experiencia puedo decir que no.
11. ¿Sabe si existe software criptográfico libre?		
No, lo desconozco	Si existen algunos paquetes en la red que encriptan datos de manera sencilla	Por el momento no conocemos ninguno, pero nuestros competidores más fuertes son SeguriData.

12. ¿Proporciona algún servicio de capacitación o difusión de una cultura de seguridad a los usuarios de sus productos y / o al público en general?		
Redes Corporativas	**SeguriData**	**Arteria Comunicaciones**
Si. Junto con las licencias y el software se proporciona el servicio de capacitación, ya que no venderíamos algo que no le sirviera a su empresa.	Si, se proporcionan estos servicios a los usuarios de nuestros productos.	Si, cualquier duda que tenga el cliente se puede aclarar así como se imparten también cursos de capacitación y actualización.
13. ¿ Posee algún otro producto (s) de protección para mantener segura la información en un sistema en red?		
Si. Antivirus y Firewalls.	Si, proporcionamos diversos productos.	Si, tenemos una gama amplia de productos para seguridad de redes.
14.Si la respuesta anterior fue sí ¿Cuál vende más, el de tipo criptográfico o el otro?		
El otro. Tal es el caso de los antivirus.	Todos los productos están basados de una u otra forma en la criptografía.	

3.13.3 Conclusiones por empresa

Red Corp Redes Corporativas	Se consiguió la entrevista con el Ing. Guillermo Peralta

Sobre protección a sistemas con criptografía se maneja una aplicación denominada CRIP IT, se trata de un software que se puede instalar en todas las máquinas que utilice el sistema en cuestión y protege la información enviada de un punto a otro de la red; seleccionando la información que se necesita sea confidencial debe pasar por este programa, quien la encripta y después la envía a su destino; este software funciona mediante un algoritmo de llave privada, por lo que el destinatario debe poseer esta llave, así como su llave secreta y además tener instalado el software en la máquina en la que recibirá la información.

Una desventaja de esta tecnología es que no siempre puede integrarse a los sistemas, si no que debe utilizarse *por fuera*, es decir dentro de la aplicación que proporciona la información confidencial no hay una opción que permita encriptarla, debe pasar forzosamente por el software CRIP IT.

Después de esta explicación el Ing. Peralta aceptó, sin embargo que la última licencia que se vendió de este software fue hace seis meses, y que a la fecha no se ha vuelto a vender.
Cabe señalar que Redes Corporativas se dedica exclusivamente a la distribución de este tipo de productos pero, éstos son fabricados por la empresa Computer Associates.

SEGURIDATA	Se obtuvo la entrevista con los ingenieros Javier Chavarri y Maribel Briseño.

La empresa cuenta con servicios de criptografía como tal para proteger documentos y crear certificados digitales, los productos y servicios con los que se cuentan son amplios, se describen a continuación brevemente cuales son las opciones que ofrece SEGURIDATA para la protección de información importante.

Uno de los productos que se ofrecen es **bSigned** se trata de una aplicación con dos componentes básicos **bSigned.com**, y **bSigned.exe,** el primero tiene como finalidad obtener las firmas y autenticarlas, registrando también la fecha y hora en que se realiza cada transacción mientras que el segundo permite intercambiar y firmar documentos de forma electrónica; cabe señalar que lo más destacado de esta aplicación es que funciona en documentos electrónicos multilaterales, es decir que pueden ser firmados por dos, tres o más personas.

Otro producto igual de interesante es **SeguriDoc** el cual fue diseñado para trabajar sobre Windows y es un producto que proporciona los servicios de seguridad básicos con que debe cumplir un software destinado a brindar protección: Integridad, Autenticidad, No-Repudio de Origen y Confidencialidad, SeguriDoc también realiza firmado digital, autenticación de archivos, encripción y desencripción de archivos.

SeguriNotary es una nueva tecnología de protección que da fe de las transacciones realizadas entre dos entidades o dos terminales. La función principal de este producto es obtener una constancia de la realización de una operación en una fecha y hora específicos.

La creación de certificados digitales es otra opción que se ha desarrollado en los últimos años con éxito y para ello SeguriData ofrece " **SeguriServer** " que es un software diseñado para crear una Autoridad Certificadora; emite y administra certificados digitales, proporcionando a la Autoridad Certificadora las funciones necesarias para adaptar los certificados a sus propias políticas"

Por último existe **SeguriSign** que es una aplicación que permite garantizar dos de los servicios de seguridad más importantes que son la integridad y la Autenticidad en la transacción de documentos electrónicos que deben estar concentrados en un servidor para una consulta posterior.

ARTERIA Comunicaciones	La entrevista la proporcionaron los ingenieros Armando Aguilar y Oscar Piña.

Esta empresa es una empresa mexicana que ofrece servicios de consultoría, outsourcing, diseño web, firewalls y diseño e implementación de redes; dentro de los servicios de consultoría de seguridad,

Arteria ofrece:
- Análisis de vulnerabilidad exterior.
- Análisis de vulnerabilidad interior.
- Análisis de configuración de Firewalls y servidores.
- Generación de políticas de seguridad.
- Creación de planes de contingencia.

La oferta de Arteria para sus clientes es desde los servicios de consultoría, hasta el diseño e implementación de redes, y aunque se trata de una empresa mexicana que desarrolla las soluciones de acuerdo a las necesidades de cada uno de sus clientes, también ofrece productos elaborados por otras empresas, tal es el caso de la empresa RSA de quien ofrecen productos de vanguardia para seguridad y autenticación de usuarios al momento de realizar la conexión a la red, también se ofrece como servicio de seguridad las VPN que son redes virtuales privadas (Virtual Private Network), las cuales son una solución en cuanto al envío y recepción de información entre las terminales de una institución o bien de una institución a otra.

3.14 ¿Qué dicen las leyes?

A pesar de que la criptografía puede ser una herramienta eficaz en la protección de datos, ésta no puede hacer mucho cuando se ha concretado un delito de índole informática.

Es difícil establecer y aprobar leyes que regulen la conducta de las personas en lo que se refiere al uso de una red, puesto que el alcance de éstas es muy amplio, tan es así que para conseguir la información de una base de datos de una empresa establecida en cierto país, el intruso no necesariamente debe encontrarse en ese territorio; aunado a esto el retraso tecnológico en México hace que sea más difícil establecer penalidades a las personas que causan daños a través de medios electrónicos.

Existen algunas leyes que aunque de manera incipiente ya regulan este tipo de conductas en nuestro País, tal es el caso la Ley Federal de Telecomunicaciones y la Ley Federal de Derechos de Autor (LFDA)en la que se incluyen algunos artículos destinados a los programas de computación y las bases de datos.

Ley Federal de Derechos de Autor y Ley Federal de Telecomunicaciones

Los programas de cómputo están protegidos por la LFDA en su Título II, Capítulo 1, Artículo 13, Fracción XI.

Al realizar el análisis de algunos de los artículos de esta ley se encuentra que existen varias regulaciones en cuanto al su uso, distribución y venta de programas de cómputo; así como las facultades y derechos que se les proporcionan a los autores, pero no se encuentra ninguna sanción para aquellas personas que violen estas disposiciones. El Capítulo IV del Título V de esta ley esta dedicado exclusivamente al tema de los programas de computación y las bases de datos este tema y en todos los artículos que abarca este capítulo se puede apreciar la protección de esta ley para con los programas mencionados, pero nunca se establece ¿Qué pasa si no se respetan estos artículos? Algunos otros artículos de esta ley también pueden ser aplicables a este tema, pero se encuentran redactados en la misma forma, es decir proporcionando derechos y obligaciones pero no una sanción.

Por su parte la Ley Federal de telecomunicaciones establece una protección diferente, si bien una red podría no ser protegida por la LFDA, la información que viaja a través de ella si esta protegida por la ley que ampara a las telecomunicaciones; esta ley dedica el Capítulo IX titulado Infracciones y sanciones, a establecer multas a quien viole lo establecido en esta ley, a continuación se traducen textualmente algunos de los artículos de este capítulo que son de interés para el presente trabajo. (los demás artículos se omiten)

Capítulo IX
Infracciones y Sanciones

Artículo 71. Las infracciones a lo dispuesto en esta Ley, se sancionarán por la Secretaría de Comunicaciones y Transportes de conformidad con lo siguiente:

A. Con multa de 10,000 a 100,000 salarios mínimos por:

V. Interceptar información que se transmita por las redes públicas de telecomunicaciones.

C. Con multa de 2,000 a 20,000 salarios mínimos por:

IV. Incurrir en violaciones a las disposiciones de información y registro contempladas en la presente Ley.

En caso de reincidencia la Secretaría podrá imponer una multa equivalente hasta el doble de las cuantías señaladas.

Se considera importante que en lo sucesivo se realizara una investigación más a fondo sobre las leyes que protegen a los usuarios de redes de comunicaciones.

3.15 Anexos

3.15.1 Anexo 3-1

Formato del cuestionario aplicado a representantes de empresas dedicadas a venta y/o distribución de software criptográfico.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

Cuestionario básico para determinar aspectos importantes a cerca de empresas que se dedican a la venta y/o distribución se software con características criptográficas, que realiza Rocio Ríos Servín, alumna de la Facultad de Contaduría y Administración de la UNAM con número de cuenta 9429487-7 como parte del trabajo de tesis profesional para obtener el grado de Licenciada en Informática.

Nombre: Teléfono:
Empresa: Puesto:

1. ¿Bajo qué condiciones es necesario utilizar un software criptográfico para proteger la información que viaja por una red?

_____
_____
_____.

2. ¿Existen diversos tipos de software criptográfico? ¿Cuáles son?

_____
_____
_____.

3. ¿Hay un software para proteger e-mail y otro para bases de datos? ¿Existe otro tipo de software?

_____
_____
_____.

4. ¿Existen requisitos mínimos de sistema para poder instalar y usar un software criptográfico?

_____
_____
_____.

1

5. ¿Cuáles son las principales cualidades del software?

6. ¿Cuáles son los principales defectos del software?

7. ¿Cómo funciona el software?¿Bajo qué tipo de algoritmos? Explicación de funcionamiento

8. ¿Qué porcentaje de confiabilidad proporciona el software?

9. ¿Qué tipo de empresas son las que adquieren este tipo de software con más frecuencia?¿Han tenido alguna queja de ellas?

10. ¿Existe algún tipo de información que no pueda ser encriptada? ¿Cómo cuál?

11. ¿Sabe si existe software criptográfico libre?

12. ¿Proporciona algún servicio de capacitación o difusión de una cultura de seguridad a los usuarios de sus productos y/o al público en general?

2

13. ¿Posee algún otro producto (s) de protección para mantener segura la información en un sistema en red?

_____

_____

_____.

14. Si la respuesta anterior fue si. ¿Cuál vende más, el de tipo criptográfico o el otro?

_____

_____

_____.

Asesor de tesis
Dr. Ricardo Rivera Soler
Tel. 54 82 00 70

3

MARCO METODOLÓGICO

4. Marco metodológico

4.1 Variables

Después de haber hecho el estudio de diversas obras, recopilado la información suficiente e incluirla en el marco teórico, así como detallar conceptos importantes en el marco conceptual del presente trabajo, las variables dependiente e independiente no sufren cambios. A continuación se mencionan las mismas:

Variable independiente

> *"Al utilizar la criptografía como herramienta de seguridad para proteger la información,*

Variable dependiente

> *ésta (la información) tendrá un alto índice de probabilidad de verse libre de intromisión, alteración o destrucción parcial o total. "*

4.2 Variables de control

No he considerado variables de control intervinientes o distorsionantes, ya que este estudio abarca un rango de población que es difícil definir, puesto que las redes de computadoras y sus concernientes riesgos se encuentran presentes en casi todo el mundo.

4.3 Hipótesis definitiva

Después del desarrollo del marco teórico y el marco conceptual, la hipótesis propuesta no sufre cambio alguno; a continuación se menciona la hipótesis definitiva del presente trabajo:

> *Al utilizar la criptografía como herramienta de seguridad para proteger la información, ésta tendrá un alto índice de probabilidad de verse libre de intromisión, alteración o destrucción parcial o total.*

4.4 Determinación del universo

Determinar el universo de este trabajo es complicado debido al mismo alcance que tiene el fenómeno que se estudia, de tal forma se espera que con la recopilación de opiniones de personas calificadas en el tema, se pueda aprobar o desaprobar la hipótesis.

4.5 Determinación de la muestra

Se aplicará una *muestra no probabilística*, denominada intencional o de juicio, en el entendido de que no se pretende realizar una prueba plena. Se aplicará un cuestionario a personas calificadas en el tema y se obtendrá un cuadro comparativo de las respuestas.

A continuación se menciona la definición de muestra y una breve descripción de los tipos de muestras:

Muestra. Conjunto de elementos que constituyendo una pequeña porción de la población, son seleccionados del todo, o de parte, de la misma, con carácter homogéneo, con la finalidad de su análisis.

Muestreo probabilístico. Se trata de aquel en el que todos los individuos tienen la misma probabilidad de ser elegidos para formar parte de una muestra. Dentro de los métodos de muestreo probabilístico tenemos los siguientes:

- *Muestra aleatoria simple.* Es aquella en la que se asigna un número a cada elemento o individuo de la población y a través de algún medio mecánico se eligen tantos elementos como sea necesario para completar el tamaño de la muestra. Un ejemplo es la extracción de bolas para obtener los números premiados en la lotería.

- *Muestra sistemática.* Es aquella en la que se eligen los elementos de la población a intervalos uniformes a partir de un listado ordenado de los elementos.

- *Muestra estratificada.* Es aquella donde se consideran categorías típicas diferentes entre sí, que poseen una gran homogeneidad respecto a alguna característica. Lo que se busca con este tipo de muestra es que todos los estratos de interés se encuentran representados en la muestra.

- *Muestra por conglomerados.* Los elementos forman un grupo que llamamos conglomerado, la muestra consiste en seleccionar cierto número de conglomerados y después investigar todos lo elementos pertenecientes a los conglomerados elegidos.

Muestreo no probabilístico. En este tipo de muestreos no se tiene la certeza de que la muestra extraída sea representativa; en general se seleccionan a los sujetos siguiendo determinados criterios y procurando que la muestra sea representativa.

- *Muestra por cuotas o accidental.* Se elige la muestra basándose generalmente en el conocimiento de los estratos de la población y/o de los individuos más representativos o adecuados para los fines de la investigación. En esta muestra se fijan "cuotas" que consisten en un número de individuos que reúnen determinadas condiciones.

- *Muestra intencional o de juicio.* Se caracteriza por realizar un esfuerzo deliberado para obtener muestras representativas mediante la inclusión de grupos supuestamente típicos.

- *Muestra casual o incidental.* El investigador se encarga de seleccionar directa e intencionalmente los individuos de la población. Lo más frecuente es tomar como muestra a los individuos a los que se tiene fácil acceso.

- *Muestra bola de nieve.* Se trata de localizar algunos individuos, los cuales conducen a otros, y estos a otros, así hasta conseguir la muestra suficiente.

4.6 Definición del método de investigación

Considero la mejor forma de comprobar la relación hipotética de este trabajo conocer la opinión de personas calificadas y con experiencia en el tema, ya que los resultados obtenidos ayudará a la aprobación o desaprobación de la hipótesis. Para este fin se aplicará un cuestionario y una vez obtenidas las respuestas se procederá a realizar un cuadro comparativo de las mismas.

4.7 Costo de la investigación.

Los costos estimados de la investigación incluyen los siguientes rubros:

- Recursos humanos
- Bienes inmuebles
- Bienes muebles
- Software
- Consumibles, papelería y artículos de oficina
- Recursos, elementos y medios para estudio
- Otros gastos

A continuación se presenta una tabla con la relación de gastos de la investigación y los totales erogables, tomando en cuenta 12 meses de trabajo.

DESCRIPCION	EROGACIONES PARCIALES	TOTALES
Recursos humanos		
Investigador	$102,000.00	
Total recursos humanos		$102,000.00
Bienes inmuebles		
Renta de oficina	$12,000.00	
Total bienes inmuebles		$12,000.00
Bienes muebles		
Escritorio 1.50 X 0.80 cm.	$800.00	
Silla	$200.00	
PC Hewlett Packard Pentium III 550 MHz	$10,750.00	
Impresora Epson Stylus 777	$1,950.00	
Total bienes muebles		$13,700.00
Software		
Microsoft Office 2000	$2,300.00	
Norton Antivirus 2002	$450.00	
Total Software		$2,750.00
Consumibles, papelería y artículos de oficina		
Cartuchos de impresión	$1,750.00	
Copias fotostáticas	$1,300.00	
Diskettes	$200.00	
Papel (hojas tamaño carta)	$250.00	
Carpeta	$50.00	
Accesorios de papelería (bolígrafos, goma, perforadora, etc.)	$400.00	
Total consumibles		$3,950.00
Recursos, elementos y medios para estudio		
Internet	$500.00	
Revistas	$300.00	
Libros		
Seguridad y comercio en el web	$320.00	
Técnicas criptográficas de protección de datos	$350.00	
Seguridad informática	$250.00	
Protección de la información	$400.00	
Total elementos de estudio		$2,120.00
Otros gastos		
Luz	$1,300.00	
Agua	$250.00	
Teléfono	$2,500.00	
Transportación y viáticos	$800.00	
Total otros gastos		$4,850.00
TOTAL DE GASTOS		**$141,370.00**

4.8 Construcción del Cuestionario

En este apartado se analizaran las preguntas hechas en el cuestionario para definir el marco metodológico, el formato del cuestionario aparece en el anexo de esta sección.

1. ¿Conoce en qué consiste la seguridad de redes, y los servicios mínimos que se deben proporcionar? ( ) SI. Explique ( ) Conozco los conceptos básicos. ( ) Los servicios básicos son: confidencialidad, autenticación, no repudio disponibilidad e integridad. ( ) Todo administrador de redes debe conocer de este tema. ( ) Otra _____	( ) No. Lo desconozco. Razón:_____
Justificación: Determinar si existe el conocimiento de lo que es e implica la seguridad de una red y por lo tanto de los sistemas que en ella se basan	**Respuesta esperada:** Positiva. La seguridad en redes debe ser un punto primordial de la cual los administradores de sistemas y personas involucradas en su manejo deben estar enteradas.

2.¿Conoce alguna herramienta criptográfica para el cifrado de información? ( ) SI. ¿Cuál? ( ) Passwords o contraseñas. ( ) Firewalls. ( ) Detectores de intrusos. ( ) Programas Antivirus. ( ) Herramientas de encriptación. ( ) Otra _____	( ) No. ¿Por qué? Razón:_____
Justificación: Verificar si existe el conocimiento de vanguardia entre los encargados de la seguridad de los sistemas	**Respuesta esperada:** Positiva. Mención de por lo menos una de las herramientas criptográficas para protección de datos e información.

3. ¿Utiliza alguna técnica para el control de acceso a sus recursos de cómputo?	
( ) Sí. ¿Cuál?	( ) No. ¿Por qué?
( ) Passwords o contraseñas. ( ) Otra _____	( ) No es necesario. ( ) Desconozco si existe alguna. ( ) Otra _____
Justificación: Verificar si desde la conexión básica de los equipos de cómputo, los administradores implantan un adecuado control de acceso y con ello protegen la información que contengan los equipos.	**Respuesta esperada:** Positiva. Si hay un control de acceso a los recursos de cómputo

4. ¿En los sistemas con los que trabaja cotidianamente, se utiliza algún mecanismo de seguridad para la protección de su red y de la información?	
( ) Si. ¿Cuál? ( ) Passwords o contraseñas ( ) Ssl ( ) Ssh ( ) PGP y CGP (criptografía) ( ) Kerberos ( ) Otra	( ) No ¿Por qué? ( ) Falta de recursos ( ) Desconocimiento de las tecnologías ( ) Otra
Justificación: Conocer qué tan popular es el uso de la criptografía y herramientas basadas en ella entre los administradores de sistemas.	**Respuesta esperada:** Negativa. El uso de las herramientas basadas en criptografía se ve desplazado por herramientas como passwords, firewalls y antivirus.

5. ¿Conoce cómo funcionan esta herramientas de seguridad?	
( ) Sí. ¿Por qué?	( ) No. ¿Por qué?
( ) Su funcionamiento es sencillo y fácil de entender ( ) Otra_____	( ) Desconozco si existe alguna herramienta de seguridad para la de seguridad para la protección de la red. ( ) Conozco en teoría como funcionan. ( ) Son complicadas de entender y utilizar. ( ) Otra_____
Justificación: Indagar si en realidad existe el conocimiento de la forma en como operan las distintas herramientas para la protección de la información	**Respuesta esperada:** Positiva. Si se conoce la herramienta se espera que se conozca la forma en que opera.

6. ¿Tiene o utiliza alguna técnica de confidencialidad en el envío y recepción de información?	
( ) Sí. ¿Cuál? ( ) Passwords o contraseñas. ( ) Cifrado de información. ( ) Protocolos de red seguros. ( ) Otra____	( ) No. ¿Por qué? ( ) No es necesario. ( ) Desconozco si existe alguna. ( ) Otra_____
Justificación: Adentrarse en el uso de técnicas de protección de datos para conocer si los responsables del manejo de redes los conocen y utilizan.	**Respuesta esperada:** Positiva. Se espera la mención del cifrado de información como principal punto.

7. ¿Ha utilizado o utiliza alguna herramienta de seguridad basada en criptografía?	
( ) Sí. ¿Cuál? _____	( ) No. ¿Por qué? ( ) Son caras. ( ) Son difíciles de conseguir. ( ) Son difíciles de entender y de manejar. ( ) Desconozco este tipo de tecnología. ( ) Otra _____
Justificación: Esta pregunta permitirá conocer si la criptografía está siendo utilizada entre los actuales administradores de sistemas y si no es así; conocer porque motivo no la utilizan.	**Respuesta esperada:** Afirmativa. Se espera que la respuesta sea afirmativa y que se mencionen las herramientas usadas.

8. ¿Conoce qué servicios de seguridad le proporciona el uso de la criptografía y las herramientas basadas en ella?	
( ) Sí. ¿Cuáles? ( ) Confidencialidad, autenticación e integridad. ( ) No repudio y disponibilidad ( ) Otra _____	( ) No. ¿Por qué? ( ) No tengo conocimiento en el tema. ( ) No me interesa. ( ) Conozco lo básico. ( ) Conozco solo la teoría. ( ) Otra _____
Justificación: Determinar si existe el conocimiento de qué es realmente lo que ofrece la criptografía para la protección de la información.	**Respuesta esperada:** Afirmativa. Se espera obtener la mención de los servicios de seguridad que ofrece el uso de la criptografía tales como confidencialidad, autenticación e integridad de datos.

9. ¿Cree usted que el uso de la criptografía como herramienta de seguridad puede hacer que disminuya la probabilidad de que la información sufra intromisión, alteración o destrucción parcial o total?

( ) SI

( ) Porque brinda los servicios de seguridad necesarios para ello.
( ) Porque es una herramienta que utiliza tecnología de vanguardia.
( ) Porque es la más adecuada para proteger la información importante.
( ) Porque en realidad protege ampliamente la información.
( ) Otra _____

( ) No. ¿Por qué?

( ) Su uso es complicado.
( ) Protege la información solo contra algunos ataques.
( ) Se puede sustituir con otra herramienta.
( ) Otra _____

Justificación:	Respuesta esperada:
Esta pregunta ayudará en gran medida a comprobar la veracidad de la hipótesis planteada.	Afirmativa. Se espera que los cuestionados consideren a la criptografía como una buena herramienta para proteger la información.

10.¿Cuáles son los problemas relativos a la seguridad más frecuentes que se encuentran en el manejo de redes de computadoras?

( ) Mala administración de la red
( ) No existen políticas de seguridad
( ) No existe un control sobre la información que se maneja en la red.
( ) Pocas instituciones en México realizan investigación sobre seguridad informática.
( ) Otra _____

( ) Falta de información sobre seguridad de redes para los usuarios.
( ) No existe una cultura sobre seguridad informática.
( ) Poca difusión de temas relacionados con la seguridad en cómputo.

Justificación:	Respuesta esperada:
Conocer de manera general los problemas cotidianos a los que se enfrentan los administradores de red, durante su labor diaria.	Se esperan respuestas variadas.

11. ¿Alguna vez ha sufrido algún ataque relevante en la red que administra? ¿Cuál?

( ) Sí. ¿Cuál?

( ) Interrupción del servicio.
( ) Intercepción de información.
( ) Fabricación de información.
( ) Rompimiento de passwords.
( ) Modificación de datos o información.
( ) Virus
( ) Ataques pasivos.
( ) Otro _____

( ) No.

( ) Nunca he sufrido un ataque.
( ) No me he percatado de ello.
( ) Los ataques sufridos no han sido relevantes.
( ) Otra _____

Justificación:	Respuesta esperada:
La finalidad es mostrar los problemas de los que se hace mención en la hipótesis, tales como alteración, intromisión o destrucción de información, así como conocer si ha sufrido algún ataque y de esta forma conocer entre la muestra qué tipo de ataque es el más frecuente.	Puede haber intromisiones en las que la información puede ser robada, alterada y/o destruida, se espera que sea mencionado por lo menos un ataque, ya que ningún sistema se encuentra exento de riesgos.

12. ¿Qué nivel de seguridad en cómputo considera usted que existe en México?

( ) No existe un nivel de seguridad.
( ) Es muy pobre.
( ) El retraso tecnológico impide que México tenga un nivel de seguridad.
( ) Es el adecuado respecto a la situación tecnológica del País.
( ) Se encuentra en una etapa de desarrollo.
( ) Otra _____

Justificación:	Respuesta esperada:
Conocer si es adecuada la difusión y conocimientos de seguridad en redes en nuestro País.	Negativa. En México hace falta difusión de temas como estos que conciernen a la seguridad de redes; y de acuerdo a la respuesta se puede establecer una generalización, debido a que son expertos quienes estarán respondiendo.

13. ¿Considera que en México existe una adecuada **cultura de seguridad informática?**

( ) Sí. ¿Por qué?
( ) Existe, aunque aún es incipiente.
( ) Existe, en un nivel adecuado con respecto al nivel de cultura informática .
( ) Otra _____

( ) No. ¿Por qué?
( ) Hace falta concientizar a la población sobre el tema.
( ) No se difunde lo necesario la información sobre cultura y seguridad informática.
( ) Otra _____

Justificación:	Respuesta esperada:
Conocer opiniones diversas que lleven a una mejor apreciación de las carencias o en su caso de los puntos a favor que existen en materia de cultura en seguridad informática.	Opiniones diversas a favor y en contra.

14. ¿Sabe quién y dónde se realiza investigación sobre seguridad informática en México?	
( ) Sí. ¿Dónde?	( ) No.
( ) Empresas privadas. ( ) Universidades (UNAM, IPN) ( ) Solamente existen conferencias sobre el tema. ( ) Solo empresas o conferencistas extranjeros ( ) Otra _____	( ) Desconozco quien realice este tipo de investigación. ( ) Nadie realiza este tipo de investigación en México México. ( ) Otra _____
Justificación: Conocer si los administradores de sistemas saben a dónde recurrir en caso de estar interesados en actualizaciones, o adquisición de nuevos conocimientos en el tema.	**Respuesta esperada:** Positiva. Se espera que por lo menos sean mencionadas las principales instituciones educativas del País.

15. ¿Qué propuestas tiene para mejorar la seguridad del cómputo en México?	
( ) Crear y difundir un programa de cultura en seguridad informática. ( ) Desarrollar e implantar nuevos mecanismos de seguridad en red. ( ) Cifrar la información. ( ) Concientizar a los usuarios de la importancia que tiene la seguridad de una red. ( ) Otra _____	
Justificación: Obtener nuevas ideas que contribuyan a la mejorar la seguridad en cómputo de México.	**Respuesta esperada:** Varias ideas con respecto a la seguridad en cómputo.

4.9 Cuestionario Piloto

La aplicación de un cuestionario piloto forma parte muy importante de esta investigación, este se aplicó para determinar si era necesario realizar algún cambio en las preguntas y en las opciones de respuesta, así como para corregir errores ya sean de ortografía y/o gramática, calcular el tiempo en el que era respondido y comprobar que el número y estructura de las preguntas era el adecuado para establecer después una conclusión con respecto a la hipótesis.

4.10 Cuestionario definitivo

Después de elaborar las correcciones correspondientes se presenta el cuestionario definitivo que consta de 15 preguntas, todas ellas relacionadas con la seguridad en redes.

4.11 Realización de la investigación

Se llevó a cabo una entrevista con 5 personas calificadas con conocimientos teóricos y prácticos de seguridad en redes, estas personas pertenecen a empresas y organizaciones de distintos tipos, educativos, gubernamentales, financieras y privadas; sus opiniones en conjunto y los resultados obtenidos son una herramienta para probar la hipótesis que planteo.

Las personas entrevistadas fueron:

- Ing. Edgar Ramírez Miranda
  Departamento de seguridad de redes
  Dirección General de Servicios de Cómputo Académico
  UNAM

- Lic. Vicente Gómez Ruíz
  Servicios en Desarrollo de Sistemas de Información S.A. de C.V.

- Lic. Enrique Agustín Rocha Macedo
  Banco Nacional de México
  BANAMEX

- Ing. Rubén Darío Sarmiento Gómez
  Instituto Nacional de Estadística, Geografía e Informática
  INEGI

- Ing. Marco Antonio Bravo Ramírez
  Instituto Federal Electoral
  IFE

4.12 Tabulación de respuestas

A continuación se presentan las respuestas obtenidas en las entrevistas ya tabuladas y contablizadas.

Personas entrevistadas / Opciones de respuesta	Vicente Gómez		Edgar Ramírez		Agustín Rocha		Rubén Sarmiento		Marco A. Bravo		Totales	
	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
1. ¿Conoce en qué consiste la seguridad de una red y los servicios básicos que se deben proporcionar?	✓		✓		✓		✓		✓		5	0
Conozco los conceptos básicos	✓										1	
Los servicios básicos son: confidencialidad, autenticación, no repudio, disponibilidad e integridad.	✓		✓		✓		✓				4	
Todo administrador de sistemas debe conocerlos.	✓				✓				✓		3	
2. ¿Conoce alguna herramienta de seguridad para protección de la información que circula por una red?	✓		✓		✓		✓		✓		5	0
Passwords o contraseñas	✓				✓		✓		✓		4	
Firewalls	✓				✓		✓		✓		4	
Detectores de intrusos	✓				✓				✓		3	
Programas antivirus	✓				✓		✓		✓		4	
Herramientas o software de encriptación	✓		✓		✓		✓		✓		5	
Firmas digitales			✓		✓						2	
Herramientas de SeguriData					✓						1	
3. ¿Utiliza alguna técnica para el control de acceso a sus recursos de cómputo?	✓		✓		✓		✓		✓		5	0
Passwords o contraseñas	✓		✓		✓		✓		✓		5	
Sistemas de encriptación propia (desarrollados)	✓										1	
Control por dominio			✓								1	
Ssh. Ssl, registro de huellas digitales					✓				✓		2	
4. ¿En los sistemas en red con los que trabaja cotidianamente, se utiliza algún mecanismo de seguridad para la protección de su red?	✓		✓		✓		✓		✓		5	0
Passwords o contraseñas	✓		✓		✓		✓		✓		5	
Ssh, Ssl	✓										1	

Personas entrevistadas / Opciones de respuesta	Vicente Gómez		Edgar Ramírez		Agustín Rocha		Rubén Sarmiento		Marco A. Bravo		Totales	
	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
Kerberos			✓		✓						2	
PGP	✓		✓						✓		2	
5. ¿Conoce cómo funcionan estas herramientas de seguridad?	✓		✓		✓			✓	✓		4	1
Su funcionamiento es sencillo y fácil de entender	✓		✓		✓				✓		4	
Conozco en teoria como funcionan							✓					
6. ¿Tiene o utiliza alguna técnica de confidencialidad en el envio y recepción de información?	✓		✓		✓		✓		✓		5	0
Passwords o contraseñas	✓				✓		✓		✓		4	
Cifrado de información			✓		✓				✓		3	
Protocolos de red seguros	✓				✓		✓		✓		4	
7. ¿Ha utilizado o utiliza alguna herramienta de seguridad basada en criptografía?		✓	✓		✓		✓		✓		4	1
Ssl, Ssh, PGP			✓								1	
Herramientas disponibles en internet							✓				1	
Otra					✓				✓		2	
8. ¿Conoce qué servicios de seguridad le proporciona el uso de la criptografía y las herramientas basadas en ella?	✓		✓		✓		✓		✓		5	0
Confidencialidad, autenticación e integridad	✓		✓		✓		✓		✓		5	
No repudio y disponibilidad de la información	✓				✓						2	

Personas entrevistadas / Opciones de respuesta	Vicente Gómez		Edgar Ramírez		Agustín Rocha		Rubén Sarmiento		Marco A Bravo		Total	
	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
9. ¿Cree usted que el uso de la criptografía como herramienta de seguridad puede hacer que disminuya la probabilidad de que la información sufra intromisión, alteración o destrucción parcial o total?	✓		✓		✓		✓		✓		5	0
Porque brinda los servicios necesarios para ello	✓						✓		✓		3	
Porque es la más adecuada para proteger información importante.	✓				✓						2	
Difícilmente podría prevenir la destrucción			✓				✓				2	
10. ¿Cuáles son los problemas relativos a la seguridad más frecuentes que se encuentran en el manejo de redes de computadoras?												
Mala administración de la red	✓		✓		✓		✓		✓		5	
No existen políticas de seguridad	✓		✓		✓						3	
Pocas instituciones en México realizan investigación sobre seguridad informática	✓		✓				✓				3	
Falta de información sobre seguridad en redes para los usuarios	✓		✓				✓				3	
No existe una cultura de seguridad informática	✓		✓				✓		✓		4	
No existe un control sobre la información que se maneja en la red.					✓						1	
11. ¿Alguna vez ha sufrido un ataque relevante en la red que administra?	✓		✓		✓		✓		✓		5	0
Interrupción de servicio	✓				✓		✓				3	
Virus	✓		✓		✓		✓		✓		5	

Personas entrevistadas / Opciones de respuesta	Vicente Gómez		Edgar Ramírez		Agustín Rocha		Rubén Sarmiento		Marco A. Bravo		Totales	
	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
12. ¿Qué nivel de seguridad en cómputo considera usted que existe en México?												
Es muy pobre			✓				✓				2	
Se encuentra en una etapa de desarrollo			✓		✓				✓		3	
En organizaciones grandes hay un buen nivel	✓										1	
13. ¿Considera que en México existe una adecuada cultura de seguridad informática?			✓		✓			✓		✓	2	2
Existe, aunque aún es incipiente					✓				✓		2	
Hace falta concientizar a la población sobre el tema			✓				✓				2	
No se difunde lo necesario la información sobre cultura y seguridad informática.			✓				✓				2	
Depende del tipo de organización de que se trate	✓										1	
14. ¿Sabe quién y dónde se realiza investigación sobre seguridad informática en México?	✓		✓		✓		✓		✓		5	0
Empresas privadas			✓		✓		✓		✓		4	
Universidades (UNAM, IPN)	✓		✓		✓		✓		✓		5	
Asociación de seguridad informática	✓										1	
15. ¿Qué propuestas tiene para mejorar la seguridad del cómputo en México?												
Crear y difundir un programa de cultura en seguridad informática	✓		✓		✓		✓		✓		5	
Desarrollar e implantar nuevos mecanismos de seguridad en red.	✓						✓				2	
Cifrar la información	✓										1	
Concientizar a los usuarios de la importancia que tiene la seguridad de una red.	✓		✓		✓		✓				4	

4.13 Análisis de los resultados

En este punto se realiza un análisis por pregunta a cerca de las respuestas en conjunto que dieron los cinco entrevistados.

1. ¿Conoce en qué consiste la seguridad de una red y los servicios básicos que se deben proporcionar?

Todas las respuestas coincidieron afirmativamente, las personas entrevistadas conocen los servicios de seguridad que se deben proporcionar en la administración de una red, estos son: garantizar la confidencialidad, autenticidad, disponibilidad en integridad de la información, así como el no repudio de origen; también fue mencionada la seguridad a nivel lógico y físico.

2. ¿Conoce alguna herramienta de seguridad para protección de la información que circula por una red?

Todos los entrevistados conocen una o varias herramientas de seguridad, pero la que tuvo mayor número de menciones fue passwords o contraseñas, le siguieron los firewalls, detectores de intrusos y también herramientas de encriptación; otras mencionadas fueron las firmas digitales y los algoritmos que verifican la integridad de la información (no necesariamente información cifrada).También se mencionó que entre las herramientas para proteger la información existen algunas comerciales y otras libres y que cada una de ellas desempeña una función específica.
También fueron señaladas herramientas desarrolladas por empresas dedicadas a la seguridad en cómputo, específicamente de criptografía, incluyendo métodos de autenticación y firma digital.

3. ¿Utiliza alguna técnica para el control de acceso a sus recursos de cómputo?

Todas las menciones fueron positivas para los passwords o contraseñas, pero también fueron señaladas otras como: intercambio de llaves públicas, sistemas de encriptación propia, registro de huellas digitales, control de direcciones IP y también uso de ssl y ssh.

4. ¿En los sistemas en red con los que trabaja cotidianamente, se utiliza algún mecanismo de seguridad para la protección de su red y de la información?

Todos los entrevistados utilizan uno o más, mecanismos de seguridad, de nueva cuenta el más popular es el password; tres de los entrevistados utilizan herramientas criptográficas como PGP; otra herramienta de este tipo es SeguriServer desarrollada por la empresa de seguridad SeguriData.

5. ¿Conoce cómo funcionan estas herramientas de seguridad?

Cuatro de las respuestas afirman que el funcionamiento de las herramientas de seguridad que utilizan es sencillo y fácil de entender, además uno de ellos piensa que aprender a manejar este tipo de herramientas es un punto esencial en cualquier organización; estos cuatro entrevistados han utilizado herramientas basadas en criptografía; sin embargo uno más de ellos no sabe ni ha utilizado este tipo de herramientas, tampoco protocolos de red seguros, basa la seguridad de su red en passwords o contraseñas.

6. ¿Tiene o utiliza alguna técnica de confidencialidad en el envío y recepción de información?

Todos los entrevistados respondieron afirmativamente, en esta ocasión el cifrado de información obtuvo el mayor número de menciones; además es común el uso de protocolos de red seguros entre los entrevistados.

7. ¿Ha utilizado o utiliza alguna herramienta de seguridad basada en criptografía?

Solamente hubo una respuesta negativa, todos los demás utilizan o han utilizado herramientas como PGP, SSH, SSL, algunas disponibles en internet como ABI-CODER y otras que son desarrolladas para una organización especifica. El entrevistado que estuvo en desacuerdo con los demás, basa su respuesta en la falta de difusión y el elevado costo de las herramientas.

8. ¿Conoce qué servicios de seguridad le proporciona el uso de la criptografía y las herramientas basadas en ella?

Todos afirmaron conocer los servicios de seguridad que les puede proporcionar el uso de herramientas criptográficas, estos servicios son: confidencialidad, autenticidad e integridad de la información, ninguno de los entrevistados mostró desconocimiento sobre el tema.

9. ¿Cree usted que el uso de la criptografía como herramienta de seguridad puede hacer que disminuya la probabilidad de que la información sufra intromisión, alteración o destrucción parcial o total?

En esta pregunta hubo división de opiniones, todos los entrevistados coinciden en que el uso de la criptografía puede disminuir la probabilidad de que la información se vea afectada por intromisión o alteraciones ilícitas; pero desaprueban que esta tecnología pueda evitar la destrucción total de la información.

10. ¿Cuáles son los problemas relativos a la seguridad más frecuentes que se encuentran en el manejo de redes de computadoras?

En este punto se mencionaron diversos problemas de seguridad que se enfrentan en la administración cotidiana de una red. Uno de estos problemas y el que obtuvo todas las menciones es la mala administración de la red. La falta de información sobre seguridad de redes para los usuarios, la inexistencia de una cultura sobre seguridad informática, y que pocas instituciones en México realizan investigación sobre seguridad de redes también son problemas a los que se enfrentan los administradores de red.

11. ¿Alguna vez ha sufrido un ataque relevante en la red que administra?

Todos han sufrido algún ataque, el que tuvo mayor número de menciones fue la expansión de virus dentro de un sistema, y después de este le siguió la interrupción de servicio.

12. ¿Qué nivel de seguridad en cómputo considera usted que existe en México?

Las respuestas mencionadas en esta pregunta apuntan principalmente a que la seguridad en cómputo en nuestro País es muy pobre, pero, se encuentra en una etapa de desarrollo; también se mencionó que existen organizaciones y/o empresas de gran tamaño en las que el nivel de seguridad informática es alto, pero éstas no representan la mayoría.

13. ¿Considera que en México existe una adecuada cultura de seguridad informática?

La cultura sobre seguridad informática es otro punto crítico, algunos de los entrevistados piensan que en México no existe una cultura de este tipo, ya que hace falta concientizar a la población y difundir lo necesario la información sobre este tema, la otra parte de los entrevistados creen que sí existe esta cultura pero aún es incipiente; una vez más uno de ellos menciona el poder adquisitivo, tecnológico y por ende económico que tienen las empresas y organizaciones de gran tamaño.

14. ¿Sabe quién y dónde se realiza investigación sobre seguridad informática y criptografía?

Todas las respuestas fueron afirmativas, el 100% de los entrevistados saben que investigaciones de este tipo son realizadas en universidades de prestigio y en unas cuantas empresas privadas.

15. ¿Qué propuestas tiene para mejorar la seguridad del cómputo en México?

Todas las respuestas coincidieron en que crear y difundir una programa de cultura en seguridad informática en una de las mejores propuestas, desarrollar e implantar nuevos mecanismos de seguridad, cifrar la información y concientizar a los usuarios de la importancia que tiene la seguridad de una red son algunas de las propuestas para mejorar la seguridad del cómputo en México. Hubo una mención enfocada a la creación en México de los productos necesarios, así como el soporte para su instalación y un programa de exportación.

4.14 Conclusiones sobre los resultados

Las respuestas obtenidas con la aplicación de entrevistas llevan a las siguientes conclusiones:

- Los administradores de red, tanto de instituciones públicas y privadas conocen los servicios de seguridad de red que se deben proporcionar.

- Es generalizado el conocimiento de herramientas que proporcionan protección a la información que viaja por una red, sin embargo, una de ellas que es la más vulnerable son los passwords, y éstos se utilizan con mayor frecuencia.

- El funcionamiento de las herramientas de seguridad que se utilizan en las organizaciones es sencillo y fácil de entender y aplicar para los administradores de redes, sin embargo, existen herramientas que proporcionan un mejor nivel de seguridad y que no son conocidas y mucho menos utilizadas por estos administradores.

- Actualmente se utilizan técnicas de confidencialidad basadas en criptografía para envío y recepción de información, además de los protocolos de red seguros.

- El uso de la criptografía y herramientas basadas en ella está adquiriendo mayor popularidad entre los administradores de sistemas, que las utilizan como una buena opción para proteger su información.

- Se conocen los servicios de seguridad que proporciona el uso de la criptografía, se asegura que ésta pude disminuir en gran porcentaje la posibilidad de que la información se vea afectada por intromisiones o alteraciones ilícitas, pero no puede evitar que sea destruida.

- Existen muchos problemas de seguridad en cómputo, la mala administración de las redes y la falta de información para los usuarios y administradores son los principales.

- La seguridad informática en México se encuentra apenas en una etapa de desarrollo, las personas dedicadas al cómputo deben mostrar empeño en este tema, ya que son ellos los responsables de tener una administración segura de las redes.

- El mejor plan de acción para mejorar los problemas antes mencionados es crear y difundir un programa de cultura en seguridad informática y de redes, con el que se pueda concientizar a los usuarios de la gran importancia de este tema.

4.15 Aprobación o desaprobación de la hipótesis

En virtud de que no pretendo mostrar una prueba plena de la relación hipotética y partiendo de la toma de una muestra de juicio; determino que la opinión conjunta de los entrevistados es satisfactoria para considerar aprobatoria la siguiente hipótesis:

Al utilizar la criptografía como herramienta de seguridad para proteger la información, ésta tendrá alto índice de probabilidad de verse libre de intromisión, alteración o destrucción parcial o total.

4.16 Anexos

4.16.1 Anexo 4-1

Formato del cuestionario aplicado a administradores de red de diversas organizaciones para definir el marco metodológico del presente trabajo.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

Cuestionario básico para definir el marco metodológico de la tesis denominada: **La criptografía como herramienta de seguridad para sistemas de información en red**; que realiza Rocío Ríos Servín, alumna de la facultad de Contaduría y Administración de la UNAM, con número de cuenta 9429487-7, para obtener el grado de Licenciada en Informática.

Nombre :

Empresa: Puesto:

Grado de estudios : Teléfono

E-mail:

Este cuestionario consta de 15 preguntas, todas ellas relacionadas con la seguridad en cómputo, usted puede marcar una o varias respuestas según su experiencia y conocimientos.

1. ¿Conoce en qué consiste la seguridad de una red y los servicios básicos que se deben proporcionar?

( ) Si. Explique ( ) No. Lo desconozco.

( ) Conozco los conceptos básicos.
( ) Los servicios básicos son: confidencialidad, autenticación, no repudio disponibilidad e integridad.
( ) Todo administrador de redes debe conocer de este tema.

Razón:_____

( ) Otra _____

1

2. ¿Conoce alguna herramienta de seguridad para protección de la información que circula por una red?

( ) Sí. ¿Cuál?

( ) Passwords o contraseñas.
( ) Firewalls.
( ) Detectores de intrusos.
( ) Programas Antivirus.
( ) Herramientas de encriptación.
( ) Otra _____

( ) No. ¿Por qué?

Razón:_____

3. ¿Utiliza alguna técnica para el control de acceso a sus recursos de cómputo?

( ) Sí. ¿Cuál?

( ) Passwords o contraseñas.
( ) Otra _____

( ) No. ¿Por qué?

( ) No es necesario.
( ) Desconozco si existe alguna.
( ) Otra _____

4. ¿En los sistemas en red con los que trabaja cotidianamente, se utiliza algún mecanismo de seguridad para la protección de su red y de la información?

( ) Sí. ¿Cuál?

( ) Passwords o contraseñas
( ) Ssl
( ) Ssh
( ) Kerberos
( ) PGP Y CPG (criptografía)
( ) Otra herramienta criptográfica ¿Cuál? _____
( ) Otra _____

( ) No. ¿Por qué?

( ) Falta de recursos (humanos, monetarios).
( ) Desconocimiento de las tecnologías.
( ) Otra _____

2

5. ¿Conoce cómo funcionan estas herramientas de seguridad?

( ) Si. ¿Por qué?

( ) Su funcionamiento es sencillo y fácil de entender
( ) Otra_____

( ) No. ¿Por qué?

( ) Desconozco si existe alguna herramienta de seguridad para la protección de la red.
( ) Conozco en teoría como funcionan.
( ) Son complicadas de entender y utilizar.
( ) Otra_____

6. ¿Tiene o utiliza alguna técnica de confidencialidad en el envío y recepción de información?

( ) Si. ¿Cuál?

( ) Passwords o contraseñas.
( ) Cifrado de información.
( ) Protocolos de red seguros.
( ) Otra ____

( ) No. ¿Por qué?

( ) No es necesario.
( ) Desconozco si existe alguna.
( ) Otra_____

7. ¿Ha utilizado o utiliza alguna herramienta de seguridad basada en criptografía?

( ) Si. ¿Cuál? _____

( ) No. ¿Por qué?

( ) Son caras.
( ) Son difíciles de conseguir.
( ) Son difíciles de entender y de manejar.
( ) Desconozco este tipo de tecnología.
( ) Otra _____

8. ¿Conoce qué servicios de seguridad le proporciona el uso de la criptografía y las herramientas basadas en ella?

( ) Si. ¿Cuáles?

( ) Confidencialidad, autenticación e integridad.
( ) No repudio y disponibilidad
( ) Otra _____

( ) No. ¿Por qué?

( ) No tengo conocimiento en el tema.
( ) No me interesa.
( ) Conozco lo básico.
( ) Conozco solo la teoría.
( ) Otra _____

3

9. ¿Cree usted que el uso de la criptografía como herramienta de seguridad puede hacer que disminuya la probabilidad de que la información sufra alteración, intromisión o destrucción parcial o total?

( ) SI

( ) Porque brinda los servicios de seguridad necesarios para ello.
( ) porque es una herramienta que utiliza tecnología de vanguardia.
( ) Porque es la más adecuada para proteger la información importante.
( ) Porque en realidad protege ampliamente la información
( ) Otra _____

( ) No. ¿Por qué?

( ) Su uso es complicado
( ) Protege la información solo contra algunos ataques.
( ) Se puede sustituir con otra herramienta
( ) Otra _____

10. ¿Cuáles son los problemas relativos a la seguridad más frecuentes que se encuentran en el manejo de redes de computadoras? Marque uno o varios.

( ) Mala administración de la red .
( ) No existen políticas de seguridad.
( ) No existe un control sobre la información que se maneja en la red.
( ) Pocas instituciones en México realizan investigación sobre seguridad informática.
( ) Falta de información sobre seguridad de redes para los usuarios.
( ) No existe una cultura sobre seguridad informática.
( ) Poca difusión de temas relacionados con la seguridad en cómputo.
( ) Otra _____

11. ¿Alguna vez ha sufrido algún ataque **relevante** la red que administra?

( ) SI. ¿Cuál?

( ) Interrupción del servicio.
( ) Intercepción de información.
( ) Fabricación de información.
( ) Virus
( ) Modificación de datos o información.
( ) Ataques pasivos.
( ) Rompimiento de passwords (fuerza bruta).
( ) Otro_____

( ) No.

( ) Nunca he sufrido un ataque.
( ) No me he percatado de ello.
( ) Los ataques sufridos no han sido relevantes.
( ) Otra _____

12. ¿Qué nivel de seguridad en cómputo considera usted que existe en México?

( ) No existe un nivel de seguridad.
( ) Es muy pobre.
( ) El retraso tecnológico impide que México tenga un nivel de seguridad.
( ) Es el adecuado respecto a la situación tecnológica del País.
( ) Se encuentra en una etapa de desarrollo.
( ) Otra _____

13. ¿Considera que en México existe una adecuada cultura de **seguridad informática?**

( ) Sí. ¿Por qué?

( ) Existe, aunque aún es incipiente.
( ) Existe, en un nivel adecuado con respecto al nivel de cultura informática .
( ) Otra _____

( ) No. ¿Por qué?

( ) Hace falta concientizar a la población sobre el tema.
( ) No se difunde lo necesario la información sobre cultura y seguridad informática.
( ) Otra ____

14. ¿Sabe quién y dónde se realiza investigación sobre seguridad informática y criptografía en México?

( ) Sí. ¿Dónde?

( ) Empresas privadas.
( ) Universidades (UNAM, IPN) .
( ) Solamente existen conferencias sobre el tema.
( ) Solo empresas o conferencistas extranjeros
( ) Otra _____

( ) No.

( ) Desconozco quien realice este tipo de investigación.
( ) Nadie realiza este tipo de investigación en México.
( ) Otra _____

15. ¿Qué propuestas tiene para **mejorar la seguridad** del cómputo en México?

( ) Crear y difundir un programa de cultura en seguridad informática.
( ) Desarrollar e implantar nuevos mecanismos de seguridad en red.
( ) Cifrar la información.
( ) Concientizar a los usuarios de la importancia que tiene la seguridad de una red.
( ) Otra _____.

5

Con la finalidad de complementar este estudio se le solicita describir brevemente las actividades que realiza en su trabajo diario.

- _____
- _____
- _____
- _____
- _____

Gracias por su cooperación

¿Desea que se le envíe una copia del resultado de este estudio?

( ) SI ( ) No

Tesista
Rocío Ríos Servín
Teléfono 56 22 15 81

Asesor
Dr. Ricardo Rivera Soler
Teléfono 54 82 00 70

6

MARCO INSTRUMENTAL

5. Marco instrumental

Este apartado tiene como objetivo precisar todas las actividades que he realizado y que realizaré a corto plazo con motivo del resultado de este estudio.

5.1 Acciones tomadas

- ✓ He redactado y enviado un artículo a la revista Emprendedores que se publica en la FCA, con el fin de que al lograr su publicación luego pueda ser publicado en otras revistas especializadas. El artículo así como el oficio empleado para su envió se presentan los anexos 5-1 y 5-2 respectivamente de esta sección.

- ✓ He creado un sitio web para consulta de lo relacionado a la temática de criptografía, este sitio será constantemente actualizado y servirá como guía de aprendizaje para todos aquellos que quieran introducirse en el estudio de la criptografía, la dirección de este sitio es. http://www.cab.unam.mx/rocio/criptografia/index.html

- ✓ Me he propuesto con jefes de carrera de informática de algunas universidades privadas para ofrecer una plática basada en la temática de criptografía; el índice tentativo de esta plática aparece en el anexo 5-3 de esta sección.

5.2 Propuestas de acción

- ✓ Proponerme como conferencista para que en algún evento de carácter informático en la UNAM se incluya el tema tratado en esta tesis; el índice tentativo será el que aparece en el anexo 5-2 de esta sección.

- ✓ Una vez titulada retomar los temas esenciales de esta tesis y redactarlos con el enfoque de un libro, mismo que se enviará a alguna editorial con el fin de que sea publicado.

- ✓ Proponer un programa detallado para la enseñanza de la criptografía en la Facultad de Contaduría y Administración (FCA) de la UNAM. El formato tentativo de este programa aparece en el anexo 5-4 de esta sección.

- ✓ Proponer la inclusión de una materia optativa que trate la temática de seguridad en redes y criptografía para el décimo semestre de la carrera de informática.

5.3 Anexos

5.3.1 Anexo 5-1

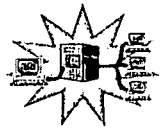
Artículo que se envió a la revista Emprendedores de la Facultad de Contaduría y Administración

Criptografía: una opción de seguridad

En los últimos años la tecnología de redes de computadoras ha cobrado verdadera importancia, ya que tareas y actividades que antes requerían cierta cantidad de tiempo y esfuerzo ahora se han simplificado con el uso de las redes: hoy en día se pueden hacer compras a través de una red, operaciones bancarias y transferencia de información entre otras, pero a la par de este gran avance tecnológico también han surgido graves problemas de seguridad; los principales peligros a los que se encuentra expuesta la información que viaja por una red son la intromisión, alteración, robo o destrucción de sus bancos de información y es por ello que en la actualidad existe preocupación entre los administradores de red por mantenerla segura y en la medida de los posible libre de intromisiones ilícitas.

La seguridad de una red consiste en garantizar la confidencialidad, integridad, autenticidad y disponibilidad de los datos transmitidos en ella y pude subdividirse en seguridad física y seguridad lógica

La seguridad física consiste en contar con los elementos de hardware necesarios para asegurar que la red funcionará en la manera que se espera; la seguridad lógica consiste en definir las políticas de uso y configurar adecuadamente los servicios informáticos que proporciona la red en cuestión.



Existe una gran diversidad de herramientas para brindar los servicios de seguridad necesarios y proteger la información que se transmite y cada una desempeña una función en particular; passwords, firewalls, programas antivirus, herramientas de encriptación, protocolos de red seguros, etc., cada uno de ellos actúa de forma diferente y trata de solucionar un problema de seguridad específico. Hoy en día no solo existen herramientas de protección comerciales, sino que el mercado del software libre va cobrando cada vez mayor auge y en la actualidad se encuentran herramientas de seguridad libres.

Después de estudiar la seguridad en redes y los servicios de seguridad, se puede encontrar a la criptografía como una herramienta eficaz para proteger el envió y recepción de información.

Si bien hoy en día existen muchas técnicas para protección de información, la criptografía.

ocupa un lugar muy importante dentro de esta lista, ya que proporciona los servicios de seguridad necesarios para mantener la información en un alto porcentaje libre de intromisiones, alteración o destrucción parcial o total.

Criptografía de clave secreta o clave privada

En los sistemas basados en clave privada, el emisor cifra el mensaje con una determinada clave que el receptor también posee y que utilizara para descifrar el mensaje; en un sistema de cifrado con clave secreta, la seguridad solo depende de un secreto que comparten emisor y receptor; el algoritmo basado en clave privada mas representativo es el DES (Data Encryption Standard)

Criptografía de llave pública

En los sistemas criptográficos de clave pública se utilizan dos llaves, una pública y otra privada; el emisor del mensaje o información cifra el mensaje con la clave pública del receptor, dicha clave deberá ser conocida, y el receptor descifra el mensaje con su propia llave privada que deberá ser solo conocida por el y permanecer en secreto.

Lo que puede y no puede hacer la criptografía

Ventajas

La criptografía proporciona confidencialidad, ya que se utiliza para ocultar el verdadero significado de la información que viaja por una red. de forma que cualquiera que intente interceptarla no pueda tener acceso al contenido real de los datos.

Proporciona autenticación, ya que mediante el empleo de llaves las personas que reciben un mensaje pueden comprobar la identidad de quien lo envió.

La información se ve libre de modificaciones en su viaje a través de la red, de esta forma la información permanece íntegra.

Desventajas

La criptografía no protege contra ataques de negación de servicio y/o destrucción total de la información

No puede proteger contra el robo de llaves de encriptación. La razón para usar encriptación es hacer que quienes tienen las llaves puedan desencriptar mensajes, por ello cualquier intruso que logre adquirir una

de estas llaves, podrá desencriptar cualquier mensaje encriptado con ella.

La criptografía no puede proteger contra un traidor, aún cuando la persona que descifra el mensaje lo haga legítimamente la criptografía no puede asegurar que esta persona no haga uso ilícito de la información obtenida.
Es importante mencionar que ni el uso de la criptografía ni el de ninguna otra herramienta de seguridad garantiza al cien por ciento que los sistemas se verán libres de alteraciones o intromisiones, pero si se usan las heramientas adecuadas, el índice de probabilidad de ser objeto de un ilícito disminuye.

Rocío Ríos Servín
Facultad de Contaduría y Administración.
Febrero 2003

5.3.2 Anexo 5-2

Oficio entregado al coordinador de la revista emprendedores con el fin de que sea publicado el artículo que aparece en el anexo 5-1 de esta sección.

México D. F. 17 de Febrero de 2003.

Lic. Adrián Méndez Salvatorio
Coordinador de la revista Emprendedores

Presente

Por este conducto me permito enviar a usted copia del artículo titulado: "Criptografía, una opción de seguridad", con el fin de que sea publicado en la revista a su digno cargo. Este artículo será de interés para todas aquellas personas relacionadas con el desarrollo de la informática, ya que cubre el tema de la seguridad de redes.

Agradezco de antemano la atención que se sirva dar a la presente y esperando que mi solicitud sea resuelta favorablemente.

Atentamente
Rocio Ríos Servín

5.3.3 Anexo 5-3

Índice tentativo para ofrecer una ponencia en relación al tema de criptografía

1. Introducción

    1.1 Seguridad de redes
    1.2 Criptografía

        1.2.1Antecedentes e historia
        1.2.2 Conceptos importantes
        1.2.3 Criptografía de llave privada

            1.2.3.1Principales sistemas criptográficos

        1.2.4 Criptografía de llave pública

            1.2.4.1Principales sistemas criptográficos

    1.3 Alcances y limitaciones de la criptografía

2. Conclusiones

5.3.4 Anexo 5-4

Propuesta tentativa de un programa para la enseñanza de la criptografía en la Facultad de Contaduría y Administración en la carrera de Informática.

Seguridad de redes: Criptografía

I. Seguridad de redes

- 1.1 Historia de las redes
- 1.2 Arquitectura de red
- 1.3 Modelo OSI
- 1.4 Servicios de seguridad
- 1.5 Posibles ataques a redes de computadoras

II. Criptología

- 2.1 Antecedentes e historia
- 2.2 Definiciones
- 2.3 Criptología clásica
  - 2.3.1 Método César
  - 2.3.2 Sustitución simple
  - 2.3.3 Cifrado Vernam
  - 2.3.4 Cifrado homofónico
  - 2.3.5 Sustitución polialfabeto
  - 2.3.6 Método de transposición
  - 2.3.7 Cifrado por producto

III. Criptografía de clave secreta

- 3.1 Cifrado en bloque
- 3.2 DES
  - 3.2.1 Estructura del DES
  - 3.2.2 Funcion F
  - 3.2.3 Cálculo de la clave
  - 3.2.4 Seguridad
- 3.3 Cifrados en flujo

IV. Criptografía de clave pública

- 4.1 Conceptos y teoría
- 4.2 Sistema RSA
- 4.3 Sistema de Rabin
- 4.4 Sistema ElGamal
- 4.5 Sistema Merkle Hellman

V. Aplicaciones de la criptografía

- 5.1 Firma digital
- 5.2 Sistemas de autenticación
- 5.3 Protocolos criptográficos

VI. Situación legal

- 6.1 Leyes que protegen a los sistemas de información en México
- 6.2 Leyes de otros países

CONCLUSIONES

Conclusiones

- ☑ En la actualidad hay administradores de sistemas que no utilizan las herramientas necesarias para proporcionar los servicios de red adecuados.
- ☑ Los administradores de red conocen las herramientas de seguridad que existen, pero no siempre las utilizan.
- ☑ Los passwords siguen siendo el método más recurrido para autenticar una entidad, y esto no es lo más adecuado, ya que la mayoría de las veces estos passwords son frases sencillas y fáciles de inferir.
- ☑ El uso de la criptografía puede hacer que disminuya la probabilidad de que la información que viaja por una red sufra intromisiones o alteración parcial o total.
- ☑ Ninguna herramienta de seguridad es efectiva al cien por ciento, pero si se usan junto con una correcta administración, pueden disminuir la posibilidad de que la información sea objeto de un ilícito.
- ☑ El estudio de la criptografía es la base para todo tipo de seguridad de sistemas.
- ☑ El uso de la criptografía tiene ventajas y desventajas, pero si se usa en combinación con otras herramientas de seguridad, proporciona una protección altamente eficaz.
- ☑ Hoy en día hace falta crear y difundir una cultura de seguridad informática entre lo usuarios de cualquier sistema basado en computadoras.
- ☑ El problema de la seguridad en redes de computadoras se presenta en todo tipo de organizaciones: publicas, privadas, gubernamentales, etc.
- ☑ Algunas empresas consideran que es mejor invertir en cuestiones de productividad, lejos de preocuparse por la seguridad de sus sistemas.
- ☑ El tamaño y recursos disponibles de las organizaciones es un factor determinante para que estas decidan invertir en la seguridad de sus sistemas.
- ☑ Siempre es mejor tener un sistema protegido y en el que sea difícil el acceso.

GLOSARIO

GLOSARIO

A

ALGORITMO
Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.

AUTENTICAR
Autorizar o legalizar alguna cosa.

B

BIT
(Binary digiT) Dígito binario. Dígito simple en un número binario (0 ó 1). En el computador, un bit es físicamente un transistor o condensador en una celda de memoria, un punto magnético en un disco o cinta, o un pulso de alto o bajo voltaje a través de un circuito.

C

CANAL DE COMUNICACION
También llamado circuito o línea, es una vía o ruta sobre la cual se transfieren datos entre dispositivos remotos. Puede referirse a todo el medio físico, como una línea telefónica, fibra óptica, cable coaxial o par de alambres trenzados, o puede referirse a una de las varias frecuencias portadoras transmitida simultáneamente dentro de la línea como en transmisión de banda ancha.

D

DNSSEC
Domain Name Server Security. Sistema diseñado para proporcionar seguridad al Sistema de Nombres de Dominio (DNS).

F

FIREWALL
Cortafuego. Nodo de red establecido como un límite para impedir que el tráfico de un segmento cruce a otro.

FIRMA DIGITAL
Mensaje codificado que se agrega a datos transmitidos a través de una red que verifica al receptor la autenticidad del emisor del mensaje. Las firmas digitales garantizan que efectivamente los emisores son quienes dicen ser.

FTP
File Transfer Protocol. Protocolo de Transferencia de Archivos. Uno de los protocolos de transferencia de ficheros mas usado en Internet. Es un método de software usado para transferir archivos desde una ubicación remota a una máquina local, o viceversa.

H

HACKER

Experto en informática capaz de de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

HOST

Anfitrión. Computador central o principal en un entorno de procesamiento distribuido. Por lo general se refiere a un gran computador de tiempo compartido o un computador central que controla una red.

I

ITERACIÓN

Repetición

K

KERBEROS

Sistema de seguridad basado en códigos simétricos.

L

LAN

Local Area Network. Red de área local.

M

MAN

Metropolitan Area Network. Red de área metropolitana.

N

NODO

Es el punto en donde se producen dos o más conexiones en una red de comunicaciones. No se trata de un elemento estrictamente físico, sino de una unidad funcional que exige hardware y software.

O

OSI

Open system interchange [interconexión de sistemas abiertos] Es un conjunto de protocolos que permiten vincularse juntas a computadoras de orígenes diferentes.

OUTSOURCING

Es la contratación de servicios especializados con terceros.

P

PCT

Private Communications Technology. Protocolo de seguridad aplicable en nivel de transporte.

PGP

Pretty Good Privacy. Sistema completo para la protección de correo electrónico y archivos adjuntos.

PROTOCOLO

Protocolo de comunicaciones. Estándares de hardware o software que gobiernan la transmisión entre estaciones. En computadores personales, los programas de comunicaciones ofrecen una variedad de protocolos (para transferir archivos a través de un módem).

R

REVOCACION

Anulación de algo que estaba establecido.

RSA

Rivest, Shamir, Adelman [public key encryption algorithm]. Algoritmo de encriptación de clave publica desarrollado por Rivest, Shamir y Adelman.

S

SERVIDOR PROXY

Servidor Caché. El Proxy es un servidor de que conectado normalmente al servidor de acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.

SET

Secure Electronic Transactions. Protocolo criptográfico diseñado para el envío de números de tarjeta de crédito a través de internet.

S-HTTP

Secure – Hyper Text Transfer Protocol. Sistema par encriptar infomración enviada mediante el protocolo http de web

SNIFFER

Literalmente "Husmeador". Pequeño programa que busca una cadena numerica o de caracteres en los paquetes que atraviesan un nodo con objeto de conseguir alguna información. Normalmente su uso es ilegal.

SSH

Secure Shell. Se trata de un intérprete de comandos seguro.

SSL

Secure Sockets Layer. Protocolo criptográfico para asegurar canales de comunicación bidireccionales.

S/MIME

Secure Multipurpose Internet Mail Extensión. Estádar seguro para enviar mensajes de correo electrónico con archivos binarios anexos.

T

TAXONOMIA

Ciencia que trata de los principios, métodos y fines de la clasificación.

TELNET

Protocolo y aplicaciones que permiten conexión como terminal remota a una computadora anfitriona, en una localización remota.

U

URL

Uniform Resource Locator. Se conoce por este nombre a las direcciones dentro de internet, normalmente aunque no necesariamente, refiriéndonos a páginas web. En este caso se distinguen por iniciarse con http://

W

WAN

Wide Area Network. Red de área ancha.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

1. CABALLERO, Pino. *Seguridad informática*, Alfaomega, 1997.
2. FINE, Leonard. *Seguridad en centros de cómputo: Políticas y procedimientos*, Trillas, 1990.
3. FÚSTER, Amparo. *Técnicas criptográficas de protección de datos*, Alfaomega Ra – Ma, 2001.
4. GARFINKEL S. y SPAFFORD G. *Practical Unix e Internet Security*, O'Reilly, 1996.
5. GARFINKEL S. y SPAFFORD G. *Seguridad y Comercio en el web*, Mc Graw Hill, O'Reilly, 1999.
6. NOMBELA, Juan José. *Seguridad informática*, Parainfo, 1997.
7. OPPLIEGER Rolph, *Sistemas de autenticación en red*, House-Inc ,1996
8. RODRÍGUEZ, Amador. *Protección de la información:Diseño de criptosistemas informáticos*, Parainfo, 1986.
9. STALLINGS, William. *Protect your privacy*, Prentice Hall, 1995.
10. TANENBAUM, Andrew. *Redes de ordenadores*, Prentice Hall, 1998.

DICCIONARIOS

- Diccionario etimológico de la lengua española. Fondo de cultura económica, 1995.
- Diccionario enciclopédico Espasa, Madrid, 1987.
- Diccionario enciclopédico ilustrado LAROUSSE.LAROUSEE, S.A. de C.V., 1998.
- Diccionario de informática. Publicaciones Cultural , 1999.
- Diccionario de informática. Díaz de Santos, Madrid, España. 1993
- Diccionario Océano de sinónimos y antónimos, Océano S.A. 1995
- Diccionario de inglés contemporáneo, Alambra, 1999.
- Diccionario de alemán Güntter Haensch, Herder, 1982.

TESIS

- López, Víctor, Análisis de riesgos en centros de cómputo, 2001 Lic. en Informática Facultad de Contaduría y Administración – UNAM.
- León, Genny, Estudio y análisis de mecanismos de autenticación en red, 2002 Lic. en Informática Facultad de Contaduría y Administración – UNAM.

INTERNET

- http://www.delitosinformáticos.com
- http://www.asc.unam.mx
- http://www.kriptopolis.com
- http://www.seguridata.com.mx